



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

n. 200 del 22/12/2022

OGGETTO: APPROVAZIONE NUOVO MANUALE DI GESTIONE DEI DOCUMENTI E CONSERVAZIONE.

L'anno **duemilaventidue** il giorno **ventidue** del mese di **dicembre** alle ore **13:00** nella residenza municipale, si è riunita la Giunta comunale.

Risultano presenti:

DAVIDDI GIUSEPPE	Sindaco	Presente
MISELLI SILVIA	Vicesindaco	Presente
RONCARATI ALESSIA	Assessore	Presente
FARINA LAURA	Assessore	Presente
BENASSI DANIELE	Assessore	Presente
AMAROSSI VALERIA	Assessore	Assente

Assiste il Vicesegretario CURTI JESSICA.

IL Sindaco DAVIDDI GIUSEPPE constatato il numero legale degli intervenuti dichiara aperta la riunione e li invita a deliberare sull'oggetto sopra indicato.



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

Oggetto: APPROVAZIONE NUOVO MANUALE DI GESTIONE DEI DOCUMENTI E CONSERVAZIONE.

LA GIUNTA COMUNALE

Richiamati i seguenti atti:

- Delibera di C.C. n. 23 del 21/03/2022 ad oggetto: "Documento Unico di Programmazione (DUP)- Periodo 2022/2024 - Nota di Aggiornamento";
- Delibera di C.C. n. 24 del 21/03/2022 ad oggetto: "Approvazione del Bilancio di Previsione 2022-2024", modificato con le segg.ti deliberazioni di consiglio comunale nn. 42,56,62,66,81 e 90 del 2022;
- Delibera di G.C. n. 27 del 23/03/2022 ad oggetto: "Approvazione del Piano Esecutivo di Gestione 2022/2024 e assegnazione delle risorse finanziarie ai responsabili di settore", modificata con le segg.ti delibere di giunta comunale nn. 27,60,74,88,92,107,139,168 e 183 del 2022;

Visti

- il D. Lgs. 82/2005, recante "Codice dell'amministrazione digitale" e ss.mm. e ii.;
- il D.P.R.445/2000, recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" e, in particolare, l'art.50 c.3, che prevede l'obbligo per le pubbliche amministrazioni di provvedere a realizzare e a revisionare i sistemi informatici e automatizzati dedicati alla gestione del protocollo informatico e dei procedimenti amministrativi;
- il D.P.C.M. 3 dicembre 2013 contenente le regole tecniche per il protocollo informatico ed in particolare l'art. 3 c.1 lett. d), e l'art.5 che prevedono per le Pubbliche Amministrazioni l'adozione di un manuale per la gestione, anche ai fini della conservazione dei documenti informatici, in grado di fornire precise istruzioni per il corretto funzionamento del servizio del protocollo informatico, della gestione dei flussi documentali e degli archivi;
- il D.P.C.M. 13 novembre 2014 che detta le regole per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici sia per i privati che per le pubbliche amministrazioni;

Premesso che con propria deliberazione n. 297 del 23/12/2003 il Comune di Casalgrande, in attuazione della normativa in materia di protocollo informatico, gestione dei flussi documentali e tenuta dell'archivio, ha adottato alcuni primi provvedimenti organizzativi:

- ha individuato nel Comune di Casalgrande un'unica Area organizzativa omogenea, denominata "Amministrazione Comunale Casalgrande";
- ha istituito il servizio "protocollo-archivio" al quale sono affidati i compiti precisati all'art. 61 del DPR 445/2000 ed affidare al responsabile del servizio stesso la predisposizione del manuale di gestione;

Dato atto che, con successiva delibera di giunta comunale n. 23/12/2015, ha proceduto all'approvazione dell'attuale manuale di gestione dei documenti e tenuta del protocollo informatico;



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

Visti:

- la deliberazione della Giunta Comunale n. 140 del 30/12/2013, avente ad oggetto l'“Approvazione schema di convenzione con l'istituto per i beni artistici, culturali e naturali della Regione Emilia Romagna (IBACN) per lo svolgimento della funzione di conservazione dei documenti informatici”;
- la deliberazione della Giunta dell'Unione Tresinaro Secchia n. 4 del 18/02/2015 avente ad oggetto: Piano di informatizzazione delle procedure per la presentazione di istanze, dichiarazioni e segnalazioni online (art.24 C.3-bis D.L. N. 90/2014 CONV. L. N.114/2014) che prevede, tra l'altro, la valutazione delle modalità di invio in conservazione sostitutiva dei documenti digitali al Parer (Polo archivistico regionale che garantisce conservazione a norma);

Premesso che:

- la gestione documentale dei procedimenti amministrativi garantisce la corretta amministrazione dei documenti, dalla produzione alla conservazione;
- in quest'ottica, con la determinazione n. 407/2020, AgID ha adottato le “Linee guida per la formazione, gestione e conservazione dei documenti informatici”, dopo aver esperito la procedura di informazione prevista dalla Direttiva (UE) 2015/1535 e dalla Legge 317/86, come modificata con D. Lgs. 223/2017;
- le linee guida sono state oggetto di consultazione pubblica, svolta dal 17 ottobre al 16 novembre 2019, ai sensi dell'articolo 71 del decreto legislativo n. 82/2005, come integrato e modificato dal D. Lgs. 217/2017, e adottate dopo aver sentito l'Autorità garante per la protezione dei dati personali e il Ministero per l'innovazione tecnologica e la digitalizzazione, nelle materie di competenza, e aver acquisito il parere della Conferenza Unificata;
- a seguito di numerose interlocuzioni e richieste di modifica provenienti da associazioni di categoria e amministrazioni, per quanto attiene in particolare l'Allegato 5 - Metadati e l'Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati, AgID ha provveduto all'aggiornamento di tali allegati, nonché alla correzione di alcuni refusi nel testo delle Linee guida adottati con nuova Determinazione n. 371/2021;

Dato atto che:

- con determinazione n. 766/2021 è stato dato in affidamento ad un'azienda specializzata in materia archivistica e di gestione documentale - Archimedia s.r.l., con sede a Modena - la revisione sistematica del manuale di gestione documentale;
- nel corso dell'anno 2022 si è provveduto alla mappatura presso i singoli settori dell'attività inerente la protocollazione e l'archiviazione della documentazione in carico ai medesimi;
- è stato realizzato con l'azienda produttrice del software del protocollo informatico – ADS s.r.l. - un intervento volto ad adeguare il software medesimo alle nuove normative;

Richiamato il Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation – Regolamento UE2016/679);

Vista la documentazione prodotta da Archimedia srl in attuazione del predetto incarico,



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

acquisita a prot. n. 22348 del 9 dicembre 2022;

Ritenuto quindi di approvare, quale parte integrante della presente delibera, il nuovo manuale di gestione documentale, revisionato ed aggiornato secondo quanto previsto dalle "Linee guida per la formazione, gestione e conservazione dei documenti informatici" emanate da Agid, nonché la documentazione ad esso allegata (allegati da 1 a 8);

Dato atto altresì che il presente provvedimento non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'Ente;

Preso atto che, sulla proposta della presente deliberazione, ai sensi degli articoli 49 comma1, e 147-bis comma 1, del D.Lgs 267/2000, il Responsabile del settore "Affari Generali" ha espresso parere favorevole in ordine alla regolarità tecnica attestante la regolarità e la correttezza dell'azione amministrativa;

Ritenuta la propria competenza ai sensi dell'art.48, comma 1 del D.Lgs 18/08/2000 n. 267;

Ritenuto di provvedere in merito;

Con voti favorevoli unanimi espressi nelle forme di legge;

DELIBERA

1. di approvare, per le motivazioni in premessa, la seguente documentazione, allegata al presente atto quale parte sostanziale:

- **"Manuale di gestione documentale e conservazione"**, aggiornato secondo quanto previsto dalle "Linee guida per la formazione, gestione e conservazione dei documenti informatici" emanate da Agid, allegato al presente atto quale parte integrante e sostanziale
- **Allegato 1** - Aree Organizzative Omogenee
- **Allegato 2** – Nomina del responsabile dell'AOO e del Servizio per la tenuta del protocollo informatico;
- **Allegato 3** – Abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica dei documenti
- **Allegato 4** – Titolario di classificazione e piano di conservazione dell'archivio
- **Allegato 5** – Documenti soggetti a registrazione in registri particolari, repertori, albi, elenchi, raccolte di dati concernente stati, qualità personali, fatti, gestiti con il sistema di protocollo informatico come indicati all'interno al manuale operativo del sistema documentale
- **Allegato 6** – Formati elettronici abilitati e manuale di conservazione Parer
- **Allegato 7** – Convenzione per la conservazione digitale



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

- **Allegato 8** – Registro di emergenza

2. di dare atto che l'allegato Manuale di gestione dei documenti ed il titolario di classificazione, ivi allegato, sostituiscono quello adottato con la precedente Deliberazione di Giunta Comunale n. 146 del 23.12.2015;
3. di dare atto che il Manuale verrà pubblicato sul sito web istituzionale, così come previsto dalla normativa vigente, e trasmesso via e-mail a tutti i responsabili di settore/servizio ed al SIA Unione Tresinaro Secchia;
4. di dare atto, altresì, che il Manuale di gestione è strumento di lavoro necessario alla corretta tenuta del protocollo ed alla gestione del flusso documentale e dell'archivio e pertanto dovrà essere aggiornato quando innovazioni tecnologiche, nuove situazioni organizzative o normative lo richiedano o, comunque ogni qualvolta si renda necessario alla corretta gestione documentale;
5. di ottemperare all'obbligo imposto dal D.Lggs. n. 33/2013, art. 23 disponendo la pubblicazione sul sito istituzionale del Comune di Casalgrande nella sezione "Amministrazione trasparente";

Ravvisata l'urgenza visto l'intervenuto aggiornamento del software di gestione documentale;

Con voto unanime e palese,

DELIBERA, inoltre

Di dichiarare la presenta deliberazione immediatamente eseguibile ai sensi e per gli effetti dell'art. 134 comma 4 del Tuel 18/08/2000 n. 267 nel suo testo vigente



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

IL Sindaco
DAVIDDI GIUSEPPE

IL Vicesegretario
CURTI JESSICA



COMUNE DI CASALGRANDE

MANUALE DI GESTIONE DOCUMENTALE E
CONSERVAZIONE

INDICE

PARTE I **DISPOSIZIONI GENERALI E ORGANIZZAZIONE**

- Art. 1 Definizioni
- Art. 2 Ambito di applicazione
- Art. 3 Aree Organizzative Omogenee
- Art. 4 Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi
- Art. 5 Responsabile della gestione documentale

PARTE II **FORMAZIONE DEI DOCUMENTI**

- Art. 6 Modalità di formazione del documento informatico
- Art. 7 Redazione/formazione del documento amministrativo informatico
- Art. 8 Il documento amministrativo informatico costituito dal corpo della PEC istituzionale
- Art. 9. Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale
- Art. 10. Validazione temporale
- Art. 11 Formato dei documenti e firme digitali
- Art. 12. Redazione/formazione del documento amministrativo analogico
- Art. 13 Segnatura di protocollo
- Art. 14 Sigillo elettronico qualificato

PARTE III **INVIO E RICEZIONE DEI DOCUMENTI**

- Art. 15 Invio e ricezione dei documenti
- Art. 16 Invio dei documenti amministrativi informatici
- Art. 17 Duplicato del documento informatico e analogico
- Art. 18 Copia per immagine su supporto informatico di documenti informatici e analogici
- Art. 19 Estratto informatico di documento amministrativo informatico
- Art. 20 Copia analogica di documento amministrativo informatico
- Art. 21 Ricezione della corrispondenza su supporto analogico
- Art. 22 Apertura della corrispondenza analogica in entrata
- Art. 23 Copie per immagine su supporto informatico di documenti analogici in entrata
- Art. 24 Validità dei documenti informatici in entrata
- Art. 25 - Documenti trasmessi tra pubbliche amministrazioni
- Art. 26 Rilascio di ricevute attestanti la consegna dei documenti

PARTE III **REGISTRAZIONE DEI DOCUMENTI**

- Art. 27 Il protocollo informatico: requisiti tecnologici e funzionalità

- Art. 28 Registrazione di protocollo
- Art. 29 Documenti soggetti a registrazione obbligatoria di protocollo
- Art. 30 Interoperabilità e cooperazione applicativa
- Art. 31 Il registro giornaliero di protocollo
- Art. 32 Annullamento o modifica delle registrazioni di protocollo
- Art. 33 Riservatezza delle registrazioni di protocollo
- Art. 34 Registro di emergenza

PARTE IV

FLUSSI DI LAVORAZIONE DEI DOCUMENTI

- Art. 35 Consegna dei documenti
- Art. 36 Smistamento ed assegnazione dei documenti
- Art. 37 Presa in carico dei documenti
- Art. 38 Classificazione dei documenti
- Art. 39 Fascicolazione dei documenti e tipologie di fascicoli
- Art. 40 Formazione, implementazione, gestione ed elenco minimo di metadati descrittivi
- Art. 41 Fascicoli ibridi o misti
- Art. 42 Tenuta degli archivi correnti, dei fascicoli e delle serie documentarie

PARTE V

SICUREZZA DEI SISTEMI E DEI DOCUMENTI INFORMATICI

- Art. 43 Misure di sicurezza nella formazione e gestione dei documenti
- Art. 44 Misure tecniche di sicurezza informatica dei sistemi
- Art. 45 Misure di sicurezza del sistema informativo integrato di gestione documentale
- Art. 46 Misure di sicurezza del sistema informativo integrato di gestione documentale
- Art. 47 Misure di sicurezza informatica di carattere organizzativo-gestione dei profili abilitativi

PARTE VI

GESTIONE DELL'ARCHIVIO DI DEPOSITO

- Art. 48 Archivio di deposito
- Art. 49 Trasferimento dei documenti all'Archivio di deposito (fascicoli analogici o ibridi)
- Art. 50. Sistema di conservazione dei documenti informatici
- Art. 51. Responsabile della conservazione
- Art. 52. Oggetti della conservazione
- Art. 53. Formati ammessi per la conservazione
- Art. 54 Modalità e tempi di trasmissione dei pacchetti di versamento
- Art. 56 Accesso al Sistema di conservazione
- Art. 57. Selezione e scarto dei documenti
- Art. 58. Misure di sicurezza e monitoraggio dei documenti digitali

Appendice A: glossario DPCM 3 dicembre 2013

Allegato 1 Aree Organizzative Omogenee

Allegato 2 – Nomina del Responsabile della Gestione documentale

Allegato 3 – Abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica dei

documenti

Allegato 4 – Titolario di classificazione

Allegato 5 - Funzionalità del sistema di gestione informatica dei documenti

Allegato 6 – Manuale di conservazione

Allegato 7 – Contratto di servizio per la conservazione digitale

Allegato 8 – Registro di emergenza

PARTE I DISPOSIZIONI GENERALI E ORGANIZZAZIONE

Art. 1 Definizioni

Ai fini del presente manuale si applicano le definizioni contenute nelle Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici in vigore dal 1° gennaio 2022.

Ulteriori norme rilevanti ai fini della gestione documentale sono:

1. le disposizioni in materia di formazione dei documenti informatici, anche di natura amministrativa, e di digitalizzazione dell'attività amministrativa di cui al d.lgs. 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale*" (di seguito anche solo "CAD")
2. le disposizioni in materia di documentazione amministrativa di cui al D.P.R. 28 dicembre 2000, n. 445 "*Disposizioni legislative in materia di documentazione amministrativa*" (di seguito anche solo "TUDA");
3. le norme sul procedimento amministrativo di cui alla L. 7 agosto 1990, n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";
4. le disposizioni sulla trasparenza di cui al D.Lgs. 14 marzo 2013, n. 33 "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*";
5. le disposizioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno di cui al Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014 (Regolamento "eIDAS");
6. le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "*Regolamento generale sulla protezione dei dati*" ("GDPR") e d.lgs. 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali*".

Art. 2 Ambito di applicazione

Il Manuale è un documento interno di contenuto sia organizzativo che operativo, utile quale strumento di supporto ai processi decisionali e operativi e, pertanto, è destinato alla più ampia diffusione presso tutto il personale dell'ente. Il presente Manuale e i suoi allegati sono approvati con delibera di Giunta su proposta del Responsabile della gestione documentale dell'Ente. L'aggiornamento degli allegati, quando non comporta modifiche sostanziali ai contenuti del presente Manuale, è effettuato con determinazione del Responsabile della gestione documentale.

Con la pubblicazione nella sezione "Amministrazione Trasparente" del sito internet istituzionale (<https://www.comune.casalgrande.re.it/ilcomune/iregolamenti/>) il Manuale è reso noto anche esternamente all'ente. Deve, inoltre, essere capillarmente divulgato alle unità organizzative responsabili (UOR) dell'unica Area Organizzativa omogenea del Comune di Casalgrande (AOO), al

fine di consentire la corretta diffusione delle nozioni e delle procedure documentali. È prevista, infine, un'attività di formazione continua e permanente in materia di gestione documentale per tutte le unità organizzative responsabili del Comune su tutti i punti contenuti in questo manuale di gestione. In quest'ottica, il Manuale costituisce altresì un documento pubblico funzionale al perseguimento del principio di trasparenza dell'azione amministrativa.

Art. 3 Aree Organizzative Omogenee

Per garantire una gestione documentale unitaria e coordinata, l'Amministrazione ha istituito un'unica Area Organizzativa Omogenea (AOO) individuata con Deliberazione della Giunta Comunale n. 297 del 3/12/2003. Le UOR che afferiscono alla AOO sono definite con riferimento all'organigramma dell'Ente disponibile al link: <https://www.comune.casalgrande.re.it/ilcomune/amministrazionetrasparente>, possono essere oggetto di modifiche e integrazioni per effetto degli interventi sulla struttura organizzativa e sono descritte nell'allegato 1.

1. L'amministrazione è accreditata presso www.indicepa.gov.it dal 01/06/2010, codice IPA amministrazione c_b893.
2. All'AOO è stata attribuita una casella di posta elettronica certificata presente sull'IPA e interoperabile con il protocollo informatico: casalgrande@cert.provincia.re.it, demografici.casalgrande@cert.provincia.re.it, e una casella di posta elettronica ordinaria (PEO) urp@comune.casalgrande.re.it.

Art. 4 Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi

1. Nell'ambito dell'AOO di cui all'articolo 3, è istituito un servizio per la tenuta del protocollo informatico e dell'archivio che coincide con l'Ufficio protocollo e archivio, di seguito denominato Servizio, i cui estremi identificativi sono riportati nell'allegato n. 1. Tale servizio garantisce la corretta gestione, tenuta e tutela dei documenti, vigila sull'osservanza degli adempimenti previsti in ambito archivistico dalla normativa in materia di gestione documentale durante l'intero ciclo di vita dei documenti.
2. Al Responsabile del Servizio sono assegnati i seguenti compiti:
 - garantisce il corretto svolgimento delle attività di gestione dei documenti, nonché la formazione, gestione, conservazione e fruizione dell'archivio;
 - attribuisce il livello di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
 - garantisce che le operazioni di registrazione, segnatura, gestione dei documenti e dei flussi documentali si svolgano nel rispetto della normativa vigente;
 - garantisce la corretta produzione e l'invio in conservazione del registro giornaliero di protocollo;
 - garantisce che le funzionalità del sistema in caso di guasti o anomalie siano ripristinati entro ventiquattrore dal blocco delle attività e, comunque, nel più breve tempo possibile.
 - La notifica ai responsabili delle UOR dell'eventuale indisponibilità del sistema e l'attivazione del registro di emergenza
 - predispone e mantiene aggiornati il titolario di classificazione dei documenti e il piano di conservazione dell'archivio, compresi gli indici e tutti gli altri strumenti archivistici necessari;
 - autorizza le operazioni di annullamento delle registrazioni di protocollo;
 - vigila sull'osservanza delle disposizioni del presente manuale e tiene aggiornati gli allegati

Art. 5 Responsabile della gestione documentale

1. A capo del Servizio è posto il Responsabile della gestione documentale cioè il Responsabile del Servizio protocollo e archivio, il cui nominativo e quello del suo vicario (nei casi di vacanza, assenza o impedimento) sono riportati nell'allegato n. 2.
2. Al Responsabile della gestione documentale sono assegnati i compiti di cui al paragrafo 3.4 delle Linee Guida AGID e art. 60 del TUDA:
 - predisporre e mantenere aggiornato il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici, nel rispetto della normativa in materia di trattamento dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione, e d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali;
 - definire e assicurare criteri uniformi di trattamento dei documenti e di classificazione e archiviazione, nonché di comunicazione interna tra le UOR e verso le AOO di altre amministrazioni;
 - predisporre, di concerto con il responsabile della conservazione, il responsabile dei sistemi informativi e con il responsabile del trattamento dei dati personali, il piano per la sicurezza informatica di continuità operativa, di protezione dei dati personali e di analisi del rischio;
 - sovrintendere e monitorare i processi e le attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;
 - formare correttamente la documentazione che andrà a costituire il pacchetto di versamento (PdV) e assicurare la sua trasmissione al sistema di conservazione con i formati concordati con il conservatore e secondo le modalità operative descritte nel manuale di conservazione del sistema di conservazione;
 - verificare l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

Il Responsabile della gestione documentale anche in riferimento alle funzioni proprie del referente dei sistemi informatici e della sicurezza informatica e del referente della protezione dei dati personali relativamente al sistema documentale può, sotto la propria responsabilità, delegare in tutto o in parte i propri compiti al personale posto sotto la propria direzione.

PARTE II – FORMAZIONE DEI DOCUMENTI

Art. 6 Modalità di formazione del documento informatico

Il documento informatico è formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software (ad esempio, mediante programmi di scrittura delle suite *Libre Office*): in tal caso il documento informatico assume le caratteristiche di immutabilità e di integrità mediante la sottoscrizione con firma digitale/firma elettronica qualificata o con l'apposizione di una validazione temporale o con il trasferimento a soggetti terzi con PEC con ricevuta completa o con la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza o con il versamento ad un sistema di conservazione;
- acquisizione:
 - di un documento informatico per via telematica o su supporto informatico
 - della copia per immagine su supporto informatico di un documento analogico
 - della copia informatica di un documento analogico: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione (ad esempio, utilizzo di software gestionali verticali)

- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei *log* di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione. (ad esempio, generazione del registro di protocollo giornaliero)

Art. 7 Redazione/formazione del documento informatico

Il documento amministrativo è qualsiasi rappresentazione, comunque formata, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione.

Gli atti formati con strumenti informatici, nonché i dati e i documenti informatici detenuti dall'AOO, costituiscono informazione primaria e originale da cui è possibile effettuare duplicazioni e copie. Il documento informatico e le istanze, le dichiarazioni e le comunicazioni previste dalla legge sono soggette a registrazione di protocollo, segnatura, fascicolatura e repertorizzazione.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità anche con la registrazione nel registro di protocollo unico per l'Area Organizzativa Omogenea (AOO), nei repertori e negli albi contenuti nel sistema di gestione documentale.

Il documento amministrativo informatico deve, di norma, contenere la denominazione del Comune di Casalgrande e l'indicazione di:

- AOO/ UOR;
- Data di sottoscrizione;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (indicare 0 *zero* se non presenti);
- Oggetto;
- Destinatario;
- Testo;
- Iniziali di redattore/responsabile;
- Sottoscrizione;
- Elementi identificativi del responsabile del procedimento.

Il documento è sottoscritto prima di essere protocollato. Le informazioni relative alla classificazione atte a identificare il fascicolo di competenza, la data di sottoscrizione, il numero di allegati sono inserite prima della sottoscrizione del documento.

Di norma, la data di sottoscrizione e la data di protocollazione coincidono.

Art. 8 Il documento amministrativo informatico costituito dal corpo della PEC istituzionale

Il documento trasmesso/ricevuto con PEC ha lo stesso valore legale della raccomandata con avviso di ricevimento. In tal caso, l'avvenuta consegna del messaggio elettronico consente tra l'altro di ricorrere contro terzi. Di norma, si dovrebbe usare la PEC per trasmettere e/o ricevere un documento informatico, ma può accadere che la comunicazione/istanza ricevuta sia costituita dal mero corpo della *email*.

In questo caso si procede alla registrazione del messaggio in arrivo nel sistema di gestione documentale solo se il contenuto è rilevante al fine giuridico probatorio.

Art. 9 Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale

L'*email* costituisce un documento informatico sottoscritto con firma elettronica semplice, in quanto il mittente viene identificato inserendo il proprio *username* e la propria *password*.

Le *email* inviate da una casella istituzionale del Comune di Casalgrande sono considerate sottoscritte con firma elettronica semplice e sono soggette a protocollazione solo se il contenuto è rilevante al fine giuridico probatorio. In questo caso si procede alla conversione dell'*email* in formato PDF/A prima di provvedere alla sua registrazione.

Art. 10 Validazione temporale

Costituiscono validazione temporale:

- i riferimenti temporali realizzati dai certificatori accreditati mediante marche temporali;
- i riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato secondo la scala di tempo UTC (IT) (INRiM) con una differenza non superiore ad un minuto primo;
- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata;
- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica.

Art. 11 Formato dei documenti e firme digitali

- Il formato del documento informatico creato dal Comune di Casalgrande deve essere scelto tra i seguenti **formati standard**: .rtf, .docx, .odt, .pdf, .xlsx, .ods, .xml.
- Eventuali formati differenti possono essere utilizzati in relazione a specifiche e comprovate esigenze. Il formato del documento informatico, in ogni caso, deve essere preferibilmente individuato tra quelli previsti nell'Allegato 2 alle Linee guida dell'AgID ed adottato osservando le raccomandazioni ivi contenute.
- Le versioni del documento precedenti alla versione definitiva (bozze, minute, ecc.), possono essere salvate in un formato che ne consenta la modificabilità (ad esempio, .docx o .odt). La versione definitiva del documento, invece, è sempre preferibile sia in formato PDF.
- I documenti di maggiore rilevanza giuridico-amministrativa (ad esempio, gli atti del Sindaco e degli organi collegiali, i contratti, le determine a contenuto provvedimentale, ecc.), prima della firma, devono essere convertiti in formato PDF/A (PDF non modificabile). I documenti in formato PDF e PDF/A sono sottoscritti con firma PADES.
- Nel caso il documento definitivo sia di un formato diverso dal PDF, la sottoscrizione avviene con firma CADES (.p7m).
- Se il documento è oggetto di conservazione deve essere predisposto il relativo formato PDF/A.

Art. 12 Redazione/formazione del documento analogico

Il documento analogico è un documento formato su supporto analogico prodotto con strumenti analogici (ad es., documento scritto a mano) o con strumenti informatici (ad es., documento prodotto con un sistema di video scrittura) e stampato su carta.

I documenti analogici dotati di firma autografa aventi per destinatario un ente o un soggetto terzo, sono di norma redatti in due esemplari, un originale per il destinatario e una minuta da conservare agli atti nel fascicolo corrispondente.

Il documento amministrativo analogico in uscita è redatto su carta intestata e deve, di norma, contenere la denominazione del Comune di Casalgrande e l'indicazione di

- AOO/ UOR;
- Data di sottoscrizione;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati;
- Oggetto;
- Destinatario;
- Testo;
- Sottoscrizione;
- Sigla eventuali istruttori;
- Elementi identificativi del responsabile del procedimento.

Il documento è sottoscritto prima di essere protocollato; di norma la data di sottoscrizione e la data di protocollazione coincidono.

Ai sensi del DPCM 21 marzo 2013, per particolari tipologie di documenti analogici originali unici, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato.

Per documenti originali unici si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta (ad es., i verbali di una commissione consiliare, etc.).

Pertanto, tutti i documenti su cui vengono apposti manualmente dati di registrazione a protocollo, sigle e firma autografa (che non sono sottoscritti con firma elettronica, semplice, avanzata o digitale), sono documenti amministrativi analogici.

Art.13 Segnatura di protocollo

Nell'ambito del sistema di interoperabilità tra enti, la segnatura di protocollo consente l'individuazione in modo inequivocabile di ciascun documento (identificazione univoca e certa).

Nei documenti informatici, la segnatura viene associata in forma permanente e immutabile al documento principale e agli allegati che con esso formano il messaggio di protocollo. La segnatura viene creata e associata in forma automatica al documento, contemporaneamente alla sua protocollazione; in questo modo, le informazioni della segnatura di protocollo vengono memorizzate nel Sistema informativo integrato di gestione documentale.

La segnatura si compone dei seguenti dati:

- indicazione dell'amministrazione mittente (Codice IPA, identificativo del Comune di Casalgrande);

- indicazione della AOO mittente (Codice AOO, identificativo del Comune di Casalgrande nell'Indice dei Domicili digitali);
- indicazione del registro nell'ambito del quale è stata effettuata la registrazione;
- numero progressivo di protocollo (generato automaticamente dal Sistema e registrato in forma non modificabile);
- data di registrazione (come sopra);
- oggetto del messaggio di protocollo;
- classificazione del messaggio di protocollo;
- fascicolo del messaggio di protocollo;
- mittente e destinatario;
- codice dell'unità che ha prodotto il documento;
- codice identificativo dell'unità a cui il documento è assegnato;
- identificazione degli allegati;
- impronta del documento principale e degli eventuali allegati.

Le informazioni della segnatura di protocollo sono parte dei dati di registrazione e sono rese disponibili, per i documenti informatici in uscita, in un file conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition), definito e aggiornato periodicamente dall'Agenzia per l'Italia digitale.

Articolo 14 - Sigillo elettronico qualificato (documenti in uscita)

Nell'ambito del sistema di interoperabilità tra enti, per tutti i documenti in uscita, il Sistema produce in automatico il sigillo elettronico qualificato, allo scopo di garantire integrità e autenticità alla segnatura di protocollo. Detto sigillo, equivalente ad una firma elettronica qualificata, afferisce non ad una persona fisica, bensì a una persona giuridica, nella fattispecie, all'Amministrazione Comune di Casalgrande.

Nello specifico, in fase di produzione della segnatura informatica delle registrazioni di protocollo informatico in uscita, con spedizione tramite PEC, il Sistema appone il sigillo elettronico qualificato in maniera trasparente all'utente, in quanto governato da apposito parametro.

L'apposizione del sigillo presuppone che la registrazione di protocollo disponga di un file, inteso come documento principale e dei metadati di classificazione. In assenza di tali requisiti, il sigillo non verrà apposto e, conseguentemente, non sarà possibile l'invio del documento via PEC.

- Nei casi di eventuale malfunzionamento della procedura di apposizione del sigillo elettronico, è prevista la possibilità di gestire manualmente la spedizione via PEC del messaggio senza segnatura.

PARTE III

INVIO E RICEZIONE DEI DOCUMENTI

Art. 15 Invio e ricezione dei documenti

I documenti, siano essi analogici o informatici, in base allo stato di trasmissione si distinguono in:

- documenti in arrivo;
- documenti in partenza;
- documenti interni (scambiati tra UOR).

La comunicazione tra l'Area Organizzativa Omogenea – AOO del Comune di Casalgrande e le AOO appartenenti a differenti PA avviene nel rispetto delle indicazioni fornite dall'allegato 6 delle Linee guida AgID. È cura del Responsabile della gestione documentale valutare periodicamente la congruità dei metadati con le disposizioni normative e, se necessario, adottare le opportune azioni per promuoverne l'adeguamento tecnico funzionale.

La trasmissione di documenti dal Comune alle altre pubbliche amministrazioni avviene mediante l'utilizzo della posta elettronica certificata o in cooperazione applicativa; in ricezione tali modalità sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

Ai fini della verifica della provenienza le comunicazioni sono valide se soddisfano una delle seguenti condizioni:

- a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
- b) sono dotate di segnatura di protocollo;
- c) è possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente;
- d) sono trasmesse attraverso sistemi di posta elettronica certificata.

Art. 16 Invio dei documenti amministrativi informatici

La spedizione dei documenti amministrativi informatici avviene a cura dell'ufficio competente sul procedimento, al termine delle operazioni di sottoscrizione, registrazione di protocollo, segnatura, classificazione e fascicolazione dei documenti stessi.

La consegna dei documenti verso altre amministrazioni, imprese, ordini professionali, dipendenti o cittadini che hanno fornito il loro domicilio digitale, avviene mediante l'utilizzo della posta elettronica certificata dell'unità organizzativa (Settore-Servizio-Ufficio), titolare del procedimento. Più precisamente, una volta protocollate, le lettere in uscita e i relativi allegati, sono inviati all'indirizzo elettronico dichiarato dal destinatario. Non sono previsti altri utilizzi delle caselle PEC.

Il Sistema garantisce l'archiviazione automatica delle ricevute elettroniche di avvenuta accettazione e consegna telematica del documento inviato, associando le stesse alla relativa registrazione di protocollo. È cura dell'ufficio mittente controllare sulla Scrivania virtuale l'eventuale ritorno di notifiche di mancata consegna dei documenti inviati e, sulla maschera della registrazione di protocollo, le ricevute di consegna e le notifiche di eccezione (rifiuto del documento da parte del destinatario). Se l'indirizzo elettronico del destinatario non è certificato, è attestata solo l'avvenuta spedizione della lettera (Ricevuta di accettazione dell'invio).

L'attestazione di avvenuta spedizione e consegna digitale è disponibile solo registrando singolarmente i destinatari ed il relativo indirizzo digitale. Nel caso di destinatari multipli, il Sistema consente la creazione di specifiche liste di distribuzione, al fine di facilitare la predisposizione dei metadati.

Per i soggetti esclusi da obbligo di domicilio digitale è prevista la spedizione tramite posta tradizionale, raccomandata, o consegna a mano di copia analogica del documento digitale conservato (cioè predisposto e disponibile) presso il Comune di Casalgrande. Dette copie analogiche, tratte dagli originali digitali tramite procedura prevista dal Sistema (funzionalità "Copia conforme"), recanti l'indicazione a mezzo stampa del responsabile pro tempore, in sostituzione della firma autografa hanno la stessa efficacia probatoria dell'originale digitale da cui sono tratte. Sono escluse da questa modalità le certificazioni rilasciate dall'Amministrazione, da utilizzarsi nei rapporti tra privati.

Art. 17 Duplicato del documento informatico e analogico

Il duplicato del documento informatico è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto. I duplicati informatici hanno il medesimo valore giuridico del documento informatico da cui sono tratti se prodotti in conformità delle regole tecniche.

Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza. Il duplicato di un documento analogico è la riproduzione di un documento analogico originale distrutto o smarrito che lo sostituisce a tutti gli effetti legali: ad esempio, il rilascio della carta di identità etc.

Art. 18 Copia per immagine su supporto informatico di documenti informatici e analogici

La copia di documento informatico è un documento informatico che, mediante processi e strumenti idonei, assicura la corrispondenza della copia alle informazioni del documento informatico di origine attraverso l'utilizzo di uno dei formati idonei ai sensi della normativa vigente. La copia di documento informatico è, dunque, un documento informatico che muta il formato del documento originario o che muta il supporto del documento originario informatico (ad es., il salvataggio di un file in un formato differente: da *.doc* a *.pdf*, oppure da *.doc* a *.ods*).

Le copie del documento informatico hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta, fermo l'obbligo di conservazione dell'originale informatico.

È possibile produrre la copia su supporto informatico di documenti amministrativi in origine su supporto analogico. La copia informatica ha il medesimo valore dell'originale analogico da cui è tratta se attestata conforme dal funzionario a ciò delegato nei modi stabiliti dalla legge. L'attestazione di conformità può essere inserita nel documento informatico contenente la copia informatica o può essere prodotta come documento separato contenente un riferimento temporale e l'impronta di ogni copia.

In entrambi i casi l'attestazione dev'essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l'impronta di ogni copia o estratto informatico oggetto dell'attestazione.

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

Le copie informatiche di documenti analogici, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali hanno la medesima efficacia probatoria degli originali se a esse è apposta o associata, da parte di colui che le spedisce o le rilascia, una ² firma digitale o altra firma elettronica qualificata e

dichiarazione di conformità:

- per “rilascio” si intende la consegna di un supporto fisico idoneo a ricevere la memorizzazione della rappresentazione corrispondente al documento analogico e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale;
- per “spedizione” si intende l’inoltro telematico del/dei file corrispondenti per il tramite di un sistema di posta elettronica o di altro sistema di comunicazione informatica e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale.

Le copie per immagine su supporto informatico di documenti originali formati su supporto analogico hanno la medesima efficacia probatoria degli originali, se:

- la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le *Linee guida* AgID;
- sono formate nel rispetto delle *Linee guida* AgID e se la loro conformità all’originale non è espressamente disconosciuta.

Art. 19 Estratto informatico di documento amministrativo informatico

La copia che riproduce solo una parte del contenuto del documento viene definita “estratto”.

L’estratto di uno o più documenti informatici, se sottoscritto con firma digitale o firma elettronica qualificata da chi effettua l’estratto, hanno la stessa efficacia probatoria dell’originale, salvo che la conformità allo stesso non sia espressamente disconosciuta.

Laddove richiesta dalla natura dell’attività, l’attestazione di conformità può essere inserita nello stesso documento informatico contenente l’estratto, oppure prodotta come documento informatico separato; in entrambi i casi l’attestazione dev’essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l’impronta di ogni copia o estratto informatico oggetto dell’attestazione.

Art. 20 Copia analogica di documento amministrativo informatico

La copia analogica di documento amministrativo informatico è, di norma, la stampa cartacea.

La copia su supporto analogico di documento informatico, sottoscritto con firma elettronica avanzata, qualificata o digitale, per avere la stessa efficacia probatoria dell’originale da cui è tratta, deve essere certificata come conforme all’originale in tutte le sue componenti da un pubblico ufficiale autorizzato a eseguire tale attestazione nell’esercizio delle sue funzioni (copia “autentica”) salvo che la conformità allo stesso non sia espressamente disconosciuta. Resta fermo, ove previsto, l’obbligo di conservazione dell’originale informatico.

Art. 21 Ricezione della corrispondenza su supporto analogico

La corrispondenza in arrivo consegnata al Servizio protocollo, brevi manu dagli utenti, rispetta i seguenti orari, tutti i giorni feriali negli orari di apertura al pubblico pubblicizzati sul sito istituzionale del Comune.

I documenti consegnati direttamente agli uffici dell’AOO che non sono abilitati alla protocollazione in arrivo, se soggetti a registrazione di protocollo, sono fatti pervenire al Servizio a cura del personale che li riceve e nell’arco della stessa giornata.

I documenti consegnati direttamente agli uffici dell’AOO che sono abilitati alla protocollazione in arrivo

(ufficio protocollo e anagrafe), se soggetti a registrazione di protocollo, sono fatti pervenire a cura del personale che li riceve e nell'arco della stessa giornata agli operatori dello stesso ufficio cui compete l'attività di protocollazione. L'addetto allo smistamento dell'Ufficio Protocollo riceve i documenti analogici pervenuti all'Ente e colloca nel casellario della posta in arrivo la documentazione non soggetta a registrazione, in particolare: giornali, quotidiani, posta ordinaria restituita in quanto non recapitata, le buste contenenti le carte di identità, passaporti rilasciati dal Ministero dell'Interno e per le quali è stato richiesto il ritiro presso l'Ufficio anagrafe. Lo stesso dicasi per le licenze di porto d'armi rilasciate dal Sindaco brevi manu.

Qualora un documento cartaceo venga consegnato personalmente dall'interessato, o da altra persona incaricata, e venga richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, gli uffici abilitati possono rilasciare una fotocopia del primo foglio dopo avervi apposto il timbro meccanico riportante la data di arrivo e la sigla dell'operatore. In alternativa, l'ufficio ricevente che esegue la registrazione di protocollo rilascia la ricevuta prodotta automaticamente dal sistema di gestione informatica dei documenti. Appone sul documento ricevuto l'intestazione "Comune di Casalgrande" e la data di ricezione mediante un timbro meccanico a inchiostro nero indelebile.

Art. 22 Apertura della corrispondenza analogica in entrata

La corrispondenza in entrata su supporto cartaceo riportante la dicitura "riservato", "personale", "confidenziale", "S.P.M." o altre similari, non è aperta, ma consegnata in busta chiusa al destinatario il quale, dopo averne preso visione, se valuta che il documento ricevuto non è riservato ai sensi della normativa vigente in materia di privacy, è tenuto a trasmetterlo con la massima celerità all'ufficio preposto alla registrazione di protocollo in arrivo.

Qualora pervenga all'AOO un documento di competenza di un altro ente, altra persona fisica o giuridica, lo stesso è trasmesso a chi di competenza, se individuabile, altrimenti viene restituito al mittente.

Per quanto riguarda la corrispondenza pervenuta per errore sia in formato analogico che in formato digitale perché di competenza dell'Unione Tresinaro Secchia, il servizio protocollo

- registra in entrata la corrispondenza e la trasmette al servizio protocollo dell'Unione Tresinaro Secchia se si tratta di documento informatico
- produce una copia informatica del documento analogico, ne registra l'ingresso a sistema e lo trasmette al servizio protocollo dell'Unione Tresinaro Secchia se si tratta di documento analogico

Art. 23 Copie per immagine su supporto informatico di documenti analogici in entrata

1. I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e classificazione, possono essere acquisiti in formato digitale.
2. il processo di scansione si articola nelle seguenti fasi:
 - a) acquisizione delle immagini in modo che ad ogni documento, anche composto da più pagine, corrisponda un unico file di formato PDF/A;
 - b) verifica della qualità delle immagini acquisite e inserimento nel sistema di gestione informatica dei documenti.
 - c) collegamento delle immagini alle rispettive registrazioni di protocollo con la contestuale acquisizione delle loro impronte digitali;
 - d) memorizzazione delle immagini e delle relative impronte digitali nel sistema di gestione informatica dei documenti, in modo non modificabile.
3. I documenti ricevuti dall'Amministrazione su supporto cartaceo, ancorché digitalizzati con l'ausilio di scanner, al termine delle operazioni di registrazione, segnatura di protocollo, classificazione e assegnazione, sono fatti pervenire in originale agli uffici di competenza. Qualora la copia per immagine del documento analogico fosse prodotta al fine di sostituire l'originale, la conformità viene garantita mediante l'apposizione della firma digitale o firma elettronica avanzata da parte di chi effettua il raffronto.

Art. 24 Validità dei documenti informatici in entrata

I documenti informatici in entrata soddisfano il requisito della forma scritta qualora presentati in via telematica, con qualsiasi mezzo telematico o informatico idoneo ad accertarne la provenienza. Detta condizione è garantita qualora sia presente almeno uno dei seguenti requisiti:

- documento sottoscritto in forma autografa, scansionato e presentato unitamente alla scansione della copia del documento di identità;
- documento trasmesso dal richiedente o dal dichiarante dal proprio domicilio digitale, purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare;
- documento trasmesso tramite portali predisposti per la fruizione di servizi on line, da soggetti identificati tramite il Sistema pubblico di identità digitale (SPID) o con la carta di identità elettronica o con la carta nazionale dei servizi.

Art. 25 - Documenti trasmessi tra pubbliche amministrazioni

Ai fini del procedimento amministrativo, le comunicazioni tra il Comune di Casalgrande e le altre pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica certificata o in cooperazione applicativa; la loro validità è determinata dalla possibilità di verificarne la provenienza, condizione assolta dalla presenza di almeno uno dei seguenti requisiti:

- sottoscrizione del documento tramite firma digitale o altro tipo di firma elettronica qualificata;
- segnatura di protocollo e sigillo elettronico qualificato;
- trasmissione dei documenti attraverso cooperazione applicativa;
- trasmissione dei documenti attraverso sistemi di posta elettronica certificata.

All'interno del documento, l'indicazione del nominativo del soggetto responsabile del contenuto del documento, coincidente con il nominativo del sottoscrittore digitale, consentirà di esplicitare la fonte e la responsabilità dell'immissione e della trasmissione dell'atto, conferendo validità al contenuto del documento, fino a querela di falso.

Art. 26 Rilascio di ricevute attestanti la consegna dei documenti

Nel caso di documenti informatici in arrivo su una delle caselle PEC del Comune, provenienti da casella PEC, il Sistema invia al mittente un messaggio contenente la ricevuta di avvenuta consegna. Nel caso di istanze formate attraverso l'utilizzo dei portali messi a disposizione dall'Ente, la ricevuta di acquisizione dell'istanza viene prodotta in automatico dal Sistema nel momento stesso dell'inoltro dell'istanza, completa di segnatura di protocollo.

Nel caso di documenti cartacei consegnati a mano, qualora richiesto dal consegnatario, è previsto il rilascio, tramite procedura di protocollo, della ricevuta attestante l'avvenuta protocollazione del documento. In alternativa, e su richiesta, è prevista la semplice apposizione del timbro datario, siglato dall'operatore ricevente, su copia del documento, prodotta dall'operatore.

PARTE III **REGISTRAZIONE DEI DOCUMENTI**

Art. 27 Il protocollo informatico: requisiti tecnologici e funzionalità

Il Comune di Casalgrande utilizza l'applicativo PRISMA – Gestione Protocollo Informatico fornito dal Gruppo FINMATICA. La descrizione funzionale del protocollo informatico è costituita dal Manuale Utente aggiornato alla release in uso (allegato n. 5).

1. Ai sensi del punto 3.1.5 delle Linee Guida Agid il sistema di protocollo informatico assicura che:

- le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista dall'art. 54 del TUDA;
- le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
- le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
- per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema storicizzi tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili, nel rispetto di quanto previsto dall'art. 54, comma 2 del TUDA.
- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette da modifiche non autorizzate, archiviate e conservate.

2. Il sistema di cui al comma 1 garantisce inoltre:

- a) il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- b) il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate, archiviate e conservate.

La conformità del sistema di gestione informatica dei documenti ai requisiti minimi di cui ai commi 1 e 2 è attestata dal fornitore con idonea documentazione inclusa nella fornitura.

Il sistema di protocollo informatico dell'Amministrazione comprende la funzionalità minima, le funzionalità aggiuntive e le funzionalità interoperative, così come definite nel glossario riportato in appendice A.

Art. 28 Registrazione di protocollo

Per registrazione di protocollo si intende l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. La registrazione si effettua di norma entro la giornata di arrivo o comunque entro 24 ore lavorative dal ricevimento o, se intercorrono dei giorni festivi o di chiusura programmata del Comune, nel primo giorno lavorativo utile. Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immutabile.

La registrazione di protocollo per ogni documento è effettuata mediante la memorizzazione di elementi obbligatori immutabili, elementi obbligatori modificabili ed elementi non obbligatori e modificabili.

La registrazione degli elementi obbligatori immutabili del protocollo informatico non può essere modificata, integrata, cancellata ma soltanto annullata mediante un'apposita procedura in capo al Responsabile dell'Ufficio Archivio e Protocollo e al suo personale. L'immutabilità e l'immutabilità della registrazione di protocollo sono garantite dal sistema di gestione documentale.

Ciascuna registrazione di protocollo contiene dati obbligatori e dati accessori.

I dati obbligatori non modificabili sono:

- a) numero di protocollo, generato automaticamente dal sistema;
- b) data di registrazione di protocollo, assegnata automaticamente dal sistema;
- c) mittente per i documenti ricevuti, o destinatario per i documenti spediti;
- d) oggetto del documento;
- e) impronta del documento informatico
- f) numero degli allegati
- g) descrizione degli allegati

Gli elementi obbligatori modificabili sono:

- a) unità organizzativa responsabile del procedimento, affare,
- b) attività (UOR);

- c) responsabile del procedimento amministrativo (RPA);
- d) classificazione archivistica;
- e) fascicolo.

Gli elementi non obbligatori modificabili sono:

- a) Recapiti del mittente
- b) Collegamento ad altri fascicoli
- c) Tipologia del documento
- d) Durata della conservazione
- e) altri tipi di annotazioni

1. Le registrazioni di protocollo sono effettuate con il sistema di gestione informatica dei documenti in un'unica soluzione, ad esclusione di interventi intermedi, anche indiretti, da parte degli operatori.
2. La numerazione delle registrazioni di protocollo dei documenti di un'A OO è unica e progressiva. Essa si chiude il 31 dicembre di ogni anno e ricomincia da 1 all'inizio dell'anno successivo.
3. Il numero di protocollo è costituito da sette cifre numeriche.
4. Nella visualizzazione del numero di protocollo le posizioni più significative mancanti vengono riempite con gli '0' (zero).
5. Le lettere anonime sono registrate al protocollo generale indicando nel campo mittente la dicitura "anonimo". Fanno eccezione, e pertanto sono distrutte, quelle lettere anonime e quelle comunicazioni elettroniche il cui contenuto non riguarda le funzioni dell'Amministrazione ed è totalmente irrilevante per la comunità in genere.
6. Qualora dalla mancata registrazione a protocollo del documento nella medesima giornata lavorativa di ricezione possa venir meno un diritto di terzi, è prevista la protocollazione differita, cioè il differimento dei termini di registrazione, indicando in sede di protocollazione la data di arrivo del documento (campo specifico) e, nel campo note, le motivazioni del differimento.

Art. 29 Documenti soggetti a registrazione obbligatoria di protocollo

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dal Comune, ossia i cui destinatari sono esterni all'Ente e tutti i documenti informatici, ad eccezione di quelli espressamente esclusi dalla normativa vigente (TUDA, art. 53, comma 5) e altri documenti informatici già soggetti a registrazione particolare. Ugualmente sono esclusi gli atti relativi alle operazioni attinenti al censimento della popolazione o di altri censimenti particolari, i certificati di malattia, i DURC e la corrispondenza interna che, pur essendo parte della gestione di un procedimento amministrativo, non ha contenuto probatorio, i certificati anagrafici e di stato civile oltre ad estratti conto e comunicazioni di bonifici bancari.

Art. 30 Interoperabilità e cooperazione applicativa

1. Per quanto riguarda le registrazioni effettuate sul sistema di gestione informatica dei documenti che sono necessarie per l'aggiornamento di altre banche dati o, viceversa, ci sia la necessità di registrare su di esso i documenti prodotti e gestiti con altri sistemi dell'Amministrazione, si ricorre di norma ai meccanismi dell'interoperabilità e della cooperazione applicativa, che permettono l'interscambio automatico di dati e documenti tra software di produttori diversi.
2. Per le finalità di cui al comma 1, il sistema di protocollo informatico dell'Amministrazione implementa i meccanismi dell'interoperabilità e cooperazione applicativa basati su soluzioni tecnologiche e modelli standard conformi alle linee guida dettate dall'AGID.

Art. 31 Il registro giornaliero di protocollo

Il registro giornaliero di protocollo è prodotto in maniera automatica dal software di gestione documentale entro il giorno lavorativo seguente, mediante la generazione o il raggruppamento delle informazioni registrate secondo una struttura logica predeterminata e memorizzato in forma statica, immutabile e integra.

Il registro giornaliero è trasmesso al sistema di conservazione entro la giornata lavorativa successiva alla produzione.

Art. 32 Annullamento o modifica delle registrazioni di protocollo

1. Le registrazioni di protocollo possono essere annullate su autorizzazione del Responsabile della gestione documentale e con apposito documento autorizzativo.
2. Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema di gestione informatica dei documenti con un simbolo o una dicitura.
3. Non si annulla mai un documento informatico trasmesso con PEC in quanto il destinatario è già in possesso del documento stesso, con l'eccezione del caso in cui sia errato proprio l'indirizzo PEC del destinatario. Si può procedere con la redazione di un nuovo documento che annulla e sostituisce il precedente (in questo caso è necessario citare il riferimento del protocollo), è protocollato e inviato via PEC.
4. L'operazione di modifica di una registrazione di protocollo è eseguita con le seguenti modalità:
 - a) fra le informazioni generate o assegnate automaticamente dal sistema e registrate in forma non modificabile, l'annullamento anche di una sola di esse determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo;
 - b) delle altre informazioni, registrate in forma non modificabile, l'annullamento anche di un solo campo, che si rendesse necessario per correggere errori intercorsi in sede di immissione di dati, deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica; così analogamente per lo stesso campo, od ogni altro, che dovesse poi risultare errato.
 - c) le informazioni originarie, successivamente annullate, vengono memorizzate riportando, a seconda dei casi, un segno o una dicitura in posizione sempre visibile e tale, comunque, da consentire la loro lettura unitamente alla data, all'identificativo dell'operatore e agli estremi del provvedimento di autorizzazione.

Art. 33 Riservatezza delle registrazioni di protocollo

1. Ad ogni documento, all'atto della sua registrazione nel sistema di gestione informatica dei documenti, è assegnato un livello di riservatezza, che consente di stabilire quali utenti o gruppi di utenti possono avere accesso ad esso.
2. La visualizzazione delle informazioni nel sistema segue la logica dell'organizzazione e dei ruoli; pertanto, ciascun utente può accedere solamente ai documenti che ha prodotto o che gli sono stati assegnati direttamente, e a quelli dell'unità organizzativa cui appartiene.
3. I documenti a cui è stato assegnato un certo livello di riservatezza "PRIVACY" non vengono mai visualizzati agli utenti non autorizzati, neanche a fronte di una ricerca globale nell'archivio o una ricerca *full text*. Il sistema filtra l'accesso non soltanto al contenuto del documento ma anche ai dati della registrazione. Si tratta di tipologie di documenti per le quali sono previste particolari forme di riservatezza e di accesso controllato al protocollo unico secondo la normativa vigente relativamente a dati sensibili e giudiziari in esso contenuti.
4. Il Responsabile della gestione documentale individua, in collaborazione con Responsabile della *privacy*, le tipologie documentarie soggette a *privacy* e per ognuna di esse definisce le modalità di trattamento. Il documento risultante, denominato *policy* per la riservatezza dei dati e dei documenti gestiti nel sistema di protocollo informatico, è riportato nel sito web del Comune all'indirizzo

https://www.comune.casalgrande.re.it/wpcontent/uploads/2022/08/Privacypolicy_ComuneCasalgrande.pdf e nel “Documento programmatico della sicurezza” adottato da questo ente con deliberazione del Consiglio Comunale n. 214 in data 29 dicembre 2005 oltre al Regolamento sull'utilizzo delle risorse informatiche riportato al seguente indirizzo: <https://www.tresinarosecchia.it/wp-content/uploads/2022/09/Regolamento-utilizzo-risorse-informatiche.pdf>

Art. 34 Registro di emergenza

1. Il Responsabile della gestione documentale autorizza lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su registri di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema di gestione informatica dei documenti, allegato 8 “Registro di emergenza”.
2. In condizione di emergenza si applicano le seguenti modalità di registrazione e di recupero dei dati:
 - a) sul registro di emergenza sono riportate: la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema di gestione informatica dei documenti;
 - b) qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile della gestione documentale può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione;
 - c) per ogni giornata di registrazione di emergenza è riportato sul registro il numero totale di operazioni effettuate;
 - d) la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'Area Organizzativa Omogenea;
 - e) le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema di gestione informatica dei documenti, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza. Ciascun protocollatore è dotato degli strumenti necessari per provvedere alla protocollazione anche in condizione di emergenza e tutte le unità dovranno rivolgersi all'Ufficio Protocollo e Archivio per svolgere le operazioni di protocollazione (Iterno/Arrivo/Partenza).

PARTE IV

FLUSSI DI LAVORAZIONE DEI DOCUMENTI

Art. 35 Consegna dei documenti

Al termine delle operazioni di registrazione al protocollo e fascicolazione, i documenti pervenuti all'amministrazione in formato analogico o informatico vengono consegnati nel più breve tempo possibile ai destinatari interni competenti.

Articolo 36 Smistamento ed assegnazione dei documenti

I documenti protocollati in arrivo vengono smistati alle unità competenti e assegnati ai singoli componenti delle stesse. I destinatari ricevono in scrivania virtuale la notifica di avvenuto smistamento e/o assegnazione di documento, comprensiva dei dati essenziali del documento e della data di avvenuto smistamento. La notifica è di per sé link al documento e ai metadati di protocollo. Le funzioni di smistamento e assegnazione dei documenti si avvalgono della struttura organizzativa dell'Ente.

1. I dati di flusso (smistamento, assegnazione, presa in carico/rifiuto e archiviazione) sono accessibili direttamente accedendo alla maschera di protocollo di ciascun documento.
2. Lo smistamento e l'assegnazione su scrivania virtuale per competenza attribuiscono al ricevente una competenza di modifica dei dati archivistici del documento e la possibilità di effettuare ulteriori smistamenti per competenza.
3. L'unità che attiva lo smistamento mantiene anche successivamente i diritti di reperimento e visualizzazione sul documento smistato.

Articolo 37 Presa in carico dei documenti

I documenti notificati in scrivania virtuale possono essere presi in carico dall'ufficio, attraverso uno dei suoi componenti, o dal singolo componente destinatario in assegnazione, dopo valutazione della pertinenza del documento rispetto ai procedimenti trattati.

La presa in carico attesta l'effettiva assunzione di responsabilità sul documento da parte del destinatario ricevente.

Al momento della presa in carico, il ricevente può conservare il documento in scrivania virtuale, può smistarlo e assegnarlo a sua volta, oppure può archiviarlo all'interno dell'area documentale.

Il Sistema di gestione informatica dei documenti tiene traccia del flusso dei passaggi del documento all'interno dell'Ente, memorizzando, per ciascuno di essi, l'identificativo dell'utente che effettua l'intervento, la data e l'ora di esecuzione.

A seguito della presa in carico, l'ufficio ricevente può associare il documento ad un proprio fascicolo, utilizzando le funzionalità della classificazione e fascicolazione secondarie.

Con la funzione "Rifiuta smistamento" il destinatario di uno smistamento/assegnazione può restituire, con obbligo di motivazione, il documento ricevuto impropriamente.

Nel caso di mancata gestione di presa in carico o rifiuto di un documento da parte dell'ufficio destinatario nell'arco di sessanta giorni dalla notifica del documento in scrivania virtuale, il Sistema attiva la presa in carico automatica a carico dell'ufficio destinatario.

Articolo 38 Classificazione dei documenti

Tutti i documenti prodotti e ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, sono classificati in base al titolario riportato nell'allegato n. 4 per garantire il reperimento certo e veloce.

I documenti sono classificati a cura degli operatori che li registrano nel sistema di gestione informatica dei documenti avvalendosi del titolario, o piano di classificazione nazionale, strutturato sulla base delle funzioni dell'ente.

L'aggiornamento del titolario di classificazione dell'archivio compete al Responsabile della gestione documentale di concerto con i Responsabili delle UOR sulla base delle mutate esigenze normative ed in riferimento ai cambiamenti dell'organigramma dell'Ente. In questo caso, essi sono adottati a partire dal 1° gennaio dell'anno successivo a quello di approvazione.

Il titolario vigente è pubblicato nel sito web istituzionale, nella sezione "Amministrazione trasparente".

È garantita la storicizzazione delle variazioni del titolario di classificazione e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i vincoli tra le unità archivistiche, le unità documentarie e la struttura del titolario vigente al momento della loro produzione.

La sostituzione delle voci del titolario comporta l'impossibilità di aprire nuovi fascicoli nelle voci eliminate. Rimane possibile, invece, registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.

Art. 39 Fascicolazione dei documenti e tipologie di fascicoli

Gli atti, i documenti e i dati di procedimento e di processo, registrati al protocollo informatico o semplicemente acquisiti al Sistema, vengono raccolti in fascicoli informatici attraverso l'attività di

fascicolazione, intesa come attività sostanziale alla tenuta dell'Archivio, funzionale all'esercizio del diritto di accesso e alla efficiente gestione del procedimento amministrativo. Il fascicolo è l'unità di base dell'archivio. Ogni fascicolo conserva documenti che afferiscono a un medesimo affare, attività o procedimento amministrativo e sono classificati in maniera omogenea. La classificazione viene apposta (o associata) in base al contenuto e secondo il grado divisionale attribuito dal titolare (o piano di classificazione), salvo alcune eccezioni, come il fascicolo di persona.

All'interno di ciascun fascicolo i documenti sono inseriti secondo l'ordine cronologico di registrazione (ordine di sedimentazione), in maniera tale che l'inserzione a fascicolo individui subito il documento più recente. L'ordine di sedimentazione è rispettato anche all'interno dei sottofascicoli. L'obbligo di fascicolatura dei documenti riguarda sia i documenti contraddistinti dalla segnatura di protocollo sia i documenti istruttori e transitori non protocollati.

La corretta tenuta del fascicolo garantisce sia la sedimentazione che l'esercizio del diritto di accesso. Sono presenti cinque tipologie di fascicolo:

- *Affare*: conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata; per gli affari non esiste un termine per la conclusione previsto da norme;
- *Attività*: conserva i documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque previsto l'adozione di un provvedimento finale;
- *Procedimento amministrativo*: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un atto finale;
- *Persona fisica*: conserva i documenti relativi a diversi procedimenti amministrativi, distinti per affari o per attività, ma legati da un vincolo archivistico interno, relativo a una persona fisica determinata; la chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'Ente;
- *Persona giuridica*: conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica.

Art. 40 Formazione, implementazione, gestione ed elenco minimo di metadati descrittivi

Per ogni procedimento, affare e attività, il Comune di Casalgrande ha l'obbligo di conservare in un fascicolo gli atti, i documenti e i dati da chiunque formati su supporto informatico; Ogni fascicolo deve essere contraddistinto dai seguenti elementi, atti a determinarne l'identificazione all'interno del sistema documentale:

- amministrazione titolare del procedimento;
- altre amministrazioni partecipanti;
- nominativo del responsabile del procedimento;
- oggetto del fascicolo;
- elenco dei documenti contenuti;
- indice di classificazione (titolo, classe, etc.);
- numero del fascicolo, identificativo di una catena numerica relativamente alla classe e al titolo di riferimento dell'anno di creazione;
- data di apertura e di chiusura del fascicolo.

1. I fascicoli possono essere organizzati in sottofascicoli e inserti, i quali sono numerati progressivamente nell'ambito delle unità archivistiche che li contengono.
2. Il fascicolo contiene i documenti relativi ad un procedimento
3. Ad ogni fascicolo, può essere assegnato un livello di riservatezza. È possibile che un utente abbia accesso ad un fascicolo ma non possa vedere tutti i documenti in esso contenuti perché ad alcuni di essi è stato

attribuito un livello riservatezza superiore a quello assegnato al fascicolo.

Art. 41 Fascicoli ibridi o misti

Nel caso di fascicoli ibridi o misti, contenenti documenti formati su supporti diversi (digitale e analogico), la camicia cartacea per la conservazione esclusiva degli originali cartacei deve riportare la classifica e il numero del fascicolo digitale. Tale attività sarà svolta dall'UOR di riferimento.

Il fascicolo ibrido è composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un affare o procedimento amministrativo che dà origine a due unità archivistiche di conservazione differenti; l'unitarietà del fascicolo è garantita dall'indicazione della classe e del numero di fascicolo sul documento oppure sul fascicolo. Tale attività sarà svolta dall'UOR di riferimento. La gestione in ingresso dei documenti analogici è disciplinata seguendo le procedure indicate precedentemente riguardo alla gestione dei documenti analogici; l'ufficio protocollo, pertanto, si occuperà della riproduzione digitale dei documenti che sarà inserita nel protocollo solo dopo aver concluso l'attività di protocollazione e classifica e di apposizione dell'etichetta con barcode prodotta dal gestionale.

L'attività di protocollazione prevederà, inoltre, l'annotazione "Documento analogico" nel sistema di Gestione documentale per i documenti analogici in entrata e in uscita.

Art. 42 Tenuta degli archivi correnti, dei fascicoli e delle serie documentarie

I dirigenti sono responsabili della formazione e della tenuta degli archivi correnti dei rispettivi settori e adottano le procedure e gli strumenti stabiliti dal presente Manuale e dal Regolamento generale del Servizio Archivio del Comune.

Ai funzionari, o a loro delegato, spetta la responsabilità della formazione e della tenuta dei fascicoli e dei singoli documenti delle pratiche di loro competenza, fino al momento del loro versamento nell'Archivio di deposito, a chiusura del procedimento.

A conclusione del procedimento, la segreteria provvede alla chiusura del fascicolo all'interno del Sistema di gestione informatica dei documenti, modificandone lo stato, da "aperto" (archivio corrente) a "chiuso" (archivio di deposito). I fascicoli rimangono consultabili all'interno del Sistema di gestione informatica dei documenti.

La chiusura del fascicolo prelude al suo versamento all'Archivio di deposito che, di norma, avviene a distanza di cinque anni dalla chiusura della pratica.

PARTE V **SICUREZZA DEI SISTEMI E DEI DOCUMENTI INFORMATICI**

Art. 43 Misure di sicurezza nella formazione e gestione dei documenti

1. Il sistema di gestione informatica dei documenti dell'Amministrazione è attivato su tutte le stazioni di lavoro delle UOR che compongono l'Area Organizzativa Omogenea.
2. Il controllo degli accessi è realizzato assegnando a ciascun utente le credenziali di identificazione (User ID e Password) la cui gestione in termini di sicurezza e riservatezza è garantita dal Responsabile del Servizio sistemi informativi dell'Amministrazione e che ne determinano all'interno dell'amministrazione la corrispondente autenticazione dell'utente al sistema.
3. Il sistema di protocollo informatico gestisce diversi tipi di accesso, dalla consultazione alla possibilità di eseguire tutte le operazioni inerenti alla gestione documentale.
4. Le abilitazioni all'accesso alle funzionalità del sistema di protocollo informatico sono attribuite agli utenti dal Responsabile della gestione documentale in base al loro ruolo, ai compiti assegnati e alla struttura di appartenenza.
5. Nell'allegato n. 3, per ciascun utente del sistema di protocollo informatico, sono riportati i dati identificativi e le abilitazioni concesse dal Responsabile della gestione documentale.

6. L'accesso per via telematica al sistema di gestione informatica dei documenti da parte di utenti esterni all'AOO è consentito solo con strumenti tecnologici che permettano l'autenticazione "forte" (*strong authentication*) dei soggetti richiedenti, rappresentati:

- dalla carta d'identità elettronica (CIE) o documento digitale unificato (DDU);
- dalla carta nazionale dei servizi (CNS);
- dall'identità digitale gestita nell'ambito dello SPID (Sistema pubblico per la gestione dell'identità digitale)

Le misure di sicurezza informatica sono di carattere tecnico ed organizzativo e hanno l'obiettivo di garantire l'integrità, la disponibilità e la riservatezza dei dati e delle informazioni trattate.

Art. 44 Misure tecniche di sicurezza informatica dei sistemi

- **Misure di sicurezza fisica:** controllo degli accessi ai luoghi fisici in cui sono custoditi dati e sistemi, accesso mediante badge opportunamente abilitato;
- **Misure di sicurezza logica:** sicurezza del canale di comunicazione (es. https), architettura applicativa multi-layer;
- **Sistemi di identity management e di sicurezza:** sistemi di gestione degli account aziendali centralizzati, sistemi antivirus e sistemi di patch management per il costante aggiornamento dei sistemi operativi e di tutte le componenti applicative;
- **Politiche di backup e recovery:** produzione di copie di backup dei dati e dei documenti con frequenza giornaliera. Simulazioni trimestrali di recupero dati e sistemi.
- **Sistemi e soluzioni applicative in modalità Cloud della PA.**

Art. 45 Misure di sicurezza del sistema informativo integrato di gestione documentale

Il Sistema informativo integrato di gestione documentale rispetta le disposizioni in materia di sicurezza informatica stabilite dalla normativa vigente e le disposizioni in materia di protezione dei dati personali.

In particolare garantisce:

- l'univoca identificazione ed autenticazione degli utenti (credenziali utente con cambio password trimestrale);
- l'accesso alle sole risorse di competenza, sulla base di specifici profili abilitativi (rif. Allegato 3);
- il tracciamento permanente, su file di log, di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore;
- la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato;
- il reperimento delle informazioni riguardanti i documenti registrati;
- la formazione del registro giornaliero di protocollo e la sua trasmissione entro la giornata lavorativa successiva ai sistemi di conservazione documentale, a garanzia dell'integrità dello stesso.

Art. 46 Misure di sicurezza del sistema informativo integrato di gestione documentale

Le applicazioni utilizzate per la formazione dei documenti informatici gestiscono:

- l'identificabilità dell'Ente e del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi della normativa vigente;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati (sistemi informativi Gestionali);
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno dell'Ente, con altre AOO e con soggetti esterni.

I documenti informatici prodotti dall'Ente sono convertiti in formato pdf/A, prima della loro

sottoscrizione con firma digitale, al fine di garantire la leggibilità mediante altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento. Quando è prevista la sottoscrizione del documento amministrativo informatico, per attribuire in modo certo la titolarità del documento, la sua integrità, la sua riservatezza e la validazione temporale, il documento è sottoscritto con firma digitale.

Art. 47 Misure di sicurezza informatica di carattere organizzativo-gestione dei profili abilitativi

Sulla base delle richieste formali pervenute dai responsabili degli Uffici al Responsabile della Gestione documentale, mediante sistema informativo di gestione delle richieste di abilitazione agli applicativi, si procede all'assegnazione di un profilo abilitativo associato all'account indicato nella richiesta.

PARTE VI – GESTIONE DELL'ARCHIVIO DI DEPOSITO E STORICO

Art. 48 Archivio di deposito

L'Archivio di deposito conserva in forma temporanea i documenti dell'Ente relativi ad affari e procedimenti amministrativi conclusi nell'ultimo quarantennio. In questo arco temporale, si svolgono le periodiche operazioni di selezione dei materiali ai fini dello scarto degli atti inutili e della conservazione illimitata dei restanti documenti destinati all'Archivio storico.

All'interno dell'Archivio di deposito l'ordinamento delle serie trasferite avviene nel rispetto del principio dell'ordine originario e dell'organizzazione assunta da fascicoli e serie all'interno dell'Archivio corrente.

Art. 49 Trasferimento dei documenti all'Archivio di deposito (fascicoli analogici o ibridi)

Il Responsabile della gestione documentale opera affinché sia garantita regolare periodicità nel trasferimento, dagli archivi correnti dei servizi all'Archivio di deposito, di fascicoli riconducibili a pratiche concluse, non più necessarie allo svolgimento delle attività correnti. La disposizione di versamento, che sancisce il passaggio di responsabilità sulle unità archivistiche versate, avviene in collaborazione con il dirigente responsabile.

Le liste di versamento vengono predisposte anche nel caso di versamento di atti destinati allo scarto.

In preparazione del trasferimento, il responsabile d'ufficio esegue lo scarto di duplicati, appunti, buste e documenti non protocollati giudicati superflui, e controlla che il fascicolo contenga tutti i documenti protocollati che lo compongono, evidenziando le eventuali lacune sulla stampa dell'elenco dei documenti, da inserire all'interno del fascicolo.

Sulla base di valutazioni di natura logistica, il Responsabile della gestione documentale individua la più idonea dislocazione dei materiali destinati all'incameramento.

Art. 50. Sistema di conservazione dei documenti informatici

Il Comune di Casalgrande, per la conservazione dei documenti informatici e degli altri oggetti della conservazione, si avvale di un conservatore esterno ai sensi dell'art. 44, comma 1-quater, CAD.

Il servizio di conservazione dei documenti informatici dell'ente è stato affidato al Conservatore PARER (Servizio Polo Archivistico Regionale dell'Emilia-Romagna, d'ora in avanti anche solo "Conservatore").

Le attività affidate al Conservatore sono puntualmente indicate nella convenzione per l'affidamento del servizio.

Per la descrizione delle attività del processo di conservazione non definite nel presente Manuale, così come consentito dal par. 4.6 delle Linee Guida, è fatto rinvio al **Manuale di conservazione del Polo Archivistico Regionale - ParER (Allegato 6)**, nonché agli ulteriori documenti tecnici concernenti l'affidamento del servizio di conservazione (**allegato 7 – Schema di convenzione per lo svolgimento della funzione di conservazione dei documenti informatici**).

Art. 51. Responsabile della conservazione

Il Comune di Casalgrande ha designato un unico soggetto che riveste i ruoli di Responsabile della gestione documentale e Responsabile della conservazione.

È compito del Responsabile assicurare il rispetto della normativa vigente da parte del Conservatore e degli obblighi contrattuali dallo stesso assunti, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile agisce d'intesa con il RPD dell'ente.

Il Responsabile, ferma restando la propria responsabilità, può delegare in tutto o in parte una o più attività di propria competenza relative alla conservazione, affidandole a soggetti interni all'ente dotati di adeguate competenze. Gli atti di delega devono individuare le specifiche attività e funzioni delegate.

Art. 52. Oggetti della conservazione

Gli oggetti della conservazione sono:

- i documenti informatici formati dal Comune e i rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- i fascicoli informatici e rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- il registro del protocollo informatico;
- gli altri registri e repertori tenuti dall'ente.

Gli oggetti della conservazione sono trattati dal sistema di conservazione del Conservatore in pacchetti informativi che si distinguono in:

- a) pacchetti di versamento;
- b) pacchetti di archiviazione;
- c) pacchetti di distribuzione.

Il Responsabile provvede ad associare a ogni pacchetto di versamento almeno i seguenti metadati:

1. identificativo univoco e persistente del pacchetto di versamento;
2. riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
3. denominazione del soggetto responsabile della produzione del pacchetto;
4. impronta del pacchetto di versamento;
5. numero dei documenti compresi nel pacchetto.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie documentarie oggetto del servizio di conservazione sono dettagliatamente individuate nel Disciplinare tecnico per lo svolgimento della funzione di conservazione dei documenti informatici sottoscritto dal Comune unitamente alla convenzione di affidamento del servizio al Conservatore PARER.

Art. 53. Formati ammessi per la conservazione

I formati ammessi per la conservazione sono individuati nell'allegato 2 alle Linee guida dell'AgID. Il Responsabile, prima del versamento in conservazione, valuta i casi in cui è opportuno procedere al riversamento del documento in diverso formato, purché conforme ai formati indicati adatti alla

conservazione nell'allegato 2 alle Linee guida. In tal caso, la corrispondenza fra il formato originale e quello di riversamento è garantita dal Responsabile attraverso attestazione di conformità rilasciata secondo le modalità indicate nella Parte Seconda del presente Manuale.

Art. 54 Modalità e tempi di trasmissione dei pacchetti di versamento

All'inizio di ogni anno ciascuna UOR individua i fascicoli da versare all'archivio di deposito, dandone comunicazione al Responsabile, che provvede alla formazione e alla trasmissione dei pacchetti di versamento, secondo le modalità operative definite nel manuale del Conservatore e nei documenti tecnici sull'affidamento del servizio.

Il Responsabile genera il rapporto di versamento relativo a uno o più pacchetti di versamento e una o più impronte relative all'intero contenuto del pacchetto, secondo le modalità descritte nel manuale del Conservatore.

Prima del versamento in conservazione, il Responsabile verifica che agli oggetti della conservazione siano stati correttamente associati i rispettivi metadati e, se mancanti, richiede al produttore dell'oggetto di provvedere correttamente all'associazione dei metadati.

Il versamento dei documenti avviene secondo le seguenti tempistiche:

- versamento annuale, per cui ogni anno entro il mese di febbraio sono versati in conservazione tutti i documenti informatici dell'Unione, anche a fascicolo aperto;
- versamento automatizzato a determinate scadenze, che per il registro di protocollo giornaliero avviene entro le 24 ore successive al momento della produzione. Il Responsabile può individuare altre tipologie di versamento automatizzato a determinate scadenze per particolari tipologie di documenti;
- versamento anticipato, nelle particolari ipotesi che richiedono un versamento in conservazione prima del versamento a cadenza annuale (ad esempio, documenti con certificato di firma in scadenza).

Art. 55. Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica

I dati e i documenti informatici trattati dal Sistema di gestione documentale, vengono archiviati su server cloud qualificato dall'AgID ai sensi della normativa vigente.

La documentazione temporanea e di servizio formata negli anni precedenti alla pubblicazione del presente manuale (che si intende fascicolare e metadattare) viene conservata nel data center dell'Unione Tresinaro Secchia, a cui il Comune ha trasferito la funzione IT.

Le procedure di memorizzazione sono le seguenti:

- a) il salvataggio contestuale all'operatività avviene sui server di rete che ospitano il software di gestione documentale
- b) a cura del Servizio Sistemi Informativi dell'Unione Tresinaro Secchia vengono effettuate copie di backup, con periodicità minima giornaliera, della memoria dell'Amministrazione, riversate a loro volta su supporti di memorizzazione tecnologicamente avanzati e conservati nel Data Center adibito a Disaster Recovery.

Art. 56 Accesso al Sistema di conservazione

Gli utenti espressamente autorizzati dal Responsabile possono accedere al Sistema tramite credenziali personali rilasciate dal Conservatore e comunicate al singolo utente. L'accesso al Sistema consente di consultare i documenti digitali versati nel Sistema e le configurazioni specifiche adottate.

Art. 57. Selezione e scarto dei documenti

Periodicamente, secondo quanto previsto nel **Massimario di selezione e scarto** (v. **Allegato 12**) viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale, con eventuale invio di proposta alla competente Soprintendenza Archivistica. Le modalità per effettuare le operazioni di selezione e scarto dei documenti informatici sono descritte nel Massimario di selezione e scarto.

Art. 58. Misure di sicurezza e monitoraggio dei documenti digitali

Il Manuale di Conservazione e il Piano della sicurezza del Conservatore descrivono le modalità con cui il fornitore del servizio assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i *backup* degli archivi e il *Disaster recovery*.

Il Conservatore provvede altresì al periodico monitoraggio al fine di verificare lo stato delle componenti infrastrutturali del sistema e l'integrità degli archivi.

Il Responsabile vigila affinché il Conservatore provveda alla conservazione integrata dei documenti, dei fascicoli e dei metadati associati nelle fasi di gestione e di conservazione. A tal fine, con cadenza almeno annuale, richiede al Conservatore l'esibizione di un campione di documenti o fascicoli.

Nel caso siano riscontrate irregolarità, provvede a sollecitare il Conservatore affinché vi ponga rimedio, anche attraverso gli strumenti contrattuali previsti negli atti di affidamento del servizio.

GLOSSARIO DEI TERMINI E DEGLI ACRONIMI

TERMINE	DEFINIZIONE
Accesso	Operazione che consente di accedere al Sistema di gestione informatica dei documenti, con declinazioni abilitative diverse, a seconda del ruolo operativo

Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche
Area Organizzativa Omogenea	Insieme di funzioni e uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel
TERMINE	DEFINIZIONE
	momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi
Classificazione	Attività di organizzazione di tutti i documenti del soggetto produttore, secondo uno schema costituito da un insieme di voci articolate in modo gerarchico, che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore

Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Destinatario	Soggetto o sistema al quale il documento è indirizzato
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Esibizione	Operazione che consente di visualizzare un documento conservato
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di bit che può essere elaborata da una procedura informatica
TERMINE	DEFINIZIONE
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS

Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti
hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "digest"
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione
TERMINE	DEFINIZIONE
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi

Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture
Manuale di gestione documentale	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi
Metadati	Dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con
TERMINE	DEFINIZIONE
	le modalità riportate nel manuale di conservazione
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso

Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi
Piano della sicurezza del sistema di gestione Informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Presa in carico	Accettazione da parte dell'unità organizzativa o del
TERMINE	DEFINIZIONE
	singolo componente della stessa di un documento ricevuto in smistamento/assegnazione tramite scrivania virtuale
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita
Produttore dei PdV	Persona fisica, diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.
Protocollo Informatico	Componente software del sistema di "Sistema di Gestione Informatica dei Documenti" che assicura la gestione contemporanea della registrazione di protocollo e segnatura di protocollo.

Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del Sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare
Regolamento eIDAS	electronic IDentificationAuthentication and Signature, Regolamento (UE) No 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
Repertorio	Registro su cui vengono annotati con un numero progressivo specifiche tipologie documentarie (es. contratti, ordinanze, delibere, ecc.) o fascicoli, secondo l'ordine cronologico in cui vengono creati
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del Sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia
Responsabile della gestione documentale	Soggetto responsabile della gestione del Sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e
TERMINE	DEFINIZIONE
	delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC)
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione

Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica)
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
TERMINE	DEFINIZIONE
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti.

ALLEGATI

N. 1 – Aree Organizzative Omogenee

a) i dati identificativi dell'Amministrazione

Codice identificativo dell'AOO	C_b893
Nome esteso dell'AOO	Comune di Casalgrande
Nome referente	Jessica
Cognome referente	Curti

b) i dati identificativi di ogni AOO istituita

Codice identificativo dell'AOO	C_b893
Nome esteso dell'AOO	Comune di Casalgrande
Indirizzo di posta elettronica certificata istituzionale	casalgrande@cert.provincia.re.it
Nome del Responsabile	Jessica
Cognome del Responsabile	Curti
Data istituzione	13/02/2018
Numero "n" uffici afferenti	4

c) i dati identificativi del Servizio attivato in ogni AOO

Codice ufficio	UFXUVJ
Denominazione	Ufficio fatturazione
Codice dell'AOO di appartenenza	C_b893
Nome del Responsabile della gestione documentale	Jessica
Cognome del Responsabile della gestione documentale	Curti
Vicario del Responsabile della gestione documentale	ATTO DI NOMINA ATTRAVERSO DECRETO SINDACALE

Codice ufficio	C54W8J
Denominazione	Servizi demografici ed elettorale
Codice dell'AOO di appartenenza	C_b893
Nome del Responsabile della gestione documentale	Jessica
Cognome del Responsabile della gestione documentale	Curti
Vicario del Responsabile della gestione documentale	ATTO DI NOMINA ATTRAVERSO DECRETO SINDACALE

Codice ufficio	40EK0B
Denominazione	SUAP- sportello unico attivita' produttive- commercio - manifestazione
Codice dell' AOO di appartenenza	C_b893
Nome del Responsabile della gestione documentale	Jessica
Cognome del Responsabile della gestione documentale	Curti
Vicario del Responsabile della gestione documentale	ATTO DI NOMINA ATTRAVERSO DECRETO SINDACALE

Codice ufficio	HYUKDK
Denominazione	Ufficio per la transizione digitale
Codice dell' AOO di appartenenza	C_b893
Nome del Responsabile della gestione documentale	Jessica
Cognome del Responsabile della gestione documentale	Curti
Vicario del Responsabile della gestione documentale	ATTO DI NOMINA ATTRAVERSO DECRETO SINDACALE

d) i dati identificativi delle unità organizzative che compongono ciascuna AOO con la loro articolazione gerarchica

Codice ufficio	UFXUVJ
Denominazione	Uff efatturaPA
Codice dell' AOO di appartenenza	C_b893
ndirizzo di posta elettronica certificata dichiarata (eventuale)	Fatture.casalgrande@cert.provincia.re.it
Nome del Responsabile dell'ufficio	Alessandra
Cognome del Responsabile dell'ufficio	Gherardi



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

SETTORE AFFARI GENERALI
SEGRETERIA

DECRETO SINDACALE N. 18 / 2022

OGGETTO: CONFERIMENTO DELL'INCARICO DI POSIZIONE ORGANIZZATIVA DEL SETTORE "AFFARI GENERALI", NONCHE' DELLE FUNZIONI DI VICE SEGRETARIO GENERALE

IL SINDACO

Premesso che:

- il CCNL comparto Regioni – Autonomie Locali prevede la possibilità di istituzione dell'area delle posizioni organizzative che viene a collocarsi in posizione intermedia tra le altre aree generali e la dirigenza;
- il Comune di Casalgrande è privo di posizioni dirigenziali e la responsabilità di uffici e servizi può essere attribuita a dipendenti di categoria D, ai sensi dell'art. 13, comma 2, del CCNL del 21 maggio 2018;
- il vigente Regolamento di organizzazione degli uffici e dei servizi, approvato con deliberazione della Giunta dell'Unione Tresinaro Secchia n. 64 del 23.11.2021 disciplina la struttura organizzativa dei Comuni facenti parte dell'Unione, articolata in settori, oltre agli uffici di staff, e ha stabilito le modalità ed i criteri per il conferimento dell'incarico di responsabile (art. 4);
- con delibera di Giunta Comunale n. 108 del 30 agosto 2018 è stata ridefinita la macrostruttura organizzativa dell'ente, aggiornata con successive delibere di Giunta Comunale n. 128 del 25.09.2020 e n. 77 del 09.06.2022;

Dato atto che, in seguito alle suddette modifiche, i nuovi settori organizzativi dell'ente, con i relativi servizi sono:

- Settore Affari generali (affari legali e assicurativi, segreteria e notifiche, urp e comunicazione, segreteria sindaco, protocollo e archivio, addetto stampa, sviluppo smart city e digital transformation, politiche comunitarie);
- Settore Finanziario (programmazione e supporto al controllo di gestione, ragioneria, economato);
- Settore Pianificazione territoriale (urbanistica, edilizia, ambiente);
- Settore Attività Produttive (suap, commercio);



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

-
- Settore Lavori pubblici (lavori pubblici, patrimonio);
 - Settore vita della comunità (sport, manifestazioni, volontariato, cultura, biblioteca);
 - Settore Servizi scolastici ed educativi (servizi scolastici, servizi educativi);
 - Settore entrate (tributi)
 - Settore servizi demografici ed elettorale(anagrafe, stato civile, elettorale);

Dato atto che il CCNL comparto Funzioni Locali triennio 2016/2018 stipulato in data 21/05/2018 ha ridefinito la disciplina dell'Area delle Posizioni Organizzative;

Evidenziato, in particolare,

- l'art.14, comma 1, il quale stabilisce che *“Gli incarichi relativi all'area delle posizioni organizzative sono conferite dai dirigenti (dal Sindaco negli enti privi di dirigenza) per un periodo massimo non superiore a tre anni, previa determinazione di criteri generali da parte degli enti, con atto scritto e motivato, e possono essere rinnovati con le medesime formalità”*;
- l'art.13, comma 3, il quale prevede che *“Gli incarichi di posizione organizzativa di cui all'art.8 del CCNL del 31/03/1999 e dell'art.10 del CCNL del 22/01/2004, già conferiti e ancora in atto, proseguono o possono essere prorogati fino alla definizione del nuovo assetto delle posizioni organizzative, successivo alla determinazione delle procedure e dei relativi criteri generali previsti dal comma 1 dell'art.14 e, comunque, non oltre un anno dalla data di sottoscrizione del presente CCNL”* (cfr. 20 maggio 2019);

Richiamata la delibera di giunta n. 58 del 2 maggio 2019, mediante la quale veniva modificato il regolamento sull'ordinamento degli uffici e dei servizi, nonché l'allegato recante la metodologia per la pesatura delle posizioni organizzative, tuttora in vigore, in conformità di quanto previsto dal CCNL del 21 maggio 2018;

Preso atto che:

- il decreto n. 11 dell 30.09.2021 di attribuzione dell'incarico di posizione organizzativa per il settore “Affari generali” giunge a scadenza in data 30 settembre 2022;
- è necessario quindi procedere ad una nuova attribuzione dell'incarico di posizione organizzativa per il settore “Affari generali”;

Richiamato il vigente “Regolamento di organizzazione degli uffici e dei servizi”, ed in particolare: l'art. 22 che disciplina il conferimento dell'incarico a dirigenti/responsabili di settore, come sotto riportato:

“1.1 Dirigenti/Responsabili di Settore sono nominati dal Sindaco/Presidente, con proprio provvedimento, secondo criteri di professionalità ed in base alle potenzialità professionali accertate.



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

2. L'incarico di direzione può essere conferito anche a soggetti esterni, con contratto a tempo determinato, ai sensi dell'articolo successivo oppure attivando apposite convenzioni tra Enti.

3. L'individuazione del Dirigente/Responsabile cui attribuire le funzioni di direzione tiene conto, in particolare, dei seguenti elementi:

- a) natura e caratteristiche dei programmi ed obiettivi da realizzare
- b) attitudini, conoscenze e delle capacità professionali;
- c) dei risultati conseguiti in precedenza presso l'Ente e della relativa valutazione in coerenza con il d.lgs. 150/2009;
- d) delle specifiche competenze organizzative possedute, nonché delle esperienze di direzione eventualmente maturate all'estero, presso il settore privato o presso altre amministrazioni pubbliche, purché attinenti all'incarico da conferire.

4. Gli incarichi di direzione hanno una durata non superiore alla scadenza del mandato elettivo del Sindaco o dei Comuni che rappresentano la maggior parte della popolazione dell'Unione.

5. Il Sindaco neo-eletto può riattribuire provvisoriamente gli incarichi ai medesimi soggetti che già erano titolari allo scadere del mandato amministrativo precedente per un periodo non superiore a 90 giorni, eventualmente prorogabile per il tempo strettamente necessario alla individuazione del nuovo Responsabile.

6. Gli incarichi di direzione nei settori a più elevato rischio di corruzione individuati nel PTPCT, hanno di norma durata non superiore a tre anni; gli stessi sono attribuiti a rotazione ai dipendenti in possesso dei necessari requisiti professionali e in modo da salvaguardare la continuità della gestione amministrativa; il PTPCT dà conto delle eventuali condizioni organizzative che non consentono tale rotazione, dandone adeguata motivazione.

7. Gli incarichi sono rinnovabili con provvedimento espresso.

8. Nell'Ente privo di dirigenti, in relazione alle specifiche esigenze organizzative derivanti dall'ordinamento vigente, sono individuate, se necessario ed anche in via temporanea, le posizioni organizzative che possono essere conferite anche a personale con rapporto di lavoro a tempo parziale di durata non inferiore al 50% del rapporto a tempo pieno. Il principio di riproporzionamento del trattamento economico trova applicazione anche in riferimento alla retribuzione di posizione.

Unione Tresinaro Secchia Regolamento di organizzazione degli uffici e dei servizi

9. In applicazione dell'art. 53 comma 23 della Legge n. 388/2000, in caso di Ente con popolazione inferiore ai 5.000 abitanti, il Sindaco può attribuire la responsabilità degli uffici e dei servizi ed il potere di adottare gli atti di natura tecnica gestionale ai componenti dell'organo esecutivo, fatta salva la possibilità di assumere lui stesso l'incarico."

Richiamato, altresì l'art. 14 comma 5 del Regolamento sopracitato che disciplina come sotto riportato la nomina del vicesegretario: " Il Sindaco/Presidente dell'Unione nomina - tra i dirigenti/funzionari dell'Ente o ricorrendo a forme di collaborazione fra Enti - il Vice Segretario che coadiuva il Segretario nell'esercizio delle sue funzioni e lo sostituisce in caso di vacanza, assenza o impedimento, nei modi e nei termini previsti dalla legge. Il Vice Segretario deve essere in possesso dei requisiti previsti per l'accesso al ruolo di Segretario comunale";



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

Visto altresì l'art. 97, comma 5, del decreto legislativo n. 267/2000, ai sensi del quale: *“il regolamento sull'ordinamento degli uffici e dei servizi può prevedere un vicesegretario per coadiuvare il segretario e sostituirlo nei casi di vacanza, assenza o impedimento”*;

Richiamato, altresì, la circolare dell'Agenzia Autonoma dei segretari provinciali e comunali del 22 gennaio 2008, secondo la quale i requisiti necessari per ricoprire la figura di vice segretario devono essere analoghi a quelli per accedere al concorso pubblico per segretari;

Dato atto, che per garantire la buona funzionalità dell'Ente e la continuità dell'operatività degli uffici, è necessario provvedere al conferimento della titolarità della posizione organizzativa sopra richiamata in conformità della nuova disciplina dettata dall'art. 13 del CCNL del 21.05.2018, nonché all'individuazione della figura del vice segretario che sostituisca il segretario generale in carica, in caso di assenza o impedimento, nell'assolvimento dei compiti istituzionali ad esso riservati, attenendosi alle direttive impartite dal Sindaco e dal Segretario stesso;

Considerato che la dipendente Jessica Curti, appartenente alla categoria giuridica D:

- risulta in possesso dei titoli di studio, delle attitudini e capacità gestionali necessarie per lo svolgimento delle funzioni di responsabile del settore in oggetto;
- ha conseguito gli obiettivi in precedenza assegnati, come si evince dalle valutazioni conseguite nell'ultimo triennio;

Considerato, altresì, che la dipendente Jessica Curti risulta in possesso di laurea magistrale in Giurisprudenza, nonché di abilitazione all'esercizio della professione forense, ed è quindi idonea, per specializzazione e funzione, a ricoprire il ruolo di “vice-segretario”;

Richiamato il verbale sottoscritto dal segretario e dal sindaco, prot. n. 9421 del 16 maggio 2019, da cui risulta la pesatura delle posizioni organizzative, nonché il rispetto dei limiti del trattamento accessorio previsto dall'art. 23, comma 2, del D.Lgs. 75/2017;

Ritenuto quindi, di procedere al conferimento dell'incarico di posizione organizzativa del settore “Affari generali”, nonché all'attribuzione delle funzioni di vice segretario generale alla dipendente Jessica Curti a far data dal 1° ottobre 2022 fino al 30 settembre 2023;

Sentito il Vice Segretario Generale ed in armonia con quanto disposto dalla Giunta Comunale in merito all'organizzazione dell'ente;

decreta



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

1. di incaricare Jessica Curti, dipendente di cat. D, responsabile del Settore "Affari generali", nonchè vice segretario generale, dal 1° ottobre 2022 fino al 30 settembre 2023;
2. di attribuire alla medesima la retribuzione di posizione pari ad € 11.620,18 e la retribuzione di risultato massima pari al 25% della retribuzione di posizione, assorbente le competenze accessorie previste da CCNL, ivi compreso il compenso per lavoro straordinario, determinata come indicato nel verbale sottoscritto dal sindaco e dal segretario prot. n. 9421 del 16 maggio 2019;
3. di dare atto che il presente decreto produrrà il proprio effetto con decorrenza dal 1° ottobre 2022;
4. di ottemperare all'obbligo imposto dal D.Lgs. n. 33/2013, art.23 , disponendo la pubblicazione del presente atto sul sito istituzionale del Comune di Casalgrande nella sezione "Amministrazione trasparente".

Il presente provvedimento deve essere notificato alla dipendente Jessica Curti trasmesso in copia all'ufficio risorse umane per l'inserimento nel fascicolo personale della dipendente interessata.

Lì, 29/09/2022

IL SINDACO
DAVIDDI GIUSEPPE

(Sottoscritto digitalmente ai sensi
dell'art. 21 D.Lgs n 82/2005 e s.m.i.)

Ruolo	Funzioni
Sindaco / Vicesindaco	Vede tutti i documenti, senza alcuna eccezione, presenti nel sistema e può protocollare in uscita
Protocollatore Centrale	Vede tutti i documenti presenti nel sistema, senza alcuna eccezione. Protocollare in uscita e in Ingresso, smista e/o assegna alle unità organizzative. Può annullare protocolli.
Responsabile Area	Gestisce tutti i documenti, compresi i riservati, smistati alla sua area di appartenenza e può protocollare in uscita. Approva o respinge determine di settore e ordinanze dirigenziali. Propone Delibere di Giunta e/o Consiglio Comunale
Operatore riservato	Gestisce tutti i documenti, compresi i riservati, smistati alla sua area di appartenenza e può protocollare in uscita. Propone le Determine e le Ordinanze dirigenziali
Operatore Base	Gestisce tutti i documenti, ad esclusione dei riservati, smistati alla sua area di appartenenza e può protocollare in uscita. Propone le Determine e le Ordinanze dirigenziali



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

TITOLARIO IN VIGORE DAL 01/01/2016

I	Amministrazione generale 1. Legislazione e circolari esplicative 2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica 3. Statuto 4. Regolamenti 5. Stemma, gonfalone, sigillo 6. Archivio generale 7. Sistema informativo 8. Informazioni e relazioni con il pubblico 9. Politica del personale; ordinamento degli uffici e dei servizi 10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale 11. Controlli interni ed esterni 12. Editoria e attività informativo-promozionale interna ed esterna 13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti 14. Interventi di carattere politico e umanitario; rapporti istituzionali 15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni 16. Area e città metropolitana 17. Associazionismo e partecipazione
II	Organi di governo, gestione, controllo, consulenza e garanzia 1. Sindaco 2. Vice-Sindaco 3. Consiglio 4. Presidente del Consiglio 5. Conferenza dei capigruppo e Commissioni del Consiglio 6. Gruppi consiliari 7. Giunta 8. Commissario prefettizio e straordinario 9. Segretario e Vice-segretario 10. Direttore generale e dirigenza 11. Revisori dei conti 12. Difensore civico 13. Commissario ad acta 14. Organi di controllo interni 15. Organi consultivi
III	Risorse umane 1. Concorsi, selezioni, colloqui 2. Assunzioni e cessazioni 3. Comandi e distacchi; mobilità 4. Attribuzione di funzioni, ordini di servizio e missioni 5. Inquadramenti e applicazione contratti collettivi di lavoro 6. Retribuzioni e compensi 7. Trattamento fiscale, contributivo e assicurativo 8. Tutela della salute e sicurezza sul luogo di lavoro 9. Dichiarazioni di infermità ed equo indennizzo 10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza 11. Servizi al personale su richiesta 12. Orario di lavoro, presenze e assenze 13. Giudizi, responsabilità e provvedimenti disciplinari 14. Formazione e aggiornamento professionale 15. Collaboratori esterni

IV	Risorse finanziarie e patrimonio 1. Bilancio preventivo e Piano esecutivo di gestione (PEG) 2. Gestione del bilancio e del PEG (con eventuali variazioni) 3. Gestione delle entrate: accertamento, riscossione, versamento 4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento 5. Partecipazioni finanziarie 6. Rendiconto della gestione; adempimenti e verifiche contabili 7. Adempimenti fiscali, contributivi e assicurativi 8. Beni immobili 9. Beni mobili 10. Economato 11. Oggetti smarriti e recuperati 12. Tesoreria 13. Concessionari ed altri incaricati della riscossione delle entrate 14. Pubblicità e pubbliche affissioni
V	Affari legali 1. Contenzioso 2. Responsabilità civile e patrimoniale verso terzi; assicurazioni 3. Pareri e consulenze
VI	Pianificazione e gestione del territorio 1. Urbanistica: piano regolatore generale e varianti 2. Urbanistica: strumenti di attuazione del piano regolatore generale 3. Edilizia privata 1. Certificato di conformità edilizia e agibilità (CCEA) 2. Richiesta generica edilizia 3. Comunicazione inizio lavori (CIL) 4. Permesso a costruire 5. Segnalazione certificata inizio attività (SCIA) 4. Edilizia pubblica 5. Opere pubbliche 6. Catasto 7. Viabilità 8 Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi 9. Ambiente: autorizzazioni, monitoraggio e controllo 10. Protezione civile ed emergenze
VII	Servizi alla persona 1. Diritto allo studio e servizi 2. Asili nido e scuola materna 3. Promozione e sostegno delle istituzioni di istruzione e della loro attività 4. Orientamento professionale; educazione degli adulti; mediazione culturale 5. Istituti culturali (Musei, Biblioteche, Teatri, Scuola comunale di musica, etc.) 6. Attività ed eventi culturali 7. Attività ed eventi sportivi 8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale 9. Prevenzione, recupero e reintegrazione dei soggetti a rischio 10. Informazione, consulenza ed educazione civica 11. Tutela e curatela di incapaci 12. Assistenza diretta e indiretta, benefici economici 13. Attività ricreativa e di socializzazione 14. Politiche per la casa 15. Politiche per il sociale
VIII	Attività economiche 1. Agricoltura e pesca 2. Artigianato 3. Industria 4. Commercio 5. Fiere e mercati 6. Esercizi turistici e strutture ricettive 7. Promozione e servizi
IX	Polizia locale e sicurezza pubblica 1. Prevenzione ed educazione stradale

	2. Polizia stradale 3. Informative 4. Sicurezza e ordine pubblico
X	Tutela della salute 1. Salute e igiene pubblica 2. Trattamento Sanitario Obbligatorio 3. Farmacie 4. Zooprofilassi veterinaria 5. Randagismo animale e ricoveri
XI	Servizi demografici 1. Stato civile 2. Anagrafe e certificazioni 3. Censimenti 4. Polizia mortuaria e cimiteri
XII	Elezioni ed iniziative popolari 1. Albi elettorali 2. Liste elettorali 3. Elezioni 4. Referendum 5. Istanze, petizioni e iniziative popolari
XIII	Affari militari 1. Leva e servizio civile sostitutivo 2. Ruoli matricolari 3. Caserme, alloggi e servitù militari 4. Requisizioni per utilità militari
XIV	Oggetti diversi



Affari Generali

Prisma - Gestione Protocollo Informatico

Manuale Utente – release 4.0.0

Indice

1 Area di Lavoro: Scrivania Virtuale e Sistema Documentale	4
1.1 Scrivania Virtuale	4
1.2 Sistema Documentale e caratteristiche di accesso	5
1.2.1 Sistema di autorizzazione: ruoli e privilegi.....	5
1.2.2 Area di Lavoro	6
2 Creazione ed inserimento di nuovi documenti	8
2.1 Modalità di protocollazione dei documenti	8
2.1.1 Pulsanti Funzionali	9
2.1.2 Menu contestuali	10
2.1.3 Inserimento dei dati giuridici e archivistici	10
2.1.4 Inserimento di rapporti e gestione anagrafica.....	13
2.1.4.1 Ricerca soggetti in fase di protocollazione.....	13
2.1.4.2 Inserimento di un nuovo soggetto in fase di protocollazione	14
2.1.4.3 Modifica di un soggetto esistente in fase di protocollazione	15
2.1.4.4 Indicazione di destinatario "Per Conoscenza" sulle registrazioni di protocollo	16
2.1.5 Inserimento di smistamenti	17
2.1.6 Inserimento di allegati	19
2.1.7 Storico modifiche	20
2.1.8 Controlli in fase di protocollazione e menu "Funzionalità" in fase di creazione e protocollazione di documenti	21
2.1.9 Visualizzazione e inserimento dei riferimenti del documento	23
2.1.10 Inserimento Note al protocollo.....	23
2.2 Preferenze di applicazione.....	23
2.3 Creazione di un nuovo Fascicolo	26
2.3.1 Creazione di fascicoli dall'Area di Lavoro "Titolario"	29
2.3.2 Creazione di fascicoli dalla maschera di protocollazione.....	29
2.4 Firma di documenti principali da maschera di protocollo.....	30
2.4.1 Verifica della firma digitale e memorizzazione dell'esito	30
2.5 Gestione dei documenti non protocollati	30
2.5.1 Registrazione di "documenti da fascicolare"	30
2.6 Pubblicazione su Albo On Line dalle maschere dei documenti protocollati	32
3 Gestione delle Attività della Smart Desktop.....	33
3.1 Gestione di un singolo documento.....	33
3.2 Gestione multipla di documenti	34
3.3 Gestione dei documenti dal Sistema Documentale: "Iter Documentale"	35
3.4 Gestione degli smistamenti dei documenti non protocollati	37

4 Funzioni per la ricerca dei documenti	37
4.1 Stampa dei registri di protocollo generale e dei fascicoli.....	40
5 Classificazione dei documenti protocollati.....	40
5.1 Aggiunta di una Classificazione Secondaria.....	40
5.2 Modifica del dato di Classificazione	41
6 Invio di documenti protocollati tramite PEC.....	42
6.1 Invio convocazione gara – oscuramento destinatari	43
6.2 Multiselezione dei destinatari	43
6.3 Notifica su Smart Desktop in caso di mancato invio tramite PEC	44

1 Area di Lavoro: Scrivania Virtuale e Sistema Documentale

1.1 Scrivania Virtuale

L'accesso all'ambiente di lavoro è preceduto dalla richiesta di autenticazione dell'utente, che si realizza tramite l'inserimento di username e password (dati che vengono decisi e forniti dall'Amministrazione):

Smart*Desktop Scrivania Virtuale

Autenticazione

Utente:

Password:

Effettuato il login, si accede alla **"Smart Desktop"**. Tale ambiente di lavoro permette all'utente di visualizzare le attività che necessitano di un suo intervento specifico, con la possibilità di eseguire le varie operazioni legate ad esse, o di accedere ad applicazioni specifiche.

Questa la visione d'insieme della Smart Desktop:

Smart*Desktop

</

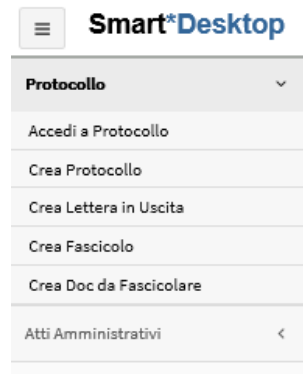
Nella parte centrale della scrivania è visualizzato l'elenco delle attività in attesa dell'intervento dell'utente; per ognuna di queste è presente un link che permette la sua gestione (cfr. Capitolo 3).

La barra "filtro ricerca" nella parte superiore permette di effettuare funzioni di ricerca all'interno delle attività presenti nella scrivania. La barra "filtro ricerca" nella parte superiore permette di effettuare funzioni di ricerca all'interno delle attività presenti nella scrivania.

Cerca

La funzione filtro  apre un menù a tendina con il quale si possono applicare dei filtri di ricerca al contenuto della scrivania virtuale (Tipologia o Tipologie di interesse, definire un intervallo di date delle attività.)

La funzione nella parte superiore  permette di aprire un menù a tendina dove verranno mostrati gli applicativi utilizzati dall'Ente con la possibilità, tramite apposita selezione, di accedere alle singole aree di lavoro per cui l'utente è abilitato.



1.2 Sistema Documentale e caratteristiche di accesso

Il Sistema Documentale è lo strumento che permette la gestione dei flussi documentali all'interno dell'Amministrazione. È appunto attraverso questo applicativo che si ha la possibilità di agire sui documenti in ogni momento: dalla creazione, alla gestione dell'iter, tracciando le modifiche apportate ai documenti stessi, in conformità con quanto previsto dalla normativa, fino alla definitiva archiviazione.

L'accesso degli utenti al Sistema Documentale è regolato in funzione delle competenze che caratterizzano gli operatori, basate principalmente sul *ruolo* e sull'Unità Organizzativa di appartenenza.

Ogni utente è stato, infatti, identificato come 'componente' di una o più Unità Organizzative dell'Amministrazione con un particolare *ruolo*: il ruolo di appartenenza stabilisce le funzionalità alle quali l'operatore ha accesso per la gestione dei documenti all'interno della propria unità di competenza. Questo implica che la visualizzazione delle varie parti del Sistema Documentale potrà essere diversa da utente a utente, in base al ruolo attribuitogli in fase di impostazione dell'applicativo.

1.2.1 Sistema di autorizzazione: ruoli e privilegi

Il sistema di profilazione utenti si basa sulla gestione di utenti, persone, ruoli e unità organizzative. Il componente lavora in base alle unità in cui un soggetto è inserito ed ai ruoli che gli sono associati definendo così le abilitazioni dell'utente. I ruoli applicativi in particolare rappresentano l'abilitazione alle funzionalità specifiche del sistema e sono attribuite al singolo componente per la/le unità di appartenenza, per l'identificazione delle competenze di inserimento, modifica e visualizzazione delle registrazioni. La politica di gestione delle abilitazioni avviene a due livelli: i ruoli, da associare agli utenti, ed i privilegi, tramite cui quali specializzare le operazioni di protocollazione, assegnazione, gestione della posta certificata, modifica dei documenti, visualizzazione dei documenti e gestione delle funzioni archivistiche (classificazione, fascicolazione).

Le discriminanti fondamentali da definire in termini di abilitazioni sono di seguito riassunte:

- ✓ Funzione: protocollatore (protocollazione e gestione), operatore (solo gestione), visualizzatore (solo visualizzazione).
- ✓ Estensione dei privilegi (è possibile anche combinare le estensioni fra loro): nessuna estensione (funzione legata soltanto alla propria unità di appartenenza), verso tutta la struttura di appartenenza, verso le unità di

pari livello dell'area di appartenenza, verso le unità di livello inferiore dell'area di appartenenza, verso le unità di livello superiore dell'area di appartenenza.

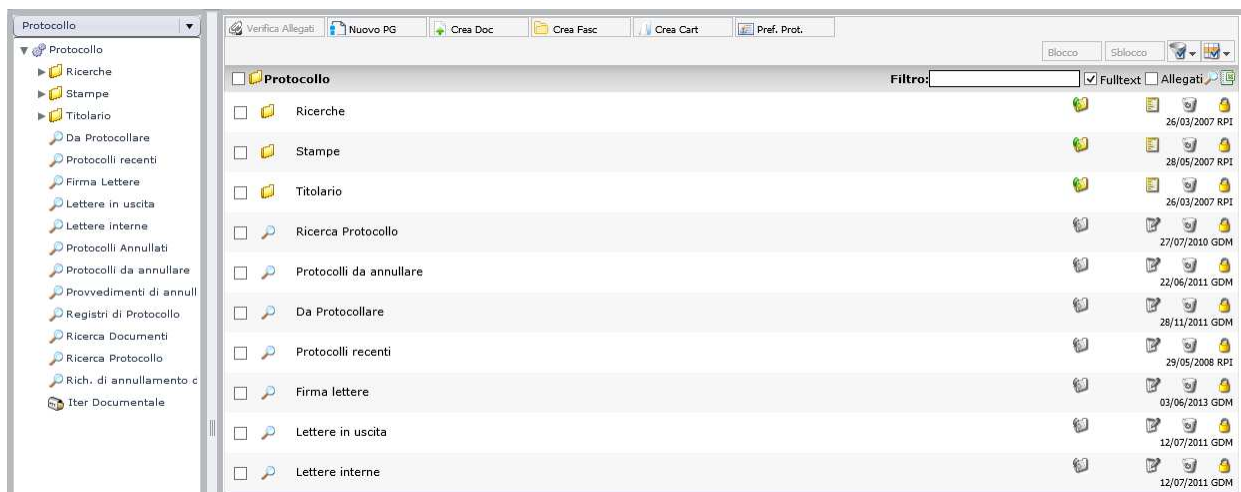
- ✓ Funzionalità estese: creazione dei fascicoli, possibilità di vedere/gestire i documenti riservati, politiche di assegnazione (es. l'utente può smistare a tutte le strutture dell'ente, alla sola area di appartenenza, l'utente non può assegnare, ecc.).

Questa situazione è però assolutamente adattabile alle necessità effettive dell'Ente: è possibile studiare e quindi creare dei ruoli ad hoc a seconda delle volontà legate alla politica di gestione ed assegnazione.

Il sistema di autorizzazione prevede inoltre la gestione delle deleghe, delle sostituzioni e dell'affiancamento; oltre alla gestione "preventiva" di queste casistiche con l'attribuzione delle relative abilitazioni ai soggetti competenti.

1.2.2 Area di Lavoro

Accedendo all'area di lavoro del Protocollo tramite il menu a tendina della Smart Desktop (come illustrato poco sopra), si avrà questa situazione:



L'area di lavoro del Sistema Documentale è divisibile in 3 parti: la finestra sulla sinistra (che presenta tipicamente strutture ad albero), il blocco di visualizzazione centrale, ed una serie di "bottoni" nella parte alta del blocco centrale.

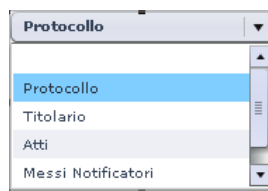
Nella parte di sinistra della finestra sono presenti delle cartelle e delle ricerche, più o meno pre-impostate (caratterizzate dall'icona della lente); la cartella "ricerche" presenta al suo interno una ulteriore serie di possibilità di ricerca (cfr. Capitolo 4).

Vi sono poi una serie di altre voci utili alla gestione dei documenti specifici dell'unità di appartenenza:

- **Documenti da protocollare:** documenti creati dal proprio utente a cui non è ancora stato attribuito il numero di protocollo.
- **Protocolli recenti:** elenca i documenti protocollati nell'ente negli ultimi tre giorni, per i quali l'utente ha i diritti di visualizzazione.

Altre voci possono essere presenti a seconda del ruolo assegnato all'utente o delle eventuali personalizzazioni effettuate su richiesta dell'Amministrazione.

Nella parte alta di questa finestra posta sulla sinistra del Sistema Documentale è presente un menu a tendina che permette l'accesso ad altre aree del Sistema Documentale, ad esempio:



Anche il numero delle voci presenti in questo menu dipende dagli applicativi installati dall'Amministrazione.

Tipicamente si avrà l'accesso all'area Titolario, dove sarà possibile visualizzare le cartelle e i relativi documenti contenuti all'interno del titolare stesso, secondo le impostazioni dettate dall'Amministrazione al momento dell'installazione dell'applicativo.

Sia che ci si trovi nell'area Protocollo, sia nell'area Titolario o in altre aree, il comportamento del Sistema Documentale è simile: cliccando su una voce nella finestra di sinistra, il risultato viene visualizzato nel blocco centrale della finestra.

Ad esempio, cliccando nella parte sinistra sulla voce "protocolli recenti", all'interno dell'area Protocollo:

Protocollo Generale - 2017 / 56 del 09/03/2017 17:38:09	Modalità:	Partenza	Destinatario		
Oggetto: PROGETTO SIS - COMUNICAZIONE ESITO VERBALE DI COLLAUDO			- GRUPPO FINMATICA FILIPPO.ANTONI@ACTALISCERTYMAIL.IT		17/03/2017 RPI
Classifica: 01-01 2016 / 1					
Stato Iter: INVIATO (26314)					
Protocollo Generale - 2017 / 57 del 10/03/2017 09:43:01	Modalità:	Partenza	Mittente/Destinatario		
Oggetto: CM VENEZIA - PRESENTAZIONE SISTEMA DI PROTOCOLLO MARZO 2017			- GRUPPO FINMATICA FILIPPO.ANTONI@ACTALISCERTYMAIL.IT		10/03/2017 NICOLA.RE
Classifica: 01-06 /					
Protocollo Generale - 2017 / 58 del 10/03/2017 09:44:16	Modalità:	Arrivo	Mittente/Destinatario		
Oggetto: CM VENEZIA - PRESENTAZIONE SISTEMA DI PROTOCOLLO MARZO 2017			- GRUPPO FINMATICA FILIPPO.ANTONI@ACTALISCERTYMAIL.IT		10/03/2017 NICOLA.RE
Classifica: 01-06 /					
Protocollo Generale - 2017 / 59 del 10/03/2017 11:02:18	Modalità:	Partenza	Destinatario		
Oggetto: CM VENEZIA - LETTERA USCITA 10 MARZO 2017			- GRUPPO FINMATICA FILIPPO.ANTONI@ACTALISCERTYMAIL.IT		17/03/2017 RPI
Classifica: 01-06 2016 / 3					
Stato Iter: INVIATO (26333)					
Protocollo Generale - 2017 / 60 del 13/03/2017 10:52:31	Modalità:	Arrivo	Mittente/Destinatario		
Oggetto: CONCORSO PUBBLICO			- COMUNE DI FIRENZE DRT_TEST@PEC.COMUNE.FI.IT		13/03/2017 ROBERTO.MONTANARI
Classifica: 01-01 /					
Protocollo Generale - 2017 / 61 del 13/03/2017 10:55:35	Modalità:	Arrivo	Mittente/Destinatario		
Oggetto: CONCORSO PUBBLICO CATEGORIA D			- COMUNE DI FIRENZE DRT_TEST@PEC.COMUNE.FI.IT		13/03/2017 ROBERTO.MONTANARI
Classifica: 01-01 /					

È visibile, all'interno del blocco centrale, il risultato della ricerca lanciata. Per ogni documento viene visualizzato il numero e la data di protocollazione, il movimento del documento, l'oggetto, la classifica, mittente/destinatari e eventuali file allegati (identificati dall'icona); nonché la data e l'utente che ha modificato per ultimo il documento:

Nel blocco di riepilogo dei dati del documento, sono presenti una serie di bottoni, uno sulla sinistra dei dati del documento, altri sulla destra.

Cliccando sul pulsante posto alla sinistra del documento, si accede in visualizzazione al documento (senza possibilità di modifica); evidenziato in rosso nell'immagine seguente:

Protocollo Generale - 2017 / 75 del 28/03/2017 07:45:12	Modalità:	Arrivo	Mittente/Destinatario		
Oggetto: PREVENTIVO STRUMENTO MONITORAGGIO			- ROSSI MARIO		28/03/2017 MICHELE.FRANCESCO
Classifica: 03-04 2016 / 1					

Il pulsante appena mostrato varia a seconda del tipo di documento a cui si riferisce; si riporta l'elenco delle varie possibilità, rimandando agli appositi paragrafi per ulteriori dettagli:



: identifica un documento inserito a sistema non protocollato ("Documento da Fascicolare").

-  : identifica un documento protocollato.
-  : identifica un messaggio proveniente da PEC o fax inserito a sistema senza protocollazione.
-  : identifica un messaggio proveniente da PEC o fax protocollato.
-  : identifica un documento protocollato annullato.
-  : identifica un documento di tipo "Lettera", creato con la funzione specifica "Lettera in Uscita" o "Lettera Interna".
-  : identifica un documento protocollato proveniente dalla funzione di protocollazione in emergenza.

I bottoni sulla destra di ogni singolo blocco di informazioni consentono:

-  L'accesso all'elenco dei collegamenti presenti all'interno del documento (ad esempio, alla voce di titolare e fascicolo nei quali il documento è stato inserito);
-  La visualizzazione del dettaglio del flusso del documento;
-  L'accesso in modalità di modifica al documento;

Nota Bene: l'icona di modifica può risultare disabilitata (nel caso sarà visualizzata in grigio), in base alle competenze associate all'utente sarà possibile o meno modificare i documenti.

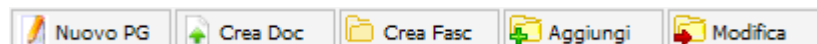
-  L'eliminazione del documento;

Nota Bene: l'icona del cestino sarà sempre disabilitata per i documenti protocollati, sarà invece possibile eliminare eventuali documenti salvati e non protocollati.

-  La visualizzazione delle competenze sul documento.

L'utilizzo di questi due ultimi bottoni dipende dalla profilazione dell'utente e potrebbero quindi risultare disabilitati.

Per concludere questa iniziale panoramica sul Sistema Documentale, si veda la serie di bottoni presenti nella parte alta del blocco di visualizzazione centrale:



- Nuovo PG: consente di accedere alla maschera per l'inserimento di un nuovo protocollo (cfr capitolo 2.1);
- Crea Doc: consente di accedere ad un menu di selezione per l'inserimento di vari documenti, secondo le applicazioni installate e le competenze dell'utente;
- Crea Fasc: consente di accedere alla finestra per l'inserimento di un nuovo fascicolo (cfr. capitolo 2.3);
- Aggiungi e Modifica: permettono di intervenire sulla classificazione secondaria del documento (aggiungi) o di modificare la classificazione primaria (modifica); Cfr. più avanti.

2 Creazione ed inserimento di nuovi documenti

2.1 Modalità di protocollazione dei documenti

Alla maschera che permette l'inserimento di un nuovo protocollo è possibile arrivare in due modalità differenti:

- attraverso il menu a tendina posto sulla **Smart Desktop**, selezionando "Crea Protocollo":



- attraverso il bottone “Nuovo PG” presente in alto nel blocco di visualizzazione del **Sistema Documentale**:



Indipendentemente dalla modalità utilizzata, viene aperta la finestra di inserimento di un nuovo protocollo:

 A screenshot of the 'Protocollo Generale' form. The form has a header with 'Protocollo Generale' and a user profile 'CECILIO CRISTIAN'. Below the header are fields for 'Tipo Documento', 'Riservato' (SI/NO), 'Oggetto', 'Doc. Principale', 'Classificazione', 'Tramite', 'Ufficio Esibente', 'Fascicolo', and 'Precedente'. There are also sections for 'Corrispondenti' and 'Smistamenti'. At the bottom, there are buttons for 'Salva', 'Protocollo', and 'Chiudi'.

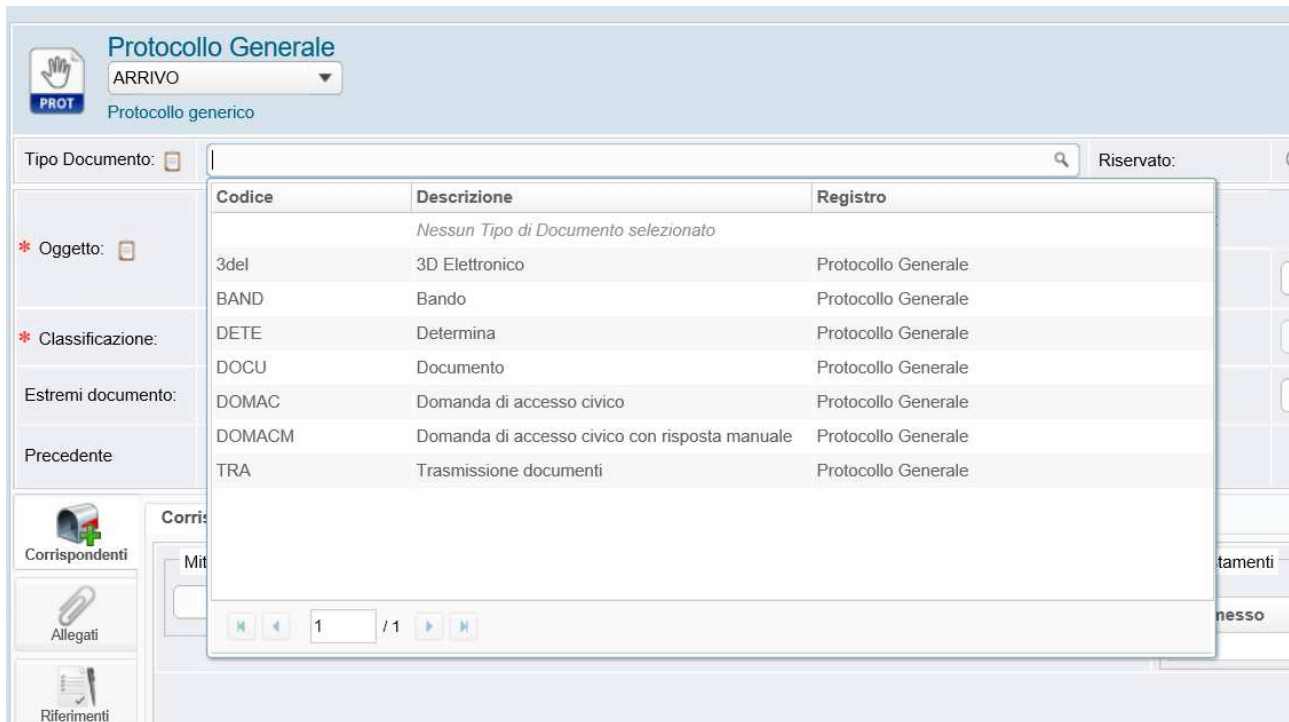
2.1.1 Pulsanti Funzionali

Nella parte inferiore del modello sono presenti i pulsanti *funzionali*:

- **Salva**: consente di salvare in ogni momento le modifiche effettuate sul documento, sia prima che dopo la protocollazione;
- **Protocollo**: attiva la funzione di protocollazione dei dati inseriti;
- **Chiudi**: chiude la maschera;
- **Funzionalità**: apre un menu contestuale allo stato del documento (cfr. più avanti);
- **Firma**: disponibile post salvataggio; permette di firmare digitalmente documento principale (cfr. più avanti);
- **Pubblica all'Albo**: disponibile post protocollazione; se presente il modulo di gestione Albo Pretorio On Line rilasciato da società del Gruppo Finmatica, e se l'utente è abilitato, apre la finestra per la pubblicazione su Albo Pretorio riportando i dati dal documento dal quale è richiamata la funzione stessa (cfr. più avanti).

2.1.2 Menu contestuali

Sono presenti dei cosiddetti “menu contestuali”: tutti i menu a tendina presenti in maschera (come la scelta del Tipo documento o della Classificazione) sono navigabili da tastiera, tramite i pulsanti di tipo “freccia”. Ad esempio, cominciando a scrivere nel campo “Tipo Documento”, automaticamente parte la ricerca contestuale:



Per selezionare il valore desiderato, è possibile muoversi con le frecce della tastiera, e confermare l’inserimento tramite il tasto “Invio”.

I campi che è possibile navigare da tastiera sono:

- Tipo Documento
- Tramite
- Classificazione
- Fascicolo

Diviene altresì possibile spostarsi di campo in campo con il tasto “TAB” o tornare indietro di un campo con la combinazione “Shift” + “TAB”.

2.1.3 Inserimento dei dati giuridici e archivistici

Modalità: Individua il movimento, ovvero se ciò che si sta protocollando è un documento in entrata (arrivo), in uscita (partenza) o di corrispondenza interna all'Amministrazione. Si valorizza attraverso l’apposito menu a tendina posto nella parte alta della maschera di Protocollo



Nota bene: la possibilità di protocollare in arrivo, partenza o interno è gestita tramite l'attribuzione di ruoli specifici all'interno dell'applicativo di Struttura Organizzativa. A seconda quindi dei ruoli attribuiti, potrebbero essere visibili combinazioni limitate di modalità di protocollazione.

Unità: Si valorizza utilizzando il relativo menu contestuale posto nella parte alta della maschera di Protocollo;

Codice	Descrizione
U_CONT	CONTRATTI
STRADE_2	Ufficio Manutenzioni Stradali
Nessuna Unità selezionata	

Nota bene: la possibilità di protocollare per più di una unità dipende dalla configurazione del componente all'interno dell'applicativo di Struttura Organizzativa; il default propone l'unità principale di appartenenza.

Tipo Documento: Si valorizza utilizzando il relativo menu contestuale, oppure attraverso l'icona  che apre una pop up dalla quale è possibile ricercare ed inserire il valore selezionato;

Codice	Descrizione	Oggetto	Classificazione	Fascicolo	Registro	Protocollo
3del	3D Elettronico					Protocollo Generale

Nota bene: la pop up carica un elenco di oggetti ricorrenti che l'Ente ha deciso di standardizzare per velocizzare l'operazione di protocollazione. A questi oggetti possono essere associate anche altre informazioni oltre al campo specifico, come Oggetto, Classificazione, Smistamenti ed altro; queste informazioni sono eventualmente modificabili in un momento successivo all'inserimento. È uno strumento utile nel caso in cui un utente si trovi a dover protocollare un numero importante di documenti simili o afferenti agli stessi particolari.

Riservato: se valorizzato a "SI" indica che la visibilità del documento è riservata all'unità protocollante e alle altre unità che siano autorizzate, tramite ruolo e competenze, a visualizzare documenti riservati.

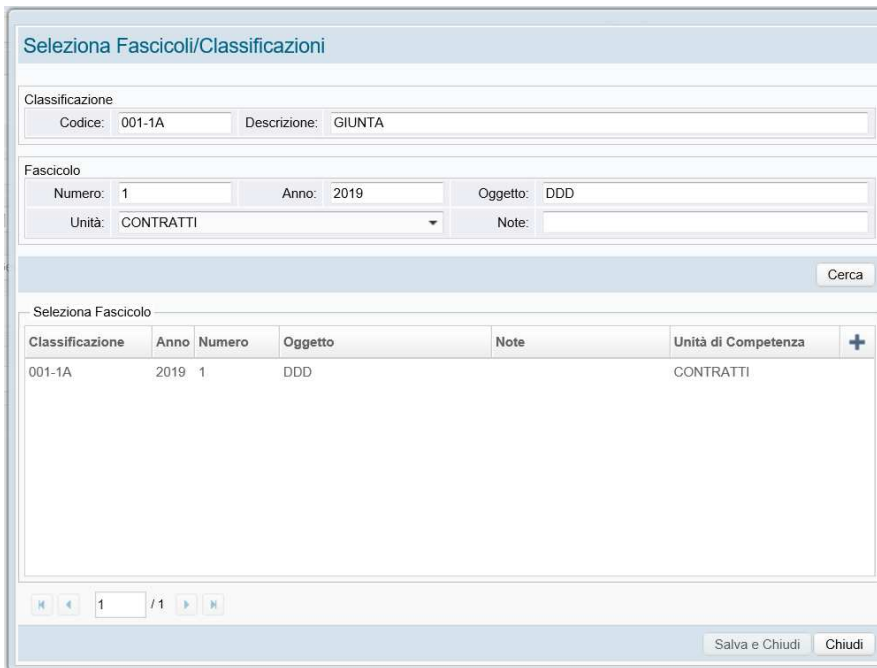
Oggetto: È il riassunto del contenuto dell'atto, dato obbligatorio ma libero. Il campo può contenere fino a 2000 caratteri. Come per il Tipo Documento, è possibile precaricare una serie di Oggetti ricorrenti, da utilizzare per velocizzare la protocollazione (pop up ).

Doc. Principale: Tramite il pulsante , il sistema accede direttamente alla maschera di Esplora Risorse di Windows, dalla quale è possibile ricercare il file da allegare. Tramite il pulsante  è possibile accedere alla funzionalità per l'acquisizione tramite scansione interattiva. Una volta inserito un file, è eventualmente possibile eliminarlo tramite l'apposito pulsante (). Il pulsante  attiva un campo editabile che consente la modifica del nome del file inserito. Se viene inserito un file firmato digitalmente, il sistema integra un sistema automatico di verifica della firma, parametrizzabile: la verifica può essere eseguita al momento della protocollazione, oppure al momento dell'eventuale invio tramite PEC del documento protocollato. Questa parametrizzazione agisce a livello di intero applicativo per tutti gli utenti.

Tramite: Relativo alle possibili modalità di ricevimento o di spedizione di un documento (es. Raccomandata, Telegramma, Fax) per avere un'ulteriore differenziazione degli atti oltre a quella per tipologia, utile per velocizzare ricerche e visualizzazioni all'interno del registro. I valori presenti sono relativi ad un dizionario personalizzabile a livello amministrativo. Si valorizza utilizzando il relativo menu contestuale

Classificazione: codice della voce di titolare con la quale si classifica il documento. L'inserimento della descrizione viene riportato automaticamente dal sistema al momento dell'inserimento. Si valorizza utilizzando il relativo menu contestuale

Fascicolo: nel caso di fascicolazione del documento, inserire l'anno e il numero del fascicolo di destinazione. Il sistema compila automaticamente il campo descrizione al momento dell'inserimento. Si valorizza utilizzando il relativo menu contestuale, oppure attraverso l'icona  che apre una pop up dalla quale è possibile ricercare ed inserire il valore selezionato;



La maschera "Selezione Fascicoli/Classificazioni" presenta i seguenti campi e sezioni:

- Classificazione:**
 - Codice: 001-1A
 - Descrizione: GIUNTA
- Fascicolo:**
 - Numero: 1
 - Anno: 2019
 - Oggetto: DDD
 - Unità: CONTRATTI (menu a tendina)
 - Note: (campo vuoto)
- Seleziona Fascicolo:**
 - Tabella con colonne: Classificazione, Anno, Numero, Oggetto, Note, Unità di Competenza.
 - Riga 1: 001-1A, 2019, 1, DDD, (vuoto), CONTRATTI.
- Controlli:**
 - Botone "Cerca" a destra della sezione Fascicolo.
 - Barra di navigazione in basso con indicatori "1 / 1".
 - Bottoni "Salva e Chiudi" e "Chiudi" in basso a destra.

Estremi del Documento: Si riferisce al numero di protocollo e data del mittente presente sul documento in arrivo che si sta protocollando. Visualizzato solo quando il Tipo Movimento (Modalità) è settato su "Arrivo".

Nota Bene: vengono gestiti su questo campo controlli automatici che segnalano un errore in fase di salvataggio o protocollazione nei casi in cui:

- I riferimenti al documento esterno risultano inseriti in altri documenti precedentemente protocollati dal proprio Ente, e non è stato esplicitamente indicata la volontà di inserire ugualmente il riferimento in oggetto, valorizzando a 'SI' l'apposito campo 'PROCEDI SE GIA' PRESENTI'. Questo tipo di controllo è utile

per evitare che lo stesso documento venga protocollato più volte da persone diverse all'interno dell'Amministrazione.

Estremi documento: del ☒ Procedi se presente

- La data del documento esterno risulta:
 - ✓ Maggiore della data odierna;
 - ✓ Maggiore della data di protocollazione.

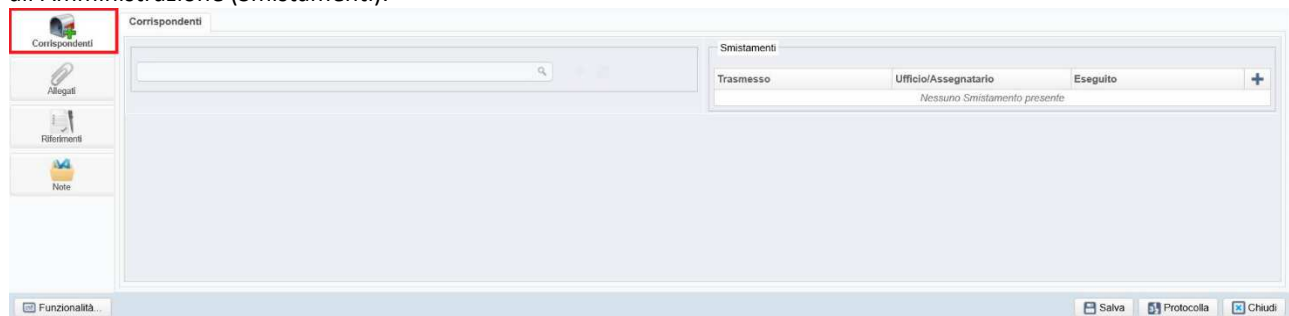
Ricevuto il: Data del "timbro" di arrivo effettivo del documento all'interno dell'ente. Viene visualizzato solo quando il Tipo Movimento (Modalità) è settato su "Arrivo".

Ufficio Esibente: Campo che diventa visibile quando viene scelta la modalità di movimento "Interno" o "Partenza". Permette, tramite il relativo menu contestuale, di valorizzare l'ufficio che ha presentato il documento alla protocollazione. A seconda della profilazione del sistema, l'indicazione dell'ufficio esibente abilita la visibilità del documento agli utenti dell'unità indicata.

Precedente: Individua il riferimento ad un protocollo precedente già esistente nei registri dell'Ente, selezionabile utilizzando il relativo menu contestuale. È presente un controllo su quanto viene inserito, in merito ad effettiva esistenza del riferimento inserito: se i dati inseriti (in termine di anno e numero di protocollo) trovano riscontro, il sistema pone un'icona di check positivo vicino ai campi (), la quale diventa un collegamento al documento inserito; in caso contrario, mostra un messaggio con l'indicazione che i dati inseriti non trovano riscontro.

2.1.4 Inserimento di rapporti e gestione anagrafica

Nella parte inferiore della maschera del protocollo, che si suddivide in più sottosezioni, di cui viene messa in evidenza la sottosezione "Corrispondenti", nella quale è possibile riportare gli eventuali destinatari esterni e interni all'Amministrazione (Smistamenti):



Una volta inserito il dato nel campo "Mittenti", premendo il pulsante Invio sulla tastiera o cliccando la lente di ingrandimento (), il sistema riporta direttamente i dati nella maschera, se quanto digitato trova riscontro univoco nelle banche dati dei soggetti. In alternativa, apre una maschera con l'elenco dei soggetti che rispettano i dati digitati. A questo punto, è sufficiente selezionare il dato desiderato per confermare l'inserimento del rapporto. Per inserire un ulteriore rapporto, è sufficiente editare un nuovo dato nel campo "Mittenti". Per eliminare un rapporto precedentemente inserito, è possibile cliccare l'apposito pulsante ().

2.1.4.1 Ricerca soggetti in fase di protocollazione

È possibile ricercare inserendo direttamente nel campo della maschera utilizzando

- Una o più parole intere (ad es. ROSSI, ROSSI MARIO, PROVINCIA BOLOGNA). Inserendo una parola intera verranno resi come risultati tutte le registrazioni che contengono la parola chiave, a prescindere dalla posizione della parola chiave nella descrizione;

- Il carattere jolly % nelle seguenti combinazioni:
 - Alla fine di porzioni di parole, per trovare tutte le parole che cominciano con la chiave utilizzata; ad esempio ROSS%
 - All'inizio di porzioni di parole, utilizzando in questo caso il doppio carattere jolly; ad esempio %%OSSI
- Intero codice fiscale o partita iva.

La ricerca viene eseguita su tutte le banche dati anagrafiche integrate nell'applicativo, tra le quali viene previsto l'accesso all'archivio dell'anagrafe dei residenti. Se alla ricerca corrisponde un solo risultato possibile, il risultato viene immediatamente riportato nella maschera, senza passare da ulteriori finestre. Al contrario, se alla ricerca corrisponde più di un risultato il sistema presenta un'ulteriore finestra che riporta tutte le corrispondenze trovate.

Accesso alla banca dati PEC di I.P.A.

Il sistema prevede l'integrazione con l'indice IPA mettendo a disposizione, degli utenti abilitati, una specifica funzione di aggiornamento dei dati e/o consentendo la sincronizzazione con tale banca dati tramite processo automatico attivato periodicamente, che l'ente può configurare in base alle specifiche esigenze (ad esempio tramite elaborazione notturna). La fase applicativa si compone di tre sezioni:

Criteri di aggiornamento: tramite la quale assegnare un nome identificativo all'operazione compilando il campo NOME CRITERI AGGIORNAMENTO (per es. "Provincia di Venezia" o "Comuni della Provincia di Venezia");

Dati Amministrazioni	
Codice Amministrazione	☒ Tutte
Descrizione	
Ricerca per ente	Comune
Nella Regione	LOMBARDIA
Nella Provincia	MILANO

Dati Amministrazioni: tramite la quale aggiornare la banca dati di una specifica amministrazione inserendone il CODICE AMMINISTRAZIONE oppure compilando il campo DESCRIZIONE con la denominazione dell'Amministrazione;

Dati AOO: tramite la quale aggiornare la banca dati di una specifica area organizzativa omogenea inserendone il CODICE AOO oppure compilando il campo DESCRIZIONE con la denominazione dell'AOO. In alternativa, è possibile scaricare tutte le Aree Organizzative Omogenee afferenti ad una data Regione o Provincia.

Nel caso in cui l'operazione di sincronizzazione non dovesse andare a buon fine, sulla Scrivania virtuale dell'utente che ha attivato l'elaborazione verrà posta una specifica attività di notifica tramite la quale sarà possibile verificare il problema e/o riattivare l'elaborazione.

Si è verificato un errore nello scarico IPA COMUNI PROV. MILANO

2.1.4.2 Inserimento di un nuovo soggetto in fase di protocollazione

Ogni utente protocollatore, in fase di registrazione di un nuovo documento, ha la possibilità di inserire nuovi corrispondenti non ancora compresi in una delle banche dati anagrafiche a disposizione.

È possibile operare in due modi distinti, a seconda che si conosca o meno il codice fiscale o partita iva del nuovo soggetto:

- Se viene inserito il codice fiscale (o partita iva), il soggetto viene registrato anche nella banca dati denominata "Altri Soggetti", e sarà ricercabile successivamente;
- Se non viene inserito il codice fiscale (o partita iva), il soggetto viene registrato soltanto sulla singola registrazione di protocollo che si sta effettuando: in questo modo si preserva la conservazione dell'informazione ma non si compromette l'integrità della banca dati dei soggetti. Questo tipo di inserimento non pregiudica il ritrovamento successivo della registrazione di protocollo tramite denominazione del corrispondente.

Per accedere alla maschera di inserimento soggetto, è necessario cliccare l'apposito pulsante . Il sistema apre la finestra dedicata, la quale è così composta:

Anche in questo caso sono presenti tre sezioni, la prima per i dati anagrafici principali, quindi la sezione Recapiti e contatti per l'inserimento dei recapiti di residenza, domicilio e relativi contatti, la terza espone i valori relativi a periodi storicizzati del soggetto. I campi obbligatori sono evidenziati da un asterisco rosso e nella maggior parte dei casi i campi sono liberamente compilabili dall'utente; gli altri:

- NI: viene compilato in automatico dal sistema con un numero progressivo al momento dell'inserimento del soggetto.
- Sesso: se individuo, scegliere dal menu a tendina.
- Tipo soggetto: consente di attribuire al soggetto l'attributo attraverso apposito menù popolato da valori confermati nell'apposito dizionario.
- Dal: il sistema propone in automatico la data corrente; è possibile modificarla tramite l'apposita pop up di calendario , o scrivendo direttamente nel campo.
- Al: il sistema propone in automatico il campo vuoto; è possibile modificare il valore impostando la data di chiusura del soggetto. Da quella data il soggetto non sarà più reperibile dalle ricerche per l'inserimento dei suoi dati nel campo corrispondente dei documenti di protocollo.
- Comune e Provincia: i campi vanno valorizzati tramite la pop up  disponibile nel campo Comune, come illustrato poco sopra.

Una volta inseriti tutti i dati, per registrare il soggetto è necessario cliccare il pulsante  posto in basso a destra nella maschera. Il sistema darà un messaggio di conferma; il dato inserito sarà visualizzabile nel corpo centrale della maschera principale. Il soggetto inserito sarà adesso utilizzabile anche in fase di protocollazione dei documenti, attraverso l'apposita funzione di inserimento dei mittenti/destinatari.

2.1.4.3 Modifica di un soggetto esistente in fase di protocollazione

Ogni utente protocollatore ha la possibilità di modificare le registrazioni anagrafiche esistenti nella banca dati "Altri Soggetti", se si renda necessario. Per poter modificare un soggetto esistente, è necessario attivare l'apposita icona  presente a destra di ogni soggetto trovato nella fase di ricerca.

Ad ogni soggetto, oltre alle informazioni relative al cognome e nome o denominazione e i dati anagrafici, possono essere

integrati i dati relativi a diversi recapiti e per ogni recapito diverse tipologie di contatto (definizione dei relativi dizionari al paragrafo 2.2.5 del presente manuale). Nell'immagine riportata di seguito viene ad esempio visualizzato il dettaglio di un soggetto per il quale sono stati registrati 3 recapiti (residenza, domicilio e sede legale): al recapito di tipo Residenza risultano associati 2 contatti, un indirizzo di tipo mail (posta elettronica semplice) e uno di tipo mail PEC (posta elettronica certificata).

Nota bene: la banca dati "Altri Soggetti", a cui fa riferimento la banca dati specifica dell'applicativo, è in realtà una banca dati trasversale ad altri applicativi rilasciati da Gruppo Finmatica potenzialmente installati. Posso esserci casi in cui il soggetto sia stato inserito da uno di questi altri applicativi (ad esempio, applicativi di Gestione Personale) e che quindi non sia modificabile come appena esposto, in quanto di priorità dell'altro applicativo.

2.1.4.4 Indicazione di destinatario "Per Conoscenza" sulle registrazioni di protocollo

L'applicativo rende disponibile la possibilità di indicare che il soggetto collegato alla registrazione di protocollo è "per conoscenza". In caso di invio tramite PEC della registrazione con destinatari per conoscenza, l'attributo confluisce nella segnatura allegata alla PEC stessa, di modo da poter essere interpretata dai sistemi interoperabili dei destinatari. Allo stesso modo, se si riceve una PEC destinata alla protocollazione, che nella segnatura riporta l'attributo, viene riportato in automatico nella registrazione di protocollo.

Per settare un soggetto come destinatario per conoscenza è necessario agire sulla casella di spunta posta sulla destra di ogni soggetto presente sulla registrazione di protocollo, nella sezione "Corrispondenti" della maschera di protocollo:

Il rapporto così contrassegnato viene mostrato in corsivo nella maschera.

Per funzionamento specifico dei sistemi di Posta Elettronica Certificata, non è possibile inviare messaggi che presentino esclusivamente destinatari per conoscenza, dovendo prevedere obbligatoriamente almeno un destinatario diretto.

2.1.5 Inserimento di smistamenti

L'inserimento degli smistamenti è possibile dalla sezione "Corrispondenti" nella parte bassa della maschera di protocollazione, dall'apposito riquadro a destra "Smistamenti". Per inserire un nuovo smistamento, è possibile cliccare l'apposito pulsante (+). Il sistema aprirà la maschera per la scelta e l'inserimento dello smistamento:

Nella parte alta della schermata è possibile scegliere se lo smistamento che si sta inserendo è per "competenza" o per "conoscenza".

La maschera si presenta suddivisa in due parti: nella parte sinistra vi è riportata la struttura organizzativa dell'Ente. Nella parte destra, due riquadri:

- Elenco Unità cui smistare il documento;
- Elenco Componenti cui assegnare il documento.

L'applicativo dà la possibilità infatti di smistare i documenti sia a una o più unità o uffici, sia direttamente a specifici utenti.

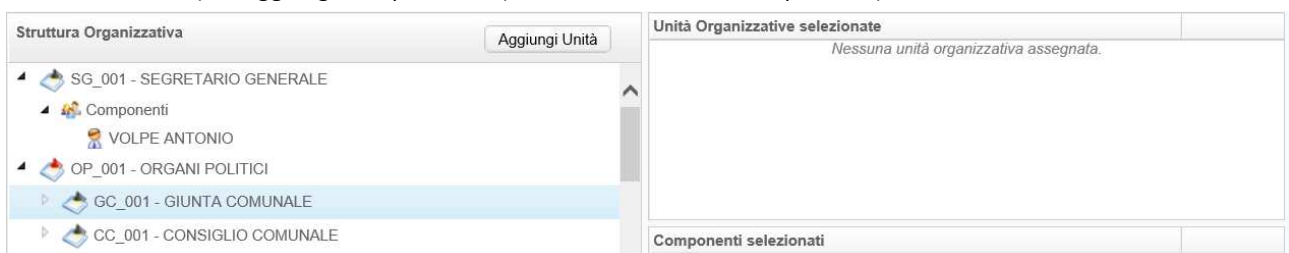
Nota bene: la possibilità di smistare e di assegnare direttamente a componenti specifici è gestita a seconda del ruolo e delle competenze assegnate all'utente protocollatore. Potrebbe quindi essere possibile che da utente a utente la schermata si presenti diversa, o che alcuni utenti non possano assegnare direttamente ad altri utenti ma solo smistare ad uffici, o altro ancora. Queste valutazioni vengono fatte insieme all'Amministrazione nella fase di installazione e configurazione degli applicativi.

Questa maschera funziona secondo il principio del "trascinamento" (drag & drop): dopo aver individuato il destinatario (ufficio o componente) da inserire, è sufficiente trascinarlo tenendo premuto il tasto sinistro del mouse, per poi rilasciare dentro la finestra scelta. Trascinando, si ottiene questo:

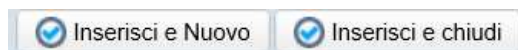


Nel caso in cui un inserimento venga fatto per errore e vada cancellato, è necessario cliccare sul cestino (🗑️) posto a destra del destinatario.

In alternativa al "trascinamento" (drag & drop), è possibile utilizzare l'apposito pulsante "Aggiungi Unità" (nel caso di selezione di Unità) o "Aggiungi Componente" (nel caso di selezione Componente):



E' possibile inserire uno o più smistamenti tramite i pulsanti:



- **Inserisci e Nuovo:** Permette di salvare lo smistamento o gli smistamenti inseriti, e di inserirne ulteriori. Ad esempio, nel caso in cui il documento necessiti di smistamenti sia per competenza che per conoscenza, si possono inserire prima gli smistamenti per competenza:

Smistamenti

Tipo di Smistamento: ☒ COMPETENZA ☐ CONOSCENZA

Unità di Trasmissione: CONTRATTI

Cerca unità o soggetti...

Struttura Organizzativa

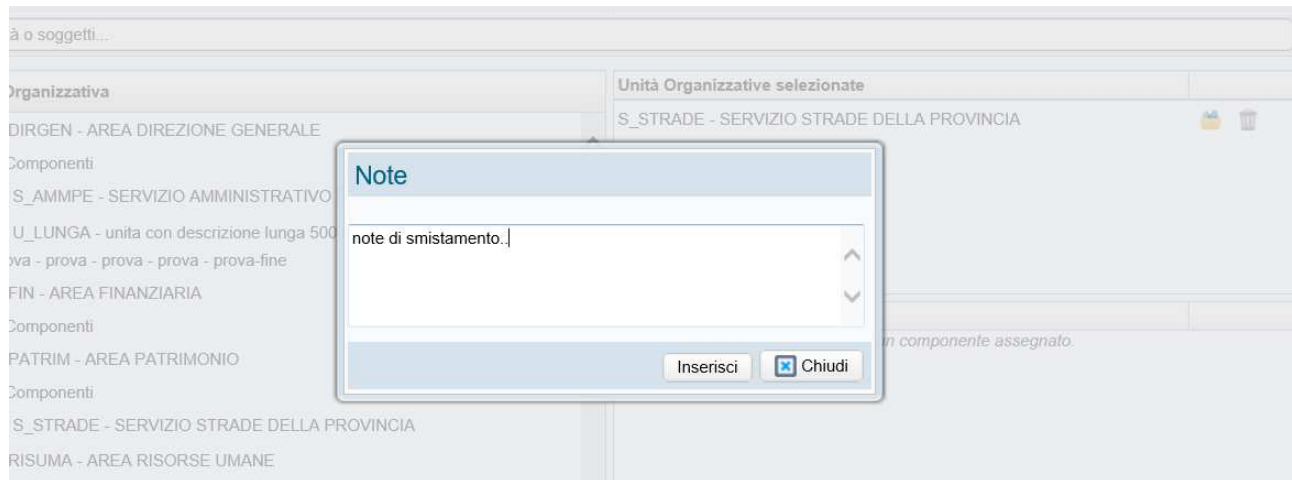
- A_DIRGEN - AREA DIREZIONE GENERALE
 - Componenti
 - S_AMMPE - SERVIZIO AMMINISTRATIVO PERSONALE
 - U_LUNGA - unità con descrizione lunga 500 caratteri x test - stefania - prova - prova - prova - prova - prova - prova - fine
 - A_FIN - AREA FINANZIARIA

Unità Organizzative selezionate

- S_STRADE - SERVIZIO STRADE DELLA PROVINCIA
- A_FIN - AREA FINANZIARIA

- Cliccando sul tasto "Inserisci e Nuovo", il sistema salva gli smistamenti inseriti e ripresenta la maschera vuota, di modo che sia possibile selezionare il tipo smistamento "Conoscenza" ed aggiungere altri smistamenti.
- **Inserisci e Chiudi:** Registra gli smistamenti inseriti e chiude la finestra, riportando l'utente alla maschera principale di inserimento protocollo.

L'icona () apre una finestra nella quale è possibile inserire delle note specifiche che accompagnano lo smistamento:



Inseriti gli smistamenti, e tornati sulla maschera principale di inserimento protocollo, il riquadro degli smistamenti apparirà popolato con i dati appena inseriti.

È altresì possibile inserire gli smistamenti dall'apposita maschera di dettaglio posta nel riquadro di inserimento "Corrispondenti": in questa, sarà possibile visualizzare le informazioni aggiuntive, come eventuali assegnatari, data/ora di presa in carico, storico degli smistamenti, dettagli degli smistamenti ripudiati, eccetera:

Corrispondenti					
Smistamenti					
Smistamenti Correnti					
Tipo	Trasmesso	Ufficio/Assegnante	Preso in carico	Assegnato	Eseguito
COMPETENZA	U_CONT - CONTRATTI	A_FIN - AREA FINANZIARIA		BOLOGNA MARIO	
	RE NICOLA 20/10/2019 10:34:23	RE NICOLA		A_FIN - AREA FINANZIARIA 20/10/2019 10:34:23	
COMPETENZA	U_CONT - CONTRATTI	A_DIRGEN - AREA DIREZIONE GENERALE			
	RE NICOLA 20/10/2019 10:34:23				
Smistamenti Storici					

2.1.6 Inserimento di allegati

Per inserire allegati generici alla registrazione di protocollo, è necessario accedere alla relativa sezione "Allegati":



Tramite l'inserimento (), la gestione () e l'eliminazione () delle informazioni inserite. Le tre funzioni sono accessibili anche tramite il menu contestuale della finestra, oppure attraverso combinazioni di tasti.

Scegliendo l'inserimento di un nuovo allegato (), il sistema presenta la relativa maschera:

È possibile inserire i dati riguardanti la quantità, il numero di pagine, scegliere dal menu a tendina la tipologia di allegato che si sta inserendo, ed inserire una descrizione, indicare se si tratta di files da Firmare digitalmente, se devono essere inclusi in Stampa Unica e se sono Riservati. Se è necessario inserire un file, è necessario salvare l'intera registrazione, tramite il pulsante "Salva" della maschera principale; successivamente, tramite il pulsante  il sistema accede all'Esplora Risorse di Windows, dal quale è possibile selezionare il file. Se è necessario acquisire l'allegato tramite scansione, cliccando il pulsante  viene avviata la funzionalità apposita. Se è necessario eliminare il file associato all'allegato, è possibile intervenire tramite il pulsante .

Una volta inserito, cliccando sul pulsante "Salva e chiudi", il sistema riporta nella sezione "Allegati" i dati appena inseriti:

Allegati				
	Tipo Allegato	Descrizione	Riservato	Da firmare
1	Allegato	documenti	No	 

Cliccando due volte sui dati di dettaglio, verrà aperta la maschera di dettaglio (accessibile anche cliccando il pulsante ). Cliccando direttamente sul pulsante  nome del file si aprirà direttamente la possibilità di visualizzare o scaricare il file vero e proprio.

2.1.7 Storico modifiche

La sezione "Storico" presente nella maschera di inserimento protocollo all'apertura si presenta vuota, in quanto la specifica funzionalità viene attivata soltanto dopo che è stata eseguita l'operazione di protocollazione.

In questa sezione è possibile visualizzare tutte le modifiche che sono state apportate al documento dalla sua creazione, nonché le date in cui le modifiche sono state effettuate e gli utenti che le hanno inserite. Questo dà la possibilità anche di tracciare le eventuali modifiche che vengono effettuate sui campi o sugli allegati dal momento della creazione (tutti i dati inseriti prima della protocollazione vengono comunque registrati e mostrati) al momento dell'interrogazione.

Storico Flusso				
Storico Protocollo				
Storico Flusso Envers				
Storico Protocollo Envers				
Ricerca storico dal: 01/10/2019		Ricerca storico al:		
Mostra Campi: -- Tutti i Campi --		Cerca		
#	Data	Utente	Campo	Valore
1	18/10/2019 16:44:23	RE NICOLA	Codice Classifica	001-1A - GIUNTA
			Movimento	ARRIVO
			Oggetto	NUOVO DOCUMENTO DEL 18/10/2019
			File Principale	registroProtocolloNuovi_2.odt
			Allegato	Allegato
			Riservato	No
			File	registroProtocolloModificati.odt
			Corrispondente	ADS SPA
				67847739920
				ISTITUZIONALEADS@CERT.LEGALMAIL.IT
				VIA C/AM/CIAM/2

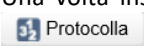
Le righe che vengono evidenziate con l'icona  sono riferite a operazioni di cancellazione di allegati (nel caso riportato nell'esempio sottostante, è stato cancellato il "File principale"):

20/10/2019 12:35:02	RE NICOLA	File Principale	registroProtocolloNuovi_2.odt
		Allegato	Allegato
		Riservato	No
		File	registroProtocolloModificati.odt

Tramite il menu a tendina "Mostra Campi" è possibile specificare per quale tipologia di "campi" effettuare la ricerca, tra i campi più significativi che compongono la maschera di inserimento protocollo:

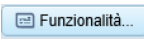
Ricerca storico dal:	01/10/2019
Mostra Campi:	-- Tutti i Campi --
Utenti	-- Tutti i Campi -- Mostra tutti i campi Dati Documento Dati principali del documento: oggetto, movimento, data Dati Fascicolazione Dati di classificazione e fascicolo Destinatari Dati dei destinatari

2.1.8 Controlli in fase di protocollazione e menu "Funzionalità" in fase di creazione e protocollazione di documenti

Una volta inseriti i dati nella maschera, è possibile procedere alla effettiva protocollazione, attraverso il pulsante , posto nella parte inferiore maschera. Il sistema procede ad una serie di controlli sui campi definiti obbligatori dall'Ente e rende un messaggio d'errore nel caso in cui non ne siano stati valorizzati, specificando il valore mancante.

Al momento che tutti i dati sono inseriti, cliccando il tasto protocolla il sistema riempie i dati relativi al Registro di protocollo e a numero e data di protocollazione; ad esempio:

Protocollo Generale n° 479 del 21/10/2019 10:00:58
PARTENZA

Durante la fase di creazione di un nuovo documento di protocollo e, limitatamente per il protocollatore (ed eventuali utenti della stessa unità abilitati), dopo la protocollazione stessa, il menu Funzionalità attivabile attraverso il pulsante  presenta queste opzioni:

- **Nuovo (INS):** apre la maschera di inserimento di un nuovo protocollo.
- **Nuova Lettera:** apre la maschera di inserimento di una nuova Lettera.

- **Copia:** crea un nuovo documento importando i dati dal documento dal quale si richiama la funzione (cfr. paragrafo 2.2 Preferenze di Applicazione).
- **Rispondi:** crea un nuovo documento importando i dati dal documento dal quale si richiama la funzione (cfr. paragrafo 2.2 Preferenze di Applicazione), ribaltando il movimento e collegandolo al numero di protocollo:

Precedente:	2019	1230	Protocollo Generale	
-------------	------	------	---------------------	---

non è disponibile se il movimento del documento dal quale si vuole richiamare la funzione è "Interno".

- **Rispondi con Lettera:** crea un nuovo documento "Lettera" importando i dati dal documento dal quale si richiama la funzione (cfr. paragrafo 2.2 Preferenze di Applicazione), ribaltando il movimento e collegandolo al numero di protocollo: non è disponibile se il movimento del documento dal quale si vuole richiamare la funzione è "Interno" o "Partenza".
- **Crea Inoltro:** crea un nuovo documento in "PARTENZA" importando i dati dal documento dal quale si richiama la funzione, collegandolo al numero di protocollo e inserendo tra gli allegati secondari il documento principale: non è disponibile se il movimento del documento dal quale si vuole richiamare la funzione è "Partenza".
- **Crea Inoltro con Lettera:** crea un nuovo documento in "Lettera" importando i dati dal documento dal quale si richiama la funzione, collegandolo al numero di protocollo e inserendo tra gli allegati secondari il documento principale: non è disponibile se il movimento del documento dal quale si vuole richiamare la funzione è "Partenza".
- **Annulla:** apre pop up nella quale inserire "Motivazione Annullamento" e Unità (tra quelle di appartenenza dell'utente) per cui effettuare la richiesta.
- **Stampa Barcode (ALT + B):** attiva la generazione del codice a barre, per la successiva stampa dello stesso.
- **Stampa Protocollo:** attiva la generazione di un report contenente i dati di protocollazione, per la successiva stampa dello stesso.
- **Stampa Ricevuta:** attiva la generazione di un report contenente i dati di protocollazione e dettagli ricevuta da consegnare al mittente.
- **Scarica la Stampa Unica:** permette di scaricare il file SU_num-prot_anno-prot.pdf comprensivo degli allegati (indicati in fase di inserimento come da includere in Stampa Unica) e Frontespizio con i metadati del protocollo (se configurato).
- **Crea la Stampa Unica:** permette di creare un file in formato pdf comprensivo degli allegati (indicati in fase di inserimento come da includere in Stampa Unica) ed eventuale Frontespizio con i metadati del protocollo (se configurato); il file prodotto verrà salvato tra gli allegati del protocollo e disponibile per la consultazione o scarico.
- **Scarica Zip Allegati:** permette di scaricare in unico file compresso tutti i file allegati alla registrazione di protocollo.

- **Importa Allegati da Documentale:** permette di importare files allegati ai documenti registrati nel sistema documentale di diverse tipologie (protocolli, atti, etc.)
- **Gestione Anagrafica:** collegamento all'applicativo Anagrafe Soggetti (Gestione Anagrafe Generale Soggetti)
- **Invia PEC:** apre la finestra dedicata all'invio del documento protocollato tramite Posta Elettronica Certificata (disponibile solo su documenti con movimento "Partenza").

Nel momento che la protocollazione è stata effettuata, il sistema provvede ad instradare i flussi associati al documento; ovvero, gli utenti destinatari degli smistamenti inseriti vedranno comparire sulle proprie Smart Desktop le attività legate al documento protocollato (cfr. capitolo 3).

2.1.9 Visualizzazione e inserimento dei riferimenti del documento

La sezione "Riferimenti" è composta da 4 pagine:

- **Collegamenti:** contiene i Collegamenti agli eventuali documenti collegati al documento in visualizzazione

Numero	Anno	Tipo Registro	Tipo Collegamento	Oggetto
479	2019	Protocollo Generale	Protocollo Precedente	TEST

Nella sezione viene mostrato il numero e anno del documento collegato, il tipo di Registro e di Collegamento, nonché l'oggetto. L'icona (🗑️) sulla destra permette di cancellare il collegamento al protocollo. L'icona (ℹ️), è il collegamento per aprire in una nuova finestra il documento collegato. È possibile aggiungere ulteriori riferimenti tramite il pulsante **+ Inserisci** indicando negli appositi campi Anno, Numero, Registro e Tipo collegamento (ad esempio "Riferimento");

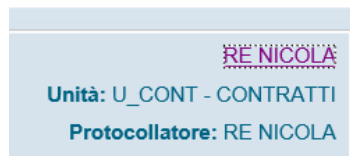
- **Riferimenti:** contiene i dettagli a eventuali pubblicazioni del documento in altri moduli (ad esempio Albo pretorio On Line);
- **Catena Documentale:** visualizza, in maniera ordinale, i protocolli precedenti e successivi collegati al documento, consultabili tramite l'icona (ℹ️);
- **Posizioni Archivistiche secondarie:** consente l'inserimento di fascicolazioni secondarie.

2.1.10 Inserimento Note al protocollo

La sezione "Note", è utilizzabile dall'utente per aggiungere note alla protocollazione, note che saranno poi visibili da questa pagina:

2.2 Preferenze di applicazione

È data la possibilità di gestire direttamente dall'utente una serie di preferenze rispetto al comportamento dell'applicativo. È possibile accedere alla finestra per la scelta delle preferenze cliccando sul nome utente, posto in alto a destra nella maschera di protocollazione:



Cliccando sul proprio nominativo, e quindi sulla pagina “Preferenze”, l’utente accede alla maschera del dettaglio delle preferenze:

L’utente ha la possibilità di selezionare la funzionalità desiderata spuntando il quadratino alla sinistra della singola voce per le preferenze on/off; tramite appositi menu a tendina è invece possibile cambiare il valore impostato per le preferenze con valori multipli; dopodiché, è sufficiente cliccare il pulsante “Salva” o “Salva e Chiudi” per registrare l’informazione e tornare alla schermata precedente.

Le preferenze di applicazione (e loro spiegazione) sulle quali è possibile intervenire:

- **Abilita stampa barcode diretta:** permette l’abilitazione di funzionalità di stampa immediata per le etichette di protocollo. È necessaria una configurazione specifica sul pc dell’utente.
- **Abilita stampa ricevuta diretta:** permette l’abilitazione di funzionalità di stampa immediata per le ricevute di protocollo. È necessaria una configurazione specifica sul pc dell’utente.
- **Duplicare i corrispondenti in fase di copia:** indica se, in caso di operazione di copia del documento, il sistema debba copiare i rapporti del documento originario, ovvero l’elenco dei mittenti/destinatari.
- **Duplicare i corrispondenti in fase di risposta:** indica se, in caso di operazione di creazione di risposta al documento, il sistema debba copiare i rapporti del documento originario, ovvero l’elenco dei mittenti/destinatari.

- **Duplicare gli smistamenti in fase di copia:** indica se, in caso di operazione di copia del documento, il sistema debba copiare gli smistamenti presenti sul documento originario.
- **Duplicare gli smistamenti in fase di risposta:** indica se, in caso di operazione di creazione di risposta al documento, il sistema debba copiare gli smistamenti presenti sul documento originario.
- **Duplicare il Fascicolo in fase di copia o risposta:** indica se, in caso di operazione di copia del documento o di creazione di risposta al documento, il sistema debba copiare anche l'informazione relativa alla fascicolazione del documento originario.
- **In fase di scansione richiedere nome file:** tramite la scelta è possibile decidere se il sistema deve ad ogni scansione interattiva richiedere il nome del file, od associare in automatico un nome file univoco ad ogni scansione.
- **In fase di scansione visualizzare le impostazioni:** permette di configurare le richieste delle impostazioni di scansione interattiva.
- **Apri il dettaglio del soggetto se univoco:** in fase di inserimento corrispondente se il soggetto ricercato è univoco apre comunque la maschera di dettaglio dell'anagrafica.
- **Modalità:** indica su quale delle modalità disponibili all'utente debba aprirsi di default la maschera per la protocollazione. Valori possibili: Arrivo, Interno, Partenza. ¹
- **Unità protocollante:** nel caso in cui l'utente abbia più assegnazioni funzionali, indica su quale unità protocollante debba aprirsi di default la maschera per la protocollazione dei documenti. Valori possibili: l'elenco delle unità alle quali l'utente è assegnato.
- **Unità iter:** nel caso in cui l'utente abbia più assegnazioni funzionali, indica su quale unità di appartenenza debba aprirsi di default la maschera per la gestione dell'Iter Documentale (cfr. più avanti).
- **Report timbro:** permette di configurare l'aspetto dell'etichetta, con o senza il codice a barre esteso (utile nel caso di stampa con stampanti a impatto).

Cliccando sul proprio nominativo, e quindi sulla pagina "Cambio Password", l'utente avrà la possibilità di gestire la propria password di accesso all'applicativo:

¹ Si ricorda che la visualizzazione delle modalità è anche legata agli appositi ruoli assegnati da Struttura Organizzativa. Quindi, non tutti gli utenti potrebbero avere tutte e tre le possibilità.

Una volta inseriti i valori richiesti, cliccando sul pulsante  la nuova password verrà salvata a sistema. La funzionalità di cambio password non agisce in caso di integrazione con sistema di autenticazione federata; si invita a fare riferimento alle prassi interne ad ogni Ente per ulteriori chiarimenti.

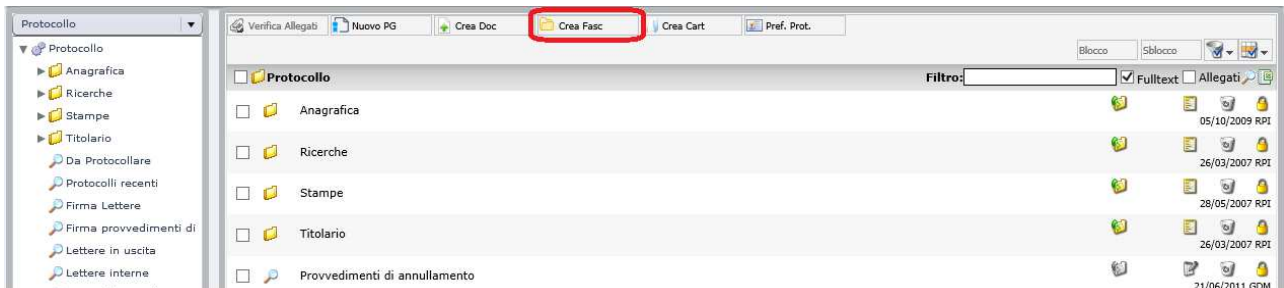
Infine, cliccando sul proprio nominativo, e quindi sulla pagina “Test Funzionalità” l’utente avrà la di testare:

- **Java:** verifica il corretto funzionamento della componente java sul pc, prerequisito per l’utilizzo delle applet di scansione diretta, edita testo e firma digitale.
- **Editor utilizzato:** indica quale editor è utilizzato sul pc, SOFFICE (Open Office) o Microsoft Word.
- **Test Edita Testo:** verifica il corretto funzionamento dell’Edita Testo con l’Editor configurato.
- **Test Firma Digitale:** verifica il corretto funzionamento della firma digitale consentendo la firma di un documento esterno selezionato.

2.3 Creazione di un nuovo Fascicolo

Per gestire al meglio le fasi di classificazione dei documenti protocollati, il sistema di gestione documentale compreso nell’applicativo incorpora una specifica funzionalità di creazione dei fascicoli. È da sottolineare però che non tutti gli utenti potrebbero avere accesso alla funzionalità, secondo quanto deciso dall’Ente in relazione a ruoli e privilegi associati ai vari utenti.

Per procedere alla creazione di un nuovo fascicolo, l'utente abilitato troverà l'apposita voce nel menu a tendina della Smart Desktop "Crea Fascicolo" o, in alternativa, dovrà portarsi nell'area di lavoro del Sistema Documentale, tramite il menu a tendina "Accedi a Protocollo". Verrà quindi aperta una nuova finestra che conterrà l'area di lavoro "Protocollo":



Nell'immagine superiore è evidenziato il pulsante "Crea Fasc", attraverso il quale è possibile accedere alla finestra di inserimento nuovo fascicolo:

Il sistema propone in automatico, nella parte superiore i dati relativi a data di creazione, modificabile tramite il pulsante posto sulla destra del campo, e Unità, modificabile a seconda delle abilitazioni dell'utente, aprendo il menu a tendina del campo stesso. Il campo "Anno" presenta a sua volta una tendina attraverso la quale è possibile scegliere l'anno di archiviazione, il quale può variare a seconda di come è configurata la classificazione; dipendendo dalla classificazione, questo menu non si popola finché non viene scelta la classificazione, appunto.

Pagina "Dati":

Classificazione: è possibile scrivere la classificazione direttamente nel campo, oppure sceglierla tramite la ricerca, accedendovi tramite la ricerca posta sulla destra del campo stesso.

Oggetto: campo libero a disposizione dell'utente.

Unità competente: il campo viene valorizzato in automatico dal sistema con l'unità di appartenenza dell'utente che sta procedendo alla creazione; nel caso in cui l'utente stesso sia abilitato alla creazione di fascicoli per più unità, tramite il menu a tendina si potrà scegliere fra queste.

Responsabile: campo libero a disposizione dell'utente.

Riservato: tramite il menu a tendina è possibile rendere riservato il fascicolo che si sta creando.

Sezione "Dati Archiviazione":

Data apertura: il sistema propone in automatico la data del giorno nel quale si sta creando il fascicolo; tramite la pop up è possibile selezionare una qualsiasi altra data.

Stato archivio: tramite il menu a tendina è possibile scegliere lo stato del fascicolo e gestirne la chiusura. Al momento in cui da questo campo si sceglie uno degli esiti di chiusura ("Deposito" o "Storico"), il sistema compila in automatico il campo "Data Chiusura".

Topografia: campo libero a disposizione dell'utente.

Note: campo libero a disposizione dell'utente.

Al momento in cui sono stati inseriti tutti i dati, è possibile procedere alla creazione del fascicolo tramite il tasto "Crea", situato sulla barra nella parte superiore della finestra. Il sistema provvede alla numerazione del fascicolo e al suo inserimento all'interno della cartella di titolario indicata dall'utente. Una volta ottenuto il numero, sulla sinistra del campo "Oggetto" compare il pulsante , il quale permette di aprire l'elenco dei documenti contenuti nel fascicolo; finestra che si andrà a popolare man mano che i documenti verranno fascicolati. Compare in più nella sezione superiore destra il menu "Funzionalità", il quale conterrà le seguenti voci:

Nuovo: apre una nuova maschera per la creazione di un nuovo fascicolo.

Crea sub: permette di creare un sub-fascicolo all'interno del fascicolo di partenza. Il numero che verrà assegnato dal sistema terrà conto del fascicolo dentro al quale viene creato il sub fascicolo. Tipicamente, la numerazione dei sub fascicoli presenta una forma del tipo:

Classifica: 01-01-02 2009 / 18.3

Dove 01-01-02 rappresenta la cartella di titolario, segue l'anno; 18.3 per indicare il terzo sub fascicolo (3) all'interno del fascicolo 18.

Duplica apre una nuova maschera per la creazione di un nuovo fascicolo, copiando i dati (oggetto, classificazione) dal fascicolo di partenza.

Documenti in Fascicolo apre una maschera con l'elenco dei documenti contenuti nel fascicolo, dalla quale è possibile verificare gli allegati al documento (verifica impronta), aggiungere nuovi documenti al fascicolo o modificare classificazione o fascicolo al/ai documenti selezionati.

Stampa copertina lancia la funzionalità di generazione automatica del pdf riportante i dati del fascicolo, da poter usare appunto come "copertina".

Stampa documenti in fascicolo: genera un pdf contenente i dati dei documenti al momento inseriti nel fascicolo stesso.

Pagina "Smistamenti":

Questa sezione è attiva se l'impostazione generale di "Iter Fascicolare" è attiva a livello di Ente. In questo caso, in questa sezione è possibile inserire smistamenti con le stesse modalità illustrate per la maschera di protocollo nei paragrafi precedenti. Al momento della creazione e numerazione del fascicolo, viene creato uno smistamento automatico all'unità di competenza indicata in maschera. Non è possibile la presenza contemporanea di due smistamenti per competenza: nel caso, il primo deve essere "eseguito", o deve essere effettuato un "inoltro" (cfr. più avanti in questo manuale).

Pagina "Relazioni"

La terza pagina della maschera introduce il concetto di relazione tra fascicoli. Una volta che il fascicolo è stato numerato, è possibile metterlo in relazione con fascicoli precedenti. È possibile inserire relazioni attive o passive: inserendo una relazione attiva verrà creata la corrispondente passiva sul fascicolo collegato, e viceversa. Questo permette di avere un collegamento rapido ai fascicoli collegati a quello in consultazione. Per inserire una relazione è necessario spostarsi nella pagina dedicata della maschera e cliccare il pulsante "Aggiungi" (+) nella sezione delle Relazioni Attive o Passive. Viene aperta una finestra che si presenta come segue:

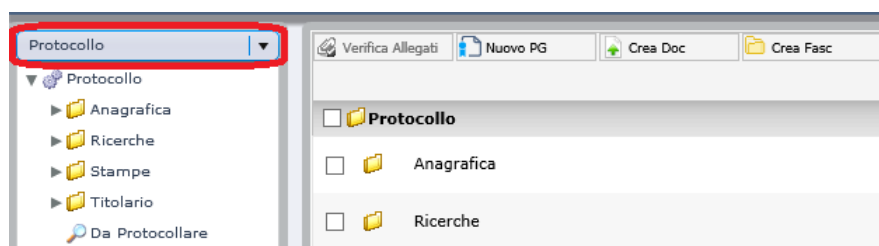
Dal menu a tendina “tipo Relazione” è possibile specificare se si sta inserendo un collegamento generico tra fascicoli (“Collegamento tra Fascicoli”) o una vera e propria relazione “Precedente/Seguente”; in quest’ultimo caso, sarà possibile inserire solo una relazione di questo tipo. Le informazioni sulle relazioni saranno inserite anche nei “collegamenti e riferimenti” dei fascicoli, accessibili da Sistema Documentale.

Pagina “Storico Modifiche”

Allo stesso modo della omonima pagina presente sulle maschere di protocollo, nella nuova maschera del fascicolo è presente una pagina contenente lo storico delle modifiche apportate al fascicolo in consultazione. A partire dalla numerazione, il sistema tiene traccia della situazione precedente e registra data e utente di modifica.

2.3.1 Creazione di fascicoli dall’Area di Lavoro “Titolario”

La funzione “Crea Fascicolo” assume particolarità nel caso in cui la creazione cominci dall’area di lavoro riservata al Titolare. Come prima cosa, è possibile accedere a questa area dall’area Protocollo già vista, tramite il menu a tendina situato in alto nella parte sinistra della finestra:



Tramite questo menu a tendina, è possibile spostarsi alle varie aree di lavoro autorizzate per l’utente, tra cui l’area Titolare. La quantità di voci presenti in questo menu dipende sia dagli applicativi installati, sia dal ruolo assegnato all’utente. Accedendo a quest’area di lavoro l’utente potrà navigare tra le varie cartelle di classificazione e fascicoli che compongono il titolario di classificazione archivistica dell’Ente.

Nella parte centrale della finestra, in alto, è presente la barra funzioni, dove è presente il già incontrato pulsante . La particolarità di accedere alla funzione da una posizione di titolare sta nell’ereditare dalla posizione di creazione la classifica per il nuovo fascicolo. Ad esempio, cliccando il tasto “Crea Fasc” a partire dalla cartella 01-01, nella finestra di creazione che si apre il campo “Classificazione” sarà già valorizzato con i dati relativi.

2.3.2 Creazione di fascicoli dalla maschera di protocollazione

La funzione di creazione di un nuovo fascicolo è richiamabile anche dalla maschera di protocollazione, di modo da poter gestire la necessità del nuovo fascicolo senza necessità di uscire dal documento di protocollo che lo necessita. Per

accedere alla funzione è necessario cliccare sull'icona di ricerca del campo fascicolo (), che apre una pop up dalla quale è possibile ricercare ed inserire il valore selezionato;

A prescindere che la maschera mostri dei risultati, sarà possibile aggiungere un nuovo fascicolo cliccando sul  posto alla destra delle descrizioni dei campi, nella sezione "Seleziona Fascicolo", che apre la maschera di creazione nuovo fascicolo descritta nei paragrafi precedenti.

2.4 Firma di documenti principali da maschera di protocollo

È disponibile la funzione di firma digitale dei documenti principali allegati alle maschere di protocollo. Sarà possibile apporre la firma digitale soltanto prima della protocollazione. Il pulsante  che lancia la funzione è posizionato nella parte inferiore destra della maschera di protocollazione. Solo nel caso sia presente l'allegato principale, e soltanto prima della protocollazione, lancia l'apposita applicazione di firma digitale, nella quale sarà necessario inserire il codice PIN del dispositivo di firma collegato preventivamente. Una volta eseguita l'attività di firma, il sistema riproporrà la maschera di protocollazione con il file firmato e il pulsante di Firma non sarà più visibile. La funzionalità è sensibile a particolare autenticazione gestita su singolo utente.

2.4.1 Verifica della firma digitale e memorizzazione dell'esito

È inoltre disponibile la funzione di memorizzazione della data/ora di verifica della firma digitale, oltre all'esito della verifica stessa. L'informazione della data/ora di verifica viene visualizzata sulla riga corrispondente all'allegato principale.

2.5 Gestione dei documenti da fascicolare

L'applicativo integra nativamente la funzionalità dedicata all'introduzione all'interno del Sistema di Gestione Documentale di documenti che non necessitano di protocollazione. Sarà quindi possibile inserire nel sistema, classificare e/o fascicolare, gestire l'iter documentale su documenti dei quali non si ritenga necessario provvedere alla registrazione nel repertorio ufficiale di protocollo, né in nessun altro repertorio.

In particolare, sarà possibile gestire come documenti non protocollati sia messaggi provenienti da PEC o dall'integrazione con il Fax Server, sia documenti non presenti in nessuna forma nel sistema.

2.5.1 Registrazione di "documenti da fascicolare"

La tipologia rappresentata dai documenti da inserire nel sistema e che non siano precedentemente presenti nel sistema è stata nominata "documenti da fascicolare". Per poter inserire nuovi "documenti da fascicolare", è necessario lanciare l'apposita funzione dal menu a tendina della Smart Desktop. È prevista una nuova maschera dedicata, la quale all'apertura si presenta come nell'immagine seguente; la possibilità di creare documenti di questo tipo è a sua volta dipendente da specifica abilitazione su singolo utente.

I campi disponibili per la registrazione delle informazioni sono:

- Tipo Documento** il campo funziona con la stessa logica e mostra gli stessi campi del corrispettivo sulla maschera di protocollo; non riporta eventuali informazioni sul registro associato al tipo documento.
- Riservato** come per le registrazioni di protocollo, è possibile rendere riservate anche le registrazioni dei documenti classificabili. La logica di visualizzazione dei documenti riservati è analoga a quanto avviene per i documenti protocollati.
- Oggetto** il campo segue la stessa logica dell'analogo campo oggetto sulle maschera di protocollo.
- Classificazione e Fascicolo** è possibile classificare e/o fascicolare i documenti classificabili. Questo permette di renderli visibili all'interno delle cartelle relative del titolare.

Le ulteriori sezioni che compongono la maschera sono:

- Allegati** è possibile inserire file come allegati alle registrazioni dei documenti classificabili, sia direttamente tramite l'esplorazione risorse di Windows, sia tramite scansione ottica interattiva; analogamente a quanto accade nella maschera di protocollo è inoltre possibile inserire "Smistamenti" sui documenti classificabili, gestendo quindi l'iter documentale anche per questa tipologia documentale.
- Riferimenti** è possibile inserire "Classificazioni secondarie", nelle modalità descritte nella analoga pagina sulle registrazioni di protocollo.
- Note** è utilizzabile dall'utente per aggiungere note alla protocollazione, note che saranno poi visibili da questa pagina.

Una volta inserite le informazioni obbligatorie (le quali dipendono dalle stesse impostazioni legate alle registrazioni di protocollo in termini di oggetto, classifica e fascicolo), attraverso il pulsante SALVA posto nella parte inferiore destra della maschera, le informazioni vengono registrate a sistema e vengono istanziati gli eventuali smistamenti. Pur non trattandosi di una registrazione di protocollo, il sistema salva sulla maschera le informazioni legate a data/ora di salvataggio, utente e unità di registrazione.

I documenti classificabili saranno identificabili nel Sistema Documentale da una specifica icona e da uno specifico titolo nel blocco documentale, ad esempio:

Documento del 04/09/2017 12:51:00	
Oggetto:	NOTE INTERNE
Classifica:	01/01 2016 / 1

2.6 Pubblicazione su Albo On Line dalle maschere dei documenti protocollati

L'applicativo integra nativamente la funzionalità che permette la pubblicazione dei documenti protocollati sull'Albo On Line gestito dall'applicativo *AGSME – Gestione Messaggi Notificatori e Albo Pretorio* rilasciato da *Gruppo Finmatica*. La versione minima di *AGSME* per la gestione dell'integrazione è 1.4.1. L'integrazione si realizza con un pulsante presente nelle maschere di protocollo, identificato dalla descrizione "Pubblica all'albo".

Cliccando sul pulsante verrà aperta la relativa maschera per l'inserimento di nuove pubblicazioni, riportando le informazioni presenti nella maschera di protocollo, nel dettaglio:

- ✓ Oggetto della registrazione di protocollo = Oggetto della pubblicazione
- ✓ Riservato sulla registrazione di protocollo = Riservato sulla pubblicazione
- ✓ Tipo documento della registrazione di protocollo = Tipo documento della pubblicazione
- ✓ Mittente se registrazione di protocollo in arrivo = Ente Richiedente della pubblicazione
- ✓ Destinatario se registrazione di protocollo in partenza = Ente Richiedente della pubblicazione.

L'eventuale allegato principale della registrazione di protocollo verrà importato come allegato principale nella pubblicazione; allo stesso modo, eventuali allegati secondari saranno riportati come allegati secondari alla pubblicazione. Dalla maschera di inserimento della nuova pubblicazione così composta sarà possibile inserire le ulteriori informazioni non gestite direttamente da protocollo (ad esempio l'intervallo di pubblicazione) e numerare la registrazione nel registro di Albo Pretorio.

La numerazione nel registro di Albo Pretorio attiverà un collegamento nella cartella "Elenco dei collegamenti e riferimenti per il documento", accessibile dal sistema documentale ed identificata dall'icona 📄, per il singolo documento protocollato pubblicato; questo permetterà di accedere alla registrazione su albo partendo dalla ricerca del documento di protocollo. Eventuali modifiche sulla registrazione di protocollo di un documento già pubblicato all'albo non allineano automaticamente la pubblicazione stessa: un messaggio in questo senso viene dato all'utente all'atto del salvataggio delle informazioni sulla registrazione di protocollo. Sarà comunque sempre possibile accedere alla pubblicazione numerata cliccando la stessa voce di menu "Pubblica all'Albo" del menu funzionalità.

In caso di annullamento della registrazione di protocollo, verrà automaticamente annullata la relativa pubblicazione. Nel caso in cui venga annullata la pubblicazione, il protocollo pubblicato sarà nuovamente pubblicabile con altro numero sul registro di Albo Pretorio.

La funzionalità di pubblicazione all'albo on line è disponibile su tutte le maschere riportanti documenti protocollati (maschera di protocollo, maschera di protocollo di documenti provenienti da interoperabilità, maschera della lettera);

La funzionalità viene abilitata da uno specifico privilegio (PUBALBO), il quale di default viene automaticamente associato ai ruoli per la creazione di nuove registrazioni di Albo Pretorio sull'applicativo specifico; la funzionalità sarà quindi abilitata sulle maschere di protocollo soltanto agli utenti aventi almeno un ruolo nell'applicativo di *Gestione Messaggi Notificatori e Albo Pretorio*.

3 Gestione delle Attività della Smart Desktop

Si è detto poco sopra che al momento in cui viene lanciata dall'utente la protocollazione, il sistema provvede a far partire gli smistamenti associati al documento protocollato. Per gli utenti destinatari degli smistamenti, questo si concretizza con la comparsa sulla propria Smart Desktop di un'attività legata allo smistamento stesso. La situazione che si presenta all'utente destinatario di uno smistamento è la seguente:

Cerca			
		Prendi in carico	Prendi in carico - PG 2019 / 0000299: LETTERA DI COMUNICAZIONE AGGIUDICAZIONE DEFINITIVA
			21/10/2019 11:57:43 19/01/2020 11:57:43
		Prendi in carico	Prendi in carico - PG 2019 / 264 del 27/09/2019 ARRIVO : DOMANDA DI PARTECIPAZIONE AL CONCORSO
			27/09/2019 15:49:43 26/12/2019 00:00:00
		Prendi in carico	Prendi in carico - PG 2019 / 259 del 25/09/2019 ARRIVO : DOMANDA DI ACCESSO AGLI ATTI RICEVUTA DA XXXX
			25/09/2019 16:34:47 24/12/2019 00:00:00

Per ognuna delle attività, oltre ai dati principali che sono specializzati per tipologia di documento, l'utente vede una serie di informazioni accessorie quali: la tipologia, le date di attivazione e di scadenza, un link che direttamente dalla scrivania virtuale permette l'accesso alla pagina applicativa completa in relazione al documento , il pulsante che mostra i dettagli dell'attività da cui possono essere consultati anche gli eventuali allegati presenti e le note inseribili su ciascuna attività grazie alla funzione .

Nei prossimi paragrafi, verranno affrontate le possibilità presenti nell'applicativo per la gestione e il proseguimento degli iter documentali. Si sottolinea che anche per i documenti non protocollati la gestione dell'iter documentale è del tutto simile a quanto verrà mostrato per i documenti protocollati.

3.1 Gestione di un singolo documento

Al momento che l'utente destinatario di smistamento visualizza l'attività relativa al documento protocollato sulla propria scrivania, attività del tipo "prendi in carico", entrando nel documento (attraverso il pulsante) avrà nel menu Funzionalità (Funzionalità...) alcune voci in più, relative alla gestione dell'iter documentale, ovvero dello smistamento stesso.

Nel dettaglio, le voci sono:

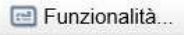
- **Rifiuta Smistamento:** apre una finestra nella quale il destinatario dello smistamento può inserire le motivazioni del rifiuto dello smistamento stesso. L'ulteriore click sul pulsante "Ripudia" creerà un'attività sulla scrivania virtuale dell'unità protocollante relativa alla notifica di smistamento rifiutato, oltre che riportare il motivo inserito.
- **Prendi in carico:** l'attività di presa in carico, riproporrà sulla scrivania virtuale lo stesso documento nello stato "in carico", con possibilità quindi di modifica da parte dell'utente destinatario.
- **Prendi in carico ed inoltra:** apre la maschera per l'inserimento della unità (o unità, o singoli componenti a seconda delle abilitazioni date all'utente) destinataria dell'inoltro. Rispetto ad ulteriore smistamento, con l'inoltro l'attività viene tolta dalla scrivania virtuale di chi inoltra, e vengono anche tolte le competenze di modifica sul documento. Sarà comunque possibile continuare a visualizzare il documento dalle ricerche del Sistema di Gestione Documentale.
- **Prendi in carico ed esegui:** come per Prendi in carico; in più introduce anche l'esecuzione dell'attività, che toglie la stessa dalla scrivania virtuale.

- **Prendi in carico ed assegna:** oltre alla presa in carico, apre una finestra attraverso la quale si ha la possibilità di assegnare ad ulteriori componenti della propria unità. L'attività rimarrà in carico.
- **Prendi in carico, smista ed esegui:** prima di eseguire l'attività (cfr. sopra), apre la maschera per inserire nuovi smistamenti ad altre unità (o singoli componenti a seconda delle abilitazioni date all'utente). La differenza fondamentale con l'inoltro è che ricercando il documento da Sistema di Gestione Documentale l'utente avrà mantenuto i diritti di modifica.

Quindi, le operazioni a disposizione dell'utente si dividono in operazioni che mantengono l'annotazione delle attività sulla scrivania virtuale, e operazioni che "eseguono" direttamente l'attività, eliminando il promemoria dalla scrivania.

Si è detto poco sopra che se viene scelta dal menu la voce "Prendi in carico", l'attività rimane sulla scrivania con lo stato modificato:



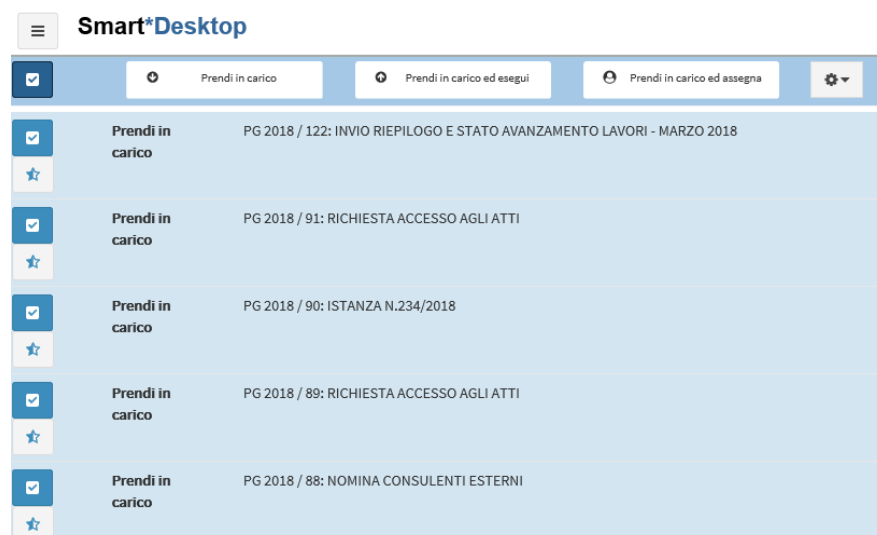
Al momento che, dopo aver eseguito l'operazione di presa in carico, l'utente destinatario di smistamento visualizza l'attività relativa al documento protocollato sulla propria scrivania, attività del tipo "in carico", entrando nel documento (come di consueto, attraverso il pulsante ) avrà nel menu Funzionalità () le voci che seguono. Per il dettaglio si rimanda a quanto scritto poco sopra:

- **Assegna**
- **Inoltro**
- **Esegui**

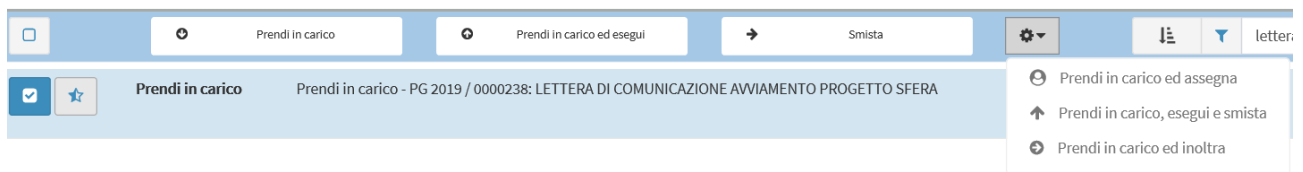
Attraverso queste funzionalità, si ha la possibilità di rimuovere il promemoria dell'attività dalla propria Smart desktop, ovvero dichiarare "eseguita" l'attività legata al documento ricevuto.

3.2 Gestione multipla di documenti

Dalla Smart desktop è possibile effettuare alcune operazioni anche su più documenti contemporaneamente, selezionando una o più attività omogenee per Tipologia con un check sul pulsante , vengono attivati i bottoni per poter eseguire le funzioni contestuali associate.

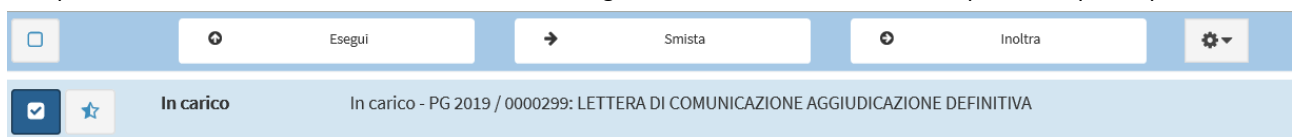


Eventuali ulteriori funzioni associate alla Tipologia, potranno essere raggiunte tramite la funzione 



Ogni attività infine, può essere contraddistinta per priorità: attraverso il pulsante , sarà possibile assegnare una priorità alta , normale  o bassa  da utilizzare anche ai fini dell'ordinamento.

Se il pulsante  viene selezionato su un documento già in carico all'utente, la finestra presenta questa pulsantiera:



Quindi, attraverso le funzionalità della Smart Desktop, l'utente ha la possibilità di avere sempre sotto controllo la situazione relativa alle sue attività, e di permettere il proseguimento degli iter documentali. Man mano che gli utenti effettuano le operazioni di presa in carico, di esecuzione o di inoltra, o aggiungono smistamenti ai documenti, su ogni singolo documento è possibile seguire i passi che il documento ha effettuato. Entrando in visualizzazione sul singolo protocollo, e posizionandosi sulla pagina relativa agli smistamenti, saranno valorizzati in automatico dal sistema i campi descrittivi degli iter seguiti dal documento. Ad esempio:

Corrispondenti					
Smistamenti					
Smistamenti Correnti					
Tipo	Trasmesso	Ufficio/Assegnante	Preso in carico	Assegnato	Eseguito
COMPETENZA	UFFICIO PROTOCOLLO RE NICOLA 21/10/2019 11:57:33	SETTORE AFFARI GENERALI ED ISTITUZIONALI	CECILIJOT CRISTIAN 22/10/2019 10:36:55		
Smistamenti Storici					

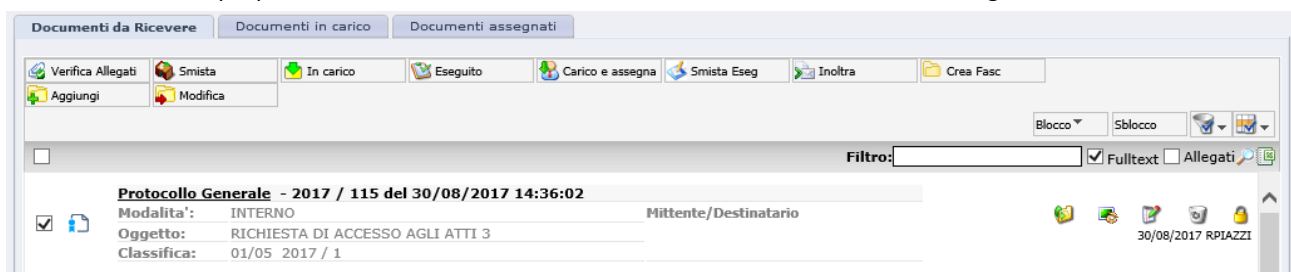
3.3 Gestione dei documenti dal Sistema Documentale: "Iter Documentale"

Nel paragrafo precedente si è vista la gestione delle attività poste sulla scrivania virtuale. È possibile arrivare agli stessi risultati anche dall'area di lavoro "Protocollo", alla quale si accede dal menu a tendina posto nella parte superiore della Smart Desktop. Nella parte sinistra della finestra principale del sistema documentale, come ultima voce è presente "Iter Documentale", la quale si presenta come segue:



Nel caso l'utente sia componente di più unità organizzative, attraverso il menu a tendina "Unità Organizzativa" potrà selezionare l'unità per cui desidera visualizzare gli smistamenti, quindi lanciare la ricerca con l'apposito pulsante.

L'esito della ricerca proporrà l'elenco dei documenti nella visualizzazione consueta, ma integrata nella nuova maschera:

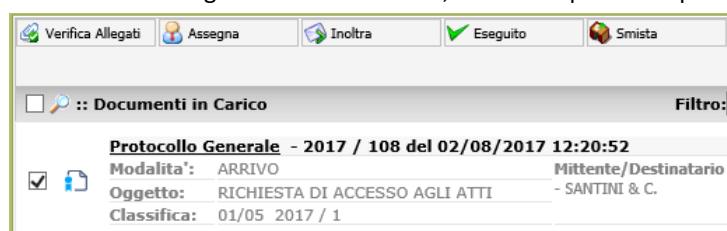


Mantenendo quindi sia la possibilità di visualizzare/modificare il documento attraverso le icone consuete, sia la possibilità di continuare a gestire in multi selezione i documenti presenti nelle viste, con le stesse modalità visualizzate nel paragrafo precedente attraverso gli appositi pulsanti.

Il funzionamento di questi pulsanti è simile ai loro omonimi presenti nella gestione del singolo documento esposta poco sopra. Il dettaglio dei pulsanti:

	"Smista", apre la finestra degli smistamenti, permettendo di aggiungerne ai documenti selezionati.
	"Prendi in carico".
	"Prendi in carico e Assegna".
	"Eseguito", identico a "Prendi in carico e Esegui".
	"Smista e Esegui", identico a "Prendi in carico, Smista e Esegui".
	"Inoltra", identico a "Prendi in carico e Inoltra".

Se la selezione viene attivata sui documenti già in carico all'utente, la finestra presenta questa pulsantiera:



I pulsanti presenti (Assegna, Inoltra, Eseguito, Smista) hanno funzionamento identico a quello dei loro omonimi già incontrati.

3.4 Gestione degli smistamenti dei documenti da fascicolare

Come visto poco sopra, è possibile inserire smistamenti sui documenti da fascicolare, sia per competenza che per conoscenza. L'inserimento dello smistamento porterà alla creazione sulla Smart Desktop degli utenti destinatari delle attività di gestione dell'iter documentale, in modo analogo a quanto succede per gli smistamenti dei documenti protocollati. Le attività relative agli smistamenti dei documenti da fascicolare saranno del tipo "Da ricevere – Documento oggetto del *data di registrazione*". Accedendo da Smart Desktop, saranno presenti le voci per la gestione dell'iter documentale, secondo la stessa logica degli smistamenti dei documenti protocollati:

- Prendi in carico
- Prendi in carico ed inoltra
- Prendi in carico ed esegui
- Prendi in carico ed assegna
- Prendi in carico, smista ed esegui
- Rifiuta smistamento.

Analogamente a quanto previsto sulle maschere dei documenti protocollati, le attività di presa in carico (e eventuali ulteriori) verranno registrate nella maschera del singolo documento. In caso di presa in carico semplice, il documento rimarrà sulla Smart Desktop degli utenti fino a sua esecuzione. È possibile gestire gli iter documentali dei documenti classificabili anche in multi selezione, sia dagli elenchi dei documenti da ricevere per unità della Smart Desktop (check selezione a fianco di ogni documento), sia dalla funzione "Iter Documentale" dell'area di lavoro Protocollo del Sistema di Gestione Documentale.

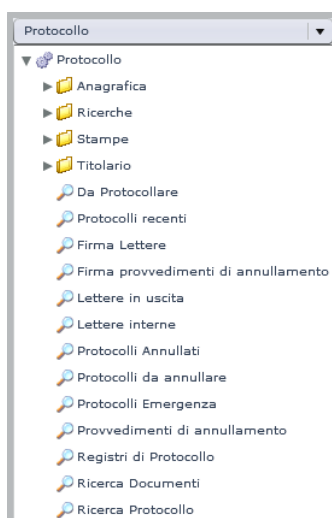
4 Funzioni per la ricerca dei documenti

Una delle principali funzionalità presenti in un applicativo di gestione documentale è sicuramente legata alla possibilità di ricercare e di avere un accesso rapido ai documenti precedentemente inseriti. L'applicativo qui presentato ha integrato un numero notevole di ricerche, che permettono all'utente di effettuarle a partire dai campi più svariati presenti nelle varie maschere di creazione documenti.

In linea di principio generale, esistono due tipologie distinte di ricerche:

- Ricerche preimpostate (e che quindi restituiscono già risultati senza necessità di ulteriori inserimenti di dati da parte dell'utente; queste sono dette "query")
- Ricerche parametriche (e che quindi restituiscono una maschera all'interno della quale l'utente deve inserire almeno un dato perché la ricerca abbia senso).

Per avere accesso alle ricerche è necessario posizionarsi nell'area di lavoro del sistema documentale, tramite il menu a tendina presente nella parte inferiore della scrivania virtuale, selezionando quindi "Protocollo". Nella parte sinistra della finestra dell'area di lavoro, dove è presente la struttura ad albero, si trovano le "lenti" () , cliccando sulle quali si accede alle varie funzionalità di ricerca. In particolare, le voci "Da Protocollare" e "Protocolli Recenti", ad esempio, sono ricerche preimpostate (query):



Le query sono ricerche mirate a velocizzare alcune funzioni utili agli utenti del sistema. Ad esempio, la prima “lente” ( Da Protocollo) rende nella parte centrale della finestra i documenti salvati dall’utente e non ancora protocollati. Analogamente, le altre query restituiscono nella parte centrale della finestra i risultati coincidenti con la ricerca impostata.

All’interno della cartella “Ricerche” ( Ricerche) è possibile trovare ulteriori maschere di ricerca, ovvero quelle finestre che permettono all’utente di andare ad affinare le ricerche stesse per vari campi tra quelli presenti nei documenti creati. Le maschere di ricerca a disposizione sono mostrate nell’esempio poco sotto; per accedere ad una maschera di ricerca, è sufficiente cliccare la “lente” () di riferimento.



Sono presenti ricerche generiche (per esempio, le ricerche di classificazioni, fascicoli o protocolli) e alcune ricerche sui protocolli incentrate su campi specifici (per esempio, a partire dal dato relativo allo smistamento del protocollo).

Per quanto riguarda la compilazione dei campi che le compongono, le maschere di ricerca seguono una logica simile alle maschere di inserimento documenti che sono già state presentate in questo manuale. Ad esempio, nell’immagine che segue è rappresentata la maschera di ricerca generica sui documenti protocollati ( Ricerca Protocollo):

Ricerca documenti di protocollo

Dati			
Anno	2014	Data Protocollo	dal al
Numero	dal al	Data Arrivo	dal al
Doc. Esterno		Data Doc.	dal al
Modalita'	☐ ARRIVO ☐ INTERNO ☐ PARTENZA		
Registro	Protocollo Generale		
Protocollato da			
Ufficio esibente			
Utente			
Tipo Doc.			
Tramite			
Classificazione		Fascicolo	/
Oggetto			
Note			

Dati Emergenza	
Numero	dal al Registro

Per eseguire la ricerca basta compilare anche un solo campo fra quelli proposti; è chiaro che più informazioni si immettono, più sarà possibile rifinire la ricerca. Le icone che sono presenti accanto ai vari campi sono già comparse altrove nell'applicativo; in ogni caso sono:



pop up generica, apre una maschera di ricerca relativa al campo al quale è legata. Ad esempio, cliccando sulla pop up accanto al campo "Classificazione", viene aperta la maschera di ricerca che permette di ricercare all'interno del titolario la classificazione desiderata, in modo analogo alla scelta della classificazione che si effettua nella maschera di inserimento protocollo.



pop up di calendario, presente ogni qual volta il campo sia di tipo "data". Apre una finestra con un calendario attraverso la quale è possibile scegliere la data desiderata.



permette di cancellare quanto inserito nel campo a cui fa riferimento.

Dopo aver compilato i campi di interesse, è possibile lanciare le ricerche tramite l'apposito pulsante **Ricerca**, presente nella parte inferiore della finestra. I risultati verranno mostrati dal sistema nella parte centrale della finestra.

In dettaglio le principali ricerche presenti:



Ricerca Classificazioni:

permette di ricercare all'interno delle cartelle di titolario per visualizzare classificazioni.



Ricerca Fascicoli:

affina la ricerca precedente permettendo la ricerca dei fascicoli presenti nelle cartelle di titolario.



Ricerca Protocolli non Fascicolati:

permette di ricercare tra i documenti protocollati quelli che non sono stati fascicolati; la ricerca è possibile a partire dai documenti di protocollo creati dall'utente stesso.



Ricerca Protocollo:

è la ricerca generica mostrata poco sopra.



Ricerca Protocollo Amm/AOO:

permette di ricercare tra i documenti protocollati specializzando la ricerca inserendo la denominazione dell'Amministrazione/Area Organizzativa Omogenea mittente o destinataria del documento.



Ricerca Protocollo Smistamento:

permette di ricercare tra i documenti protocollati specializzando la ricerca specificando dati di trasmissione degli smistamenti (ufficio trasmittente/ufficio ricevente), il tipo di smistamento

(competenza/conoscenza) e lo stato del documento (da prendere in carico/in carico/eseguito).



permette di ricercare tra i documenti protocollati specializzando la ricerca inserendo mittente/destinatario del documento.

È possibile avere accesso alle ricerche appena presentate anche dall'area di lavoro Titolare: le ricerche saranno accessibili sempre nella parte destra dell'area di lavoro, sotto le cartelle di classificazione.

4.1 Stampa dei registri di protocollo generale e dei fascicoli

Il sistema prevede la possibilità di predisporre report parametrici in base alle specifiche esigenze di verifiche e statistiche sulle registrazioni di protocollo gestite dall'Ente, con possibilità di definizione da parte degli utenti di date specifiche o periodi temporali e altre variabili di selezione (es.: selezione campi manuale). Le stampe vengono elaborate previo indicazione, da parte dell'utente, dei parametri di riferimento per la singola estrazione ed il risultato dell'elaborazione viene filtrato in base alle competenze di visibilità dei dati e/o dei testi da parte del singolo utente. In particolare il sistema consente la produzione di report specifici quali la stampa del registro, la stampa del titolare, la stampa del contenuto dei fascicoli (in termini di voci di classificazione e di documenti), la stampa dei documenti per smistamento, la stampa di elenchi di mittenti e destinatari, ecc. Il sistema consente di esportare in file in formato aperto il risultato di tutte le ricerche effettuate dall'utente e l'elenco delle attività presenti sulla "Scrivania Virtuale" del singolo utilizzatore.

5 Classificazione dei documenti da fascicolare

5.1 Aggiunta di una Classificazione Secondaria

Nel capitolo dedicato alla funzionalità di protocollazione dei documenti, si è visto come una sezione della maschera riguardi i dati archivistici, ovvero classificazione e fascicolo.

Si è anche accennato alla pagina "Posizioni Archivistiche secondarie", la quale compare su ogni documento dal momento della creazione in avanti: in questa pagina è appunto possibile attivare la funzionalità di inserimento della posizione archivistica secondaria nella sezione "Riferimenti".

Dal dettaglio "Posizioni Archivistiche secondarie", cliccando il pulsante (+) il sistema proporrà una maschera di ricerca per classifiche e fascicoli; compilando i campi e cliccando "Cerca", il sistema renderà i risultati compatibili con i dati inseriti:

La maschera visualizzata è intitolata "Selezione Fascicoli/Classificazioni".

Campi di input:

- Classificaz. 010
- Descrizione
- Anno Fascicolo: 2018
- Numero
- Oggetto

Opzioni:

- ☒ Aperte
- ☐ Solo Classificazioni
- ☒ Aperti

Pulsante: Cerca

Area di risultati:

Aggiungi Fascicoli/Classificazioni

Risultato ricerca

010: 2018 / 1 TRASMISSIONE ATTI

Classifiche/Fascicoli selezionate

Pulsanti di navigazione: >>, >, <, <<

Pulsanti in basso: Salva e Chiudi, Chiudi

Trascinando la voce desiderata nella parte destra della finestra (oppure usando le frecce <,>,>>,<<) e cliccando successivamente su “Salva e Chiudi”, il sistema aggiungerà la classificazione secondaria al documento di partenza.

Sarà possibile ricavare il dato relativo alle classificazioni accedendo al collegamento “Elenco di collegamenti per il documento” (📁), presente accanto ad ogni documento nella finestra principale del sistema documentale:

Protocollo Generale - 2017 / 108 del 02/08/2017 12:20:52

☐  **Modalità:** ARRIVO **Mittente/Destinatario**        04/09/2017 LTRABUCCHI

Oggetto: RICHIESTA DI ACCESSO AGLI ATTI - SANTINI & C.

Classifica: 01/05 2017 / 1

Si aprirà una finestra che mostrerà i dati relativi a classifica primaria e, se presente, classifica secondaria:

Collegamenti **Riferimenti**

Elenco Cartelle Collegate al Documento n: 3279070

Filtra Collegamenti: TUTTI

Cartelle

 01/05 - 2017 / 1 **Stato:** Corrente **Anno Archiviazione:** 2017
Oggetto: FASCICOLO ARCHIVISTICO
 inserito da RIZAL01 il 02/08/2017

 01/03 - STATUTO
 Valida dal: 01/01/2005 al: In Uso: SI
 inserito da LTRABUCCHI il 04/09/2017

Cliccando sulle cartelle relative (📁) il sistema provvederà ad aprire il sistema documentale posizionato nell'area di lavoro Titolario, evidenziando nella parte centrale della finestra il contenuto del fascicolo o della classifica cliccata.

5.2 Modifica del dato di Classificazione

Si è poi detto del pulsante “Modifica” (📁 Modifica), presente nella barra funzioni del sistema documentale (cfr. 1.2.1); il pulsante dà la possibilità all'utente di modificare la posizione archivistica primaria di un documento protocollato. Cliccando il pulsante, il sistema rende una maschera di ricerca simile a quella presente per il tasto “Aggiungi”:

Ricerca Classificazione/Fascicolo

Classificazione		Stato	Aperte ▼
Descrizione			
Anno Fascicolo		Numero	
Oggetto			
Stato	Aperti ▼	Ricerca su TUTTO il Titolario	NO ▼
Cerca			

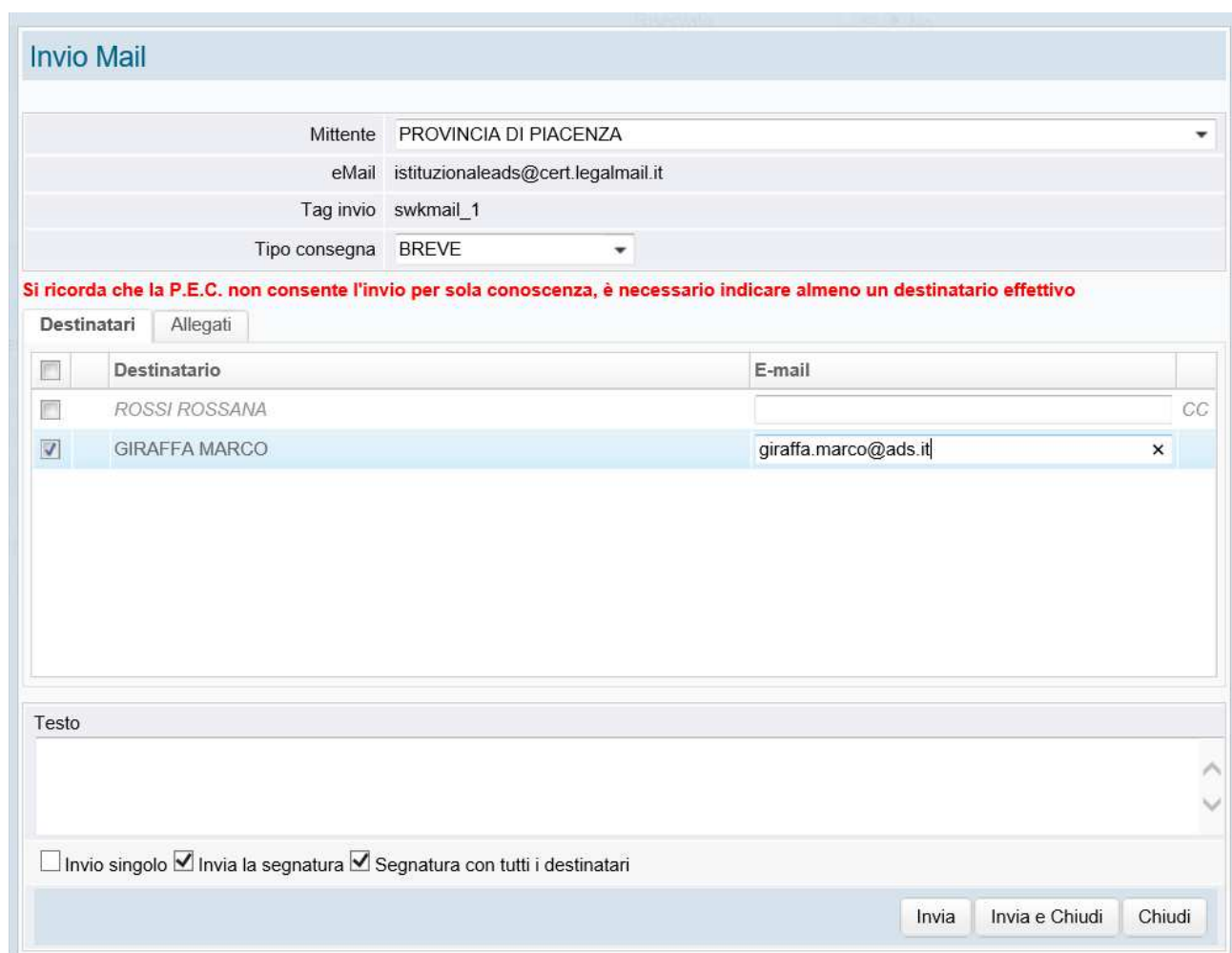
Inserendo i dati e cliccando “Cerca”, il sistema renderà nella parte inferiore della finestra i risultati attinenti. Selezionato il desiderato, per cambiare la classifica al documento è sufficiente cliccare il tasto  **Modifica**, posto nella barra nella parte superiore della finestra. L'operazione permette di agire anche in multiselezione, andando quindi a modificare la posizione archivistica primaria di più documenti con un'unica azione.

6 Invio di documenti protocollati tramite PEC

L'applicativo integra un motore di invio e scarico della Posta Elettronica Certificata; secondo le volontà di configurazione dell'Ente, soltanto alcuni utenti con particolari privilegi avranno accesso alle funzioni di scarico e invio della posta. Particolarmente ogni utente potrà gestire, se opportunamente configurate le abilitazioni, accedere all'invio dei documenti protocollati o attraverso la casella istituzionale o attraverso caselle collegate alla propria unità organizzativa.

Per le metodologie di gestione degli allegati e del documento principale si faccia riferimento a quanto già esposto in questo manuale, nel paragrafo 2.1.

Dopo aver provveduto alla protocollazione, il sistema renderà accessibile la voce del menu Funzionalità ( Funzionalità...) "Invia PEC": richiamata, il sistema propone una nuova finestra nella quale è possibile visualizzare ed eventualmente integrare i dati relativi agli indirizzi di posta elettronica dei destinatari; nonché specificare se tutti i destinatari riceveranno la comunicazione tramite e-mail:



Si può quindi scegliere se integrare i dati, eventualmente apportare correzioni. Nella sezione inferiore della maschera, nella casella con titolo "Testo", è possibile inserire un testo libero che diverrà il vero e proprio testo della mail.

Per inviare effettivamente il messaggio di posta elettronica, è sufficiente cliccare il tasto "Invia".

È presente anche il pulsante "Invia e Chiudi", che permette di eseguire invii singoli senza la necessità di riaprire la maschera specifica, evidenziando quanto già spedito con l'operazione precedente.

Nella registrazione di protocollo relativa, verrà creata dal sistema una nuova sezione accessibile dal pulsante “Invio PEC” posto a sinistra della maschera del protocollo; nella nuova pagina verranno registrati i dati relativi agli esiti dell’invio, man mano che questi verranno resi disponibili dal servizio di Posta Elettronica Certificata:

The screenshot shows the 'Invio Pec' interface. On the left is a sidebar with icons for 'Compendio', 'Allegati', 'Riferimenti', 'Invio Pec' (highlighted with a red box), 'Note', and 'Storico'. The main area is titled 'Invio Pec' and contains two sections: 'Dettagli PEC' and 'Mail Inviato'. The 'Dettagli PEC' section shows a table with columns: Denominazione, E-mail, Consegna, Mancata Consegna, Conferma Ricezione, and Notifica Eccezione. The 'Mail Inviato' section shows a list of sent messages, including one with the subject '(Rif. 2019/483 PROT) INVIO DOCUMENTAZIONE CC - Inoltrato a casella per invio - Spedito il 22/10/2019 14:25:27'.

Tra le informazioni visualizzabili nella pagina, viene aggiunta l’informazione di data e ora di effettivo invio del messaggio, visualizzabile nella parte inferiore della maschera (Mail Inviato), sulla destra di ogni singolo invio eseguito.

6.1 Invio convocazione gara – oscuramento destinatari

In seguito a segnalazioni riguardanti la necessità che i destinatari di un invio di protocollo tramite PEC non vedano gli altri destinatari, è presente un’apposita funzione, in modo da poter scegliere se inviare la segnatrice completa di tutti i destinatari di protocollo, o se inviare segnatrice che oscura ai singoli destinatari gli altri invitati.

La nuova funzione è selezionabile direttamente dalla maschera di invio PEC, nella parte inferiore.

È possibile definire la gestione separata dei destinatari in segnatrice anche attraverso la creazione di un tipo di documento specifico. Nella maschera di creazione del tipo documento, nella pagina “Dati Protocollo”, è stato aggiunto il valore per la funzionalità:

Con segnatrice: ☒ Sì ☐ No

Dove il check su “Sì” provvederà a creare, in caso di invio, la segnatrice standard completa di tutti i destinatari. Se il check viene salvato su “NO”, in caso di invio separato la segnatrice conterrà solo i destinatari effettivamente selezionati per l’invio, e non tutti i destinatari del protocollo. In altre parole, per poter gestire l’invio a, ad esempio, 2 destinatari diversi con segnatrice che non contengano le informazioni dell’altro destinatario, sarà necessario provvedere a due invii distinti, selezionando un solo destinatario alla volta (checkbox “Mail” posto accanto ad ogni nominativo).

6.2 Multiselezione dei destinatari

La maschera di invio PEC permette di selezionare per invio PEC tutti i destinatari presenti sulla registrazione attraverso l’apposito check (seleziona tutti/deseleziona tutti) posto in alto, sopra ai “Destinatari”:

The screenshot shows the 'Destinatari' section of the 'Invio Pec' interface. It features a table with columns: Destinataro, E-mail, and a checkbox column. The first row has a checkbox checked (highlighted with a red box), followed by 'ROSSI ROSSANA' and 'rossi.rossana@ads.it'. The second row has a checkbox checked, followed by 'GIRAFFA MARCO' and 'giraffa.marco@ads.it'. There is also a 'CC' column.

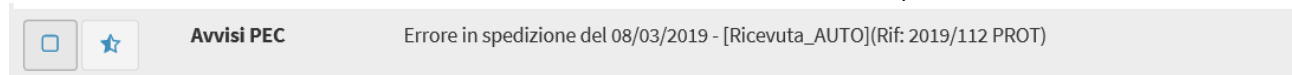
Si ricorda che per attivare l’effettivo invio tramite Posta Elettronica Certificata, è necessario che il checkbox accanto ad almeno un indirizzo sia selezionato.

6.3 Notifica su Smart Desktop in caso di mancato invio tramite PEC

L'applicativo gestisce l'invio di notifiche su Scrivania Virtuale nel caso in cui l'invio tramite PEC non vada a buon fine. Le notifiche arrivano sulla Smart Desktop dell'utente protocollatore del documento, e vengono generate nei seguenti casi:

- Mancata spedizione della e-mail per problemi sul Communication Server interno al sistema;
- Ricezione di avvisi di Mancata Accettazione da parte del server gestore della propria PEC;
- Ricezione di avvisi di Mancata Consegna da parte del server gestore della PEC del destinatario.

Le attività hanno la forma *TIPOLOGIA PROBLEMA: OGGETTO DELLA MAIL*, ad esempio:



Accedendo con il fulmine all'attività, l'utente apre una finestra di dettaglio del problema e ha la possibilità di aprire il documento dal pulsante "Dettagli" per verificare, ad esempio, la corretta sintassi dell'indirizzo del destinatario, o ulteriori problematiche:

Attività TODO

Errore in spedizione del 08/03/2019 - [Ricevuta_AUTO](Rif: 2019/112 PROT)
it.finmatica.comm.MessagingException: Exception reading response

[Chiudi](#)[Dettagli](#)[Fatto](#)

Il pulsante "Fatto" permette di togliere l'attività dalla Smart Desktop; il pulsante "Chiudi" chiude la maschera senza effetti sull'attività stessa.



GRUPPO FINMATICA



Affari Generali

Prisma - Gestione Protocollo Informatico

Novità e migliorie della versione 4.1

Indice

1	Variazioni Generali	3
2	Iter Documentale	3
2.1	Documenti da ricevere.....	4
2.2	Documenti in carico	6
2.3	Documenti assegnati	7
3	Gestione Titolario	7
3.1	Area di lavoro Titolario	8
3.2	Classificazioni	12
3.2.1	Fascicoli	12
3.2.2	Storico	13
3.3	Fascicolo.....	13
3.3.1	Documenti in fascicolo	15
3.3.2	Elenco Sub	15
3.3.3	Relazioni	16
3.3.4	Storico Modifiche	16
4	Gestione PEC.....	18
4.1	Messaggi in Arrivo	18
4.2	“Da Protocollare”	22
4.3	Ricezione e gestione dei messaggi	22
4.3.1	Messaggi indesiderati	25
4.3.2	Consultazione messaggio protocollato e riferimenti	26

1 Variazioni Generali

La release in oggetto dell'applicativo *Prisma – Gestione Protocollo Informatico* prevede il rifacimento di alcune funzionalità applicative che sono state completamente ridisegnate, sia in termini grafici che funzionali, adeguandosi alle novità stilistiche ed ergonomiche già viste sulle maschere di protocollo del progetto evolutivo Prisma 4.0. Pur mantenendo le logiche di presentazione delle funzioni e l'organizzazione generale delle maschere, la nuova versione di Prisma supera l'utilizzo della tecnologia basata su Adobe Flash, introducendo quindi una nuova interfaccia più performante e compatibile con tutti i browser di ultima generazione.

Nei prossimi paragrafi sono presenti i dettagli delle funzionalità utente rese disponibili.

2 Iter Documentale

Nell'ambito del processo di miglioramento evolutivo dell'intero applicativo di Protocollo, nella versione in oggetto viene introdotta una nuova maschera dedicata alla funzionalità di gestione dell'Iter Documentale, come detto in precedenza nonostante la maschera sia stata ridisegnata completamente, si sono mantenute le principali logiche di utilizzo.

La funzione Iter Documentale è accessibile tramite il link presente nell'area di lavoro "Protocollo" del Sistema Documentale. Ricordiamo che la particolarità di gestire gli smistamenti tramite questa funzione, risiede nel poter determinare l'unità organizzativa per la quale visualizzarli: mentre su Smart*Desktop le attività sono aggregate per utente, in modo trasversale rispetto alle unità organizzative per le quali l'utente stesso è abilitato, in Iter Documentale è l'unità organizzativa ad essere aggregante, e quindi a partire da questa verranno visualizzati gli smistamenti.

Nella nuova maschera sarà innanzitutto necessario selezionare l'Unità Organizzativa per la quale si intende

operare: nel caso in cui l'utente faccia parte di più unità organizzative bisognerà sceglierla dall'apposito menù a tendina presente sul campo. Se si fa parte di più unità organizzative è possibile scegliere l'Unità Organizzativa che verrà mostrata di default: questa configurazione può essere impostata dalle Preferenze per utente attivabile cliccando sul proprio nominativo utente e selezionando l'unità per la Preferenza "Unità iter".

Oltre che per unità organizzativa destinataria dello smistamento, gli smistamenti stessi sono organizzati per stato: la pagina è quindi divisa in Documenti da ricevere, Documenti in carico e Documenti Assegnati.

2.1 Documenti da ricevere

In questa sezione sono visibili i documenti da prendere in carico per l'Unità Organizzativa precedentemente selezionata.

L'icona a sinistra accanto a ciascuna registrazione identifica la tipologia a cui il documento appartiene, di seguito le possibili categorie:

- protocollo manuale;
- protocollo da interoperabilità;
- lettera;
- messaggio pec;
- documento da fascicolare.

L'icona graffetta eventualmente presente accanto ai documenti, permette di accedere ai file allegati alla registrazione.

Iter Documentale

Unità Organizzativa: SETTORE AGRICOLTURA

Documenti Da Ricevere | Documenti In Carico | Documenti Assegnati

<< < 1 / 1 > >>            

Documento	File
Protocollo Generale - 2020/1 del 09/01/2020 11:51:29 Oggetto: RICHIESTA DI ACCESSO AGLI ATTI Classifica: 01-04 - INCARICHI DIRIGENTI	
Protocollo Generale - 2019/393 del 20/12/2019 10:10:22 Modalità: ARRIVO Oggetto: DOMANDA DI ACCESSO AGLI ATTI RICEVUTA DA ANTONI FILIPPO - DICEMBRE 2019 Classifica: 01-03 - ARCHIVIO GENERALE	Mittente/Destinatario - ANTONI FILIPPO a.lazzarini@ads.it
Protocollo Generale - 2019/272 del 09/10/2019 09:47:23 Modalità: PARTENZA Oggetto: INVIO DOCUMENTAZIONE Classifica: 01-01 - STEMMI E GONFALONE	Mittente/Destinatario - ADS AUTOMATED DATA SISTEM a.lazzarini@ads.it

La funzione per scorrere tra le pagine di cui è formato l'elenco dei documenti è rappresentata dalle frecce

nella bottoniera orizzontale  è possibile inoltre indicare una pagina specifica per posizionarsi puntualmente su di essa. A seguire è presente il bottone di Refresh per aggiornare le

informazioni della pagina  su cui si è posizionati. L'icona Modifica  apre in modifica i documenti specifici se l'utente ha ruolo o competenze specifiche sul documento selezionato.

La bottoniera include per ultimo, un campo di ricerca per numero protocollo o per oggetto o parte di esso.



La selezione con l'apposito flag sulla colonna di sinistra, di uno o più documenti in multiselezione, attiverà una serie di bottoni relativi alle funzioni che di seguito vengono elencate:



Smista: permette di aggiungere uno o più smistamenti in competenza (solo se si hanno già i diritti di modifica sul documento) o conoscenza.



Prendi in carico: valorizza le informazioni di presa in carico sui documenti selezionati modificando lo stato del documento.



Prendi in carico ed Esegui: permette la contestuale valorizzazione sia delle informazioni di presa in carico che di esecuzione sui documenti selezionati, chiudendo di fatto lo smistamento e settando lo stato dello stesso ad "Eseguito", togliendo quindi i documenti dalle pagine di Iter documentale e della Smart*Desktop.



Prendi in carico ed Assegna: oltre a dichiarare la presa in carico, apre l'elenco degli utenti dell'unità destinataria dello smistamento, permettendo di assegnare la lavorazione ad uno o più componenti, togliendo l'attività dalle Smart*Desktop degli utenti non selezionati. Questi ultimi non perdono le competenze sul

documento assegnato a colleghi, possono infatti ritrovare il documento tramite le ricerche del sistema. Ad ogni utente assegnatario verrà creato uno smistamento dedicato, di modo che le successive esecuzioni possano essere gestite autonomamente.



Prendi in carico Smista ed Esegui: in questo caso oltre a dichiarare la presa in carico del documento, dopo aver selezionato tramite la maschera dedicata un nuovo smistamento, si provvede ad eseguire lo smistamento di partenza, valorizzando i dati di esecuzione, oltre che presa in carico, ed eliminando le notifiche sia da Iter Documentale che da Smart*Desktop.



Prendi in carico e Inoltra: oltre alla presa in carico dei documenti selezionati, viene proposta la maschera per la scelta di una o più nuove unità di destinazione; a differenza di quanto avviene con le funzionalità che inseriscono nuovi smistamenti, come Prendi in carico e smista o Prendi in carico smista ed esegui, viene eseguito un inoltra: se lo smistamento di partenza è per competenza, gli utenti dell'unità che esegue l'inoltra perdono i diritti di modifica del documento così trattato, mantenendo soltanto i diritti di visualizzazione tramite ricerca. Anche con questa funzione la notifica dello smistamento scompare sia da Iter documentale, che da Smart*Desktop. L'attività di Presa in carico del documento sarà spostata tra gli Smistamenti Storici del protocollo selezionato, verificabile attraverso l'apposita sezione presente sugli Smistamenti.

Oltre alle funzionalità relative alla gestione dell'iter documentale, ve ne sono alcune altre che potranno essere abilitate solo se l'utente è stato profilato con determinati ruoli di procedura:



Crea Fascicolo: apre la maschera dedicata per la creazione di un nuovo fascicolo, le funzionalità saranno affrontate in dettaglio nel prossimo paragrafo.



Aggiungi il documento in Classifica o Fascicolo: permette di associare ai documenti selezionati ulteriori posizioni archivistiche classificate come secondarie.



Modifica Classifica o Fascicolo principale: consente di modificare la posizione archivistica primaria eventualmente già presente sul documento o sui documenti selezionati.

2.2 Documenti in carico

In questa sezione vengono elencati i documenti in carico per l'unità selezionata.

Iter Documentale

Unità Organizzativa: SETTORE AGRICOLTURA

Documenti Da Ricevere | Documenti In Carico | Documenti Assegnati

Documenti In Carico

Documento	Mittente/Destinatario
Protocollo Generale - 2020/306 del 23/09/2020 16:17:44 Modalità: ARRIVO Oggetto: DOMANDA DI ACCESSO AGLI ATTI RICEVUTA DA CECILIO T Classifica: 01-03 - ARCHIVIO GENERALE	- ADS - Data Processing - Systematica S.r.l.
Protocollo Generale - 2020/304 del 22/09/2020 17:59:16 Modalità: ARRIVO Oggetto: DOMANDA DI ACCESSO AGLI ATTI RICEVUTA DA CC 1 Classifica: 01-03 - ARCHIVIO GENERALE	- ADS - Data Processing - Systematica S.r.l.

In aggiunta ai bottoni comuni alla sezione precedente, alla quale si rimanda per il dettaglio, troviamo le funzionalità specifiche per questa pagina:



Assegna: la funzione permette di assegnare i documenti selezionati in elenco ai componenti dell'unità destinataria dello smistamento. L'attività di assegnazione del documento farà sì che ciascun assegnatario possa trovare la propria attività su Smart* Desktop ed eseguire l'attività in autonomia.



All'assegnazione è possibile associare una nota indirizzata al destinatario utilizzando l'apposita icona.

I componenti dell'unità assegnataria non selezionati in maschera avranno comunque diritti di modifica sul documento ma non ritroveranno più l'attività su Smart*Desktop nella sez. In Carico e dovranno ricercarlo utilizzando le apposite query su Gestione Documentale.



Esegui: permette di valorizzare la data di esecuzione dell'attività togliendo le notifiche da Iter Documentale e Smart*Desktop. L'unità di esecuzione non perde i diritti in modifica sul documento, anche in questo caso scompariranno le notifiche su Iter Documentale e Smart*Desktop.



Inoltra: l'unità che inoltra il documento smistato per competenza, ad altra unità e/o a componenti della struttura organizzativa, perde i diritti di modifica sul documento, sarà sempre possibile ricercarlo e visualizzarlo tramite le apposite query di ricerca da Gestione Documentale. La funzione di Inoltro ha anche l'effetto di ripulire dalle notifiche sia Smart*Desktop che Iter Documentale.

2.3 Documenti assegnati

In questa pagina vengono elencati i documenti che sono stati assegnati per la lavorazione all'utente ma che in ogni caso restano di competenza all'unità di appartenenza. Su Smart*Desktop la notifica ricevuta dall'utente per questi documenti avrà la descrizione principale: 'Assegnato'. L'utente che abbia compiuto



l'attività assegnata può eseguirla con l'apposita icona ed eliminare così la notifica sulla propria scrivania. Per il significato dei bottoni e delle varie funzioni si rimanda alle sezioni viste in precedenza.

Iter Documentale

Unità Organizzativa: SETTORE AGRICOLTURA

Documenti Da Ricevere | Documenti In Carico | Documenti Assegnati

1 / 1

Documento	Mittente/Destinatario
Modalità: ARRIVO Oggetto: DOMANDA DI ACCESSO AGLI ATTI RICEVUTA DA ANTONI FILIPPO Classifica: 01-03 - ARCHIVIO GENERALE Protocollo Generale - 2019/370 del 06/12/2019 12:25:50	- ANTONI FILIPPO f.antonio@ads.it
Modalità: ARRIVO Oggetto: DOCUMENTAZIONE RICHIESTA Classifica: 01-01 - STEMMI E GONFALONE Protocollo Generale - 2019/368 del 06/12/2019 12:13:49	- GRUPPO FINMATICA:AOO:AOO GRUPPO FINMATICA istituzionaleads@cert.legalmail.it
Modalità: PARTENZA Oggetto: DOCUMENTAZIONE RICHIESTA N.33 Classifica: 01-03 - ARCHIVIO GENERALE Protocollo Generale - 2019/368 del 06/12/2019 12:13:49	- GRUPPO FINMATICA:AOO:AOO GRUPPO FINMATICA istituzionaleads@cert.legalmail.it
Modalità: PARTENZA Oggetto: COMUNICAZIONE URGENTE Classifica: 01-03 - ARCHIVIO GENERALE Protocollo Generale - 2019/293 del 21/10/2019 09:04:40	- ROSSI MARCO

3 Gestione Titolario

Nella versione in oggetto viene introdotta una nuova funzionalità per la gestione del Titolare,



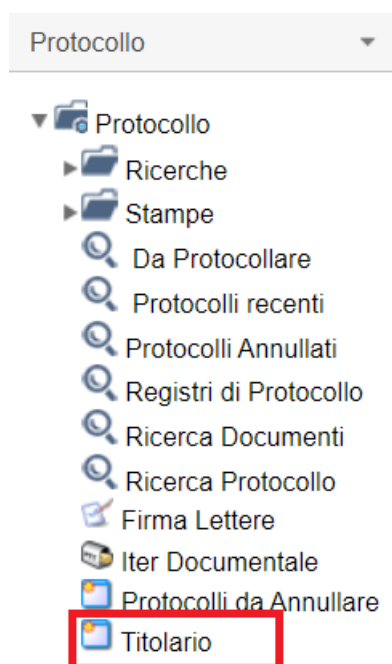
contestualmente a questo vengono rese disponibili le nuove maschere relative alla gestione delle classificazioni e dei fascicoli.

3.1 Area di lavoro Titolare

La nuova area di lavoro è accessibile selezionando il link “Titolario” presente nel menù della sezione Protocollo accessibile da Smart*Desktop



oppure nell'area di lavoro Protocollo del sistema di Gestione Documentale.



La nuova funzionalità è accessibile a tutti gli utenti e permette di consultare il titolario di classificazione attualmente in uso.

Nella prima sezione in alto sono visibili i campi su cui è possibile effettuare delle ricerche puntuali sia sulle classificazioni che sui fascicoli.

Gli utenti abilitati con appositi privilegi, avranno disponibile tra i parametri di ricerca il campo 'Titolario valido al' che gli permetterà di consultare i dati storici, visualizzando le voci di classifiche aperte alla data di riferimento indicata.

Si potrà ricercare le classifiche per codice (o parte di esso) e per Descrizione (o una sua parte). Il pulsante Ricerca avvierà la ricerca delle classifiche secondo i criteri scelti. Ulteriori criteri di ricerca delle classifiche si trovano sul pulsante Filtri: con questa funzione è possibile ricercare per intervalli di data apertura e data di chiusura di singole classificazioni oppure specificare se si intende ricercare solo le classifiche contenitori di documenti o meno (generalmente per es. le classifiche che non sono contenitori di documenti sono quelle di primo livello nella struttura del Titolario).

La sezione "Ricerca Fascicoli" sarà abilitata solo dopo aver selezionato una classifica di riferimento e verrà eseguita sui fascicoli aperti. I possibili campi di ricerca sono quelli relativi all'intervallo di anno del fascicolo,

numero fascicolo, oggetto (o una parte di esso), Ufficio Competente che potrà essere ricercato per codice o descrizione e scelto dall'apposito menù a tendina.

Ricerca Fascicoli			
Anno:	2020	-	2020
Numero:	1	-	50
Oggetto:			
Uff. Competente:			
Fascicoli:	☒ Aperti		
			Ricerca

Gli utenti abilitati con appositi privilegi, avranno a disposizione un ulteriore parametro di ricerca costituito dallo stato: Aperti, Chiusi, Futuri (con data fascicolo successiva alla data odierna) e Tutti. L'apposito pulsante Ricerca permetterà la visualizzazione dei fascicoli estratti con i parametri scelti.

Ricerca Fascicoli			
Anno:	2015	-	2016
Numero:		-	
Oggetto:	STRADA COMUNALE		
Uff. Competente:	LAVORI PUBBLICI		
Fascicoli:	☐ Aperti ☒ Chiusi ☐ Futuri ☐ Tutti		
			Ricerca

Il Titolario è rappresentato da una struttura ad albero di classificazioni, ciascuna classifica viene identificata da codice classifica – descrizione - data di validità . All'apertura della pagina il titolario mostrerà solo le classifiche di primo livello. Per visualizzare le classifiche figlie basterà cliccare sul simbolo freccia accanto all'icona

Titolario	
Ricerca Classificazioni	
Titolario valido al	21/10/2020
Codice:	
Descrizione:	
Ricerca Filtri	
Classificazioni	
☐ 01 - AMMINISTRAZIONE.Valido dal 11/03/2012	
☐ 01-01 - STEMMI E GONFALONE.Valido dal 11/03/2012	
☐ 01-03 - ARCHIVIO GENERALE.Valido dal 06/06/2017	
☐ 01-04 - INCARICHI DIRIGENTI.Valido dal 12/08/2015	
☐ 01-05 - MATERIALE DI CANCELLERIA.Valido dal 14/03/2016	
☐ 01-06 - MATERIALE INFORMATICO.Valido dal 14/03/2016	
☐ 01-07 - SISTEMA INFORMATIVO.Valido dal 28/03/2017	
☐ 01-08 - CERIMONIALE, ATTIVITÀ DI RAPPRESENTANZA; ONORIFICENZ...	
☐ 02 - ORGANI E DIREZIONE.Valido dal 11/03/2012	
☐ 03 - AMBIENTE E TERRITORIO.Valido dal 26/11/2012	

La prima icona sulla bottoniera permette di aggiornare la vista ricaricando i dati.

Spuntando la casella a sinistra in corrispondenza di una classifica, saranno attivate, nella bottoniera, le funzionalità possibili solo agli utenti abilitati.



Modifica: permette di entrare sul dettaglio della classifica. Il dettaglio può essere aperto anche con un doppio click in corrispondenza della classificazione.



Storicizza: prevede la chiusura della classificazione ad una certa data, riaprendola al giorno successivo con la nuova descrizione inserita.

La finestra "Storicizzazione Classificazione" presenta un titolo in blu. Sotto, c'è un campo "Descrizione" con il valore "ANALISI PERIODICA ACQUE". Al di sotto, un campo "Data apertura (la attuale verrà chiusa al giorno precedente)" con il valore "20/10/2020" e un'icona di calendario. Il corpo principale della finestra è un'area di testo vuota con l'header "03-04 - MONITORAGGIO ACQUE". In basso a destra, ci sono tre pulsanti: "Salva", "Salva e chiudi" e "Chiudi".



Elimina: permette di cancellare la classificazione qualora non sia stata utilizzata e non abbia classificazioni di livello inferiore associate.



Import CSV: la funzionalità permette l'operazione di import di un titolare caricato su un file csv secondo un tracciato prestabilito.



Aggiungi: questa funzione permette l'inserimento di diverse tipologie di registrazioni afferenti alla classifica che eventualmente è stata precedentemente selezionata, così si potrà creare in base alla profilazione dell'utente:

- una nuova Classifica, eventualmente figlia rispetto a quella selezionata,
- un nuovo Fascicolo,
- una nuova Lettera,
- un nuovo Protocollo generico,
- un nuovo Documento da Fascicolare.

3.2 Classificazioni

La possibilità di inserire una nuova classifica o di modificarne una esistente è abilitata solo agli utenti con apposito ruolo. La nuova maschera richiede il dato obbligatorio del codice classifica, la scelta della classificazione padre se si vuole creare una classifica figlia, la descrizione, se la classifica dovrà essere utilizzata come contenitore di documenti e se i fascicoli con sotto-fascicoli possono contenere documenti. Successivamente troviamo il campo Note e le date di validità della classifica.

Dopo aver Salvato i dati, verranno abilitate tre nuove sezioni: Fascicoli, Unità e Storico.

3.2.1 Fascicoli

La vista contiene un flag 'La numerazione del fascicolo è indipendente dall'anno?' riguardante il comportamento della numerazione del fascicolo rispetto all'anno solare: se viene spuntato la numerazione dei fascicoli in classifica procederà con la numerazione dall'anno precedente, cambiando quindi solo l'anno stesso. In caso contrario, la numerazione verrà azzerata al cambio di anno, e farà quindi ripartire i fascicoli dal numero 1 nel nuovo anno. Successivamente troviamo l'elenco aggiornato dei fascicoli eventualmente presenti sulla classifica suddivisi per anno e ultimo numero.

Anno	Ultimo numero
2020	4
2019	5
2018	4
2017	2

3.2.2 Storico

La sezione mostra le eventuali storizzazioni effettuate sulla classifica con le descrizioni e le date di apertura e chiusura.

Modifica classificazione

Classificazione Fascicoli Unità **Storico**

Elenco delle storizzazioni della classificazione

Codice	Descrizione	Data apertura	Data chiusura
13/02	RUOLI MATRICOLARI	01/01/2005	
13/02	ESTERI/EMIGRAZIONI	01/01/1951	31/12/2004

Storizza
 Chiudi classificazione

Salva
 Salva e chiudi
 Chiudi

3.3 Fascicolo

La nuova maschera del fascicolo presenta in alto l'unità organizzativa di creazione del fascicolo, che coincide con l'unità di appartenenza dell'utente, in fase di creazione, se si fa parte di più unità organizzative, va selezionata l'unità di creazione del fascicolo dall'apposito menù a tendina presente sul campo.

Fascicolo

Unità: AREA AMBIENTE

La pagina principale della maschera è divisa in due sezioni: Dati e Archiviazione.

Dati Documenti in fascicolo Elenco Sub Relazioni Storicizza Modifica Stampa

Dati

Classificazione: 01-03 - ARCHIVIO GENERALE

Anno: 2020 Numero anno prossimo

Oggetto: CONVOCAZIONI VERBALI ANNO 2020

Unità Competente: AREA AMBIENTE

Responsabile:

Riservato: ☐

Archiviazione

Data apertura: 19/10/2020

Data chiusura:

Digitale: ☐

Stato: CORRENTE

Anno: 2020

Topografia:

Note:

Nella prima sezione sono presenti i dati relativi alla classifica, che può essere interamente riportata nel campo o ricercata attraverso codice o descrizione e l'Anno del fascicolo.

Una delle novità, solo per gli utenti abilitati, è il campo 'Numera anno prossimo' presente in creazione di un

nuovo fascicolo, che permette di creare un fascicolo che verrà automaticamente numerato al cambio di anno solare, utilizzando come anno di archiviazione quindi l'anno successivo rispetto alla data di creazione.

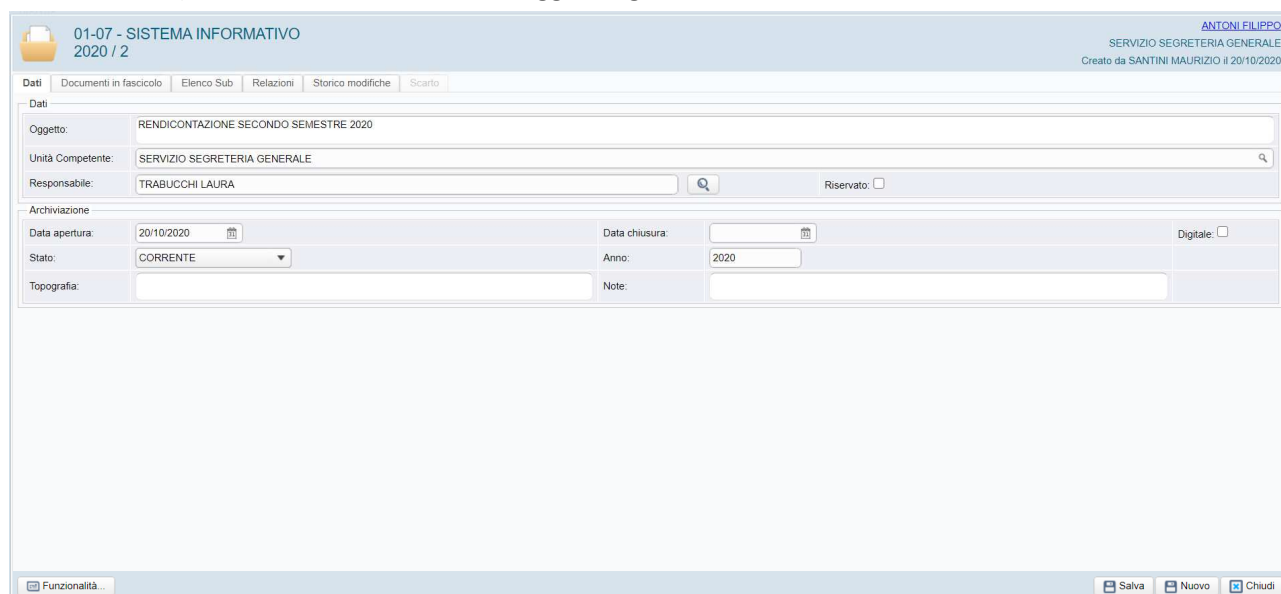
Unità Competente e Responsabile della tenuta del fascicolo, quest'ultimo valore può essere compilato direttamente sul campo o selezionato ricercando il componente navigando la struttura organizzativa

disponibile dall'apposita icona di ricerca .

Nella sezione "Archiviazione", troviamo la data di apertura del fascicolo e la data di chiusura: quest'ultima data può essere inserita manualmente oppure automaticamente qualora si cambi lo stato del fascicolo da Corrente, a Deposito o Storico. Il campo Anno mostra l'anno del fascicolo, il campo Topografia viene utilizzato quando si vuole localizzare il fascicolo in un ufficio in particolare dell'Ente. Il campo Note ospiterà eventuali note d'ufficio sul fascicolo. Una novità è rappresentata dal campo dedicato all'informazione sulla completa dematerializzazione dei documenti contenuti nel fascicolo: spuntando il campo "Digitale", si intende appunto che il fascicolo è composto di originali digitali, senza controparti originali cartacee. La spunta sul campo non ha riflessi applicativi, ma è un promemoria su quali tipologie di documenti andare a cercare in caso di archiviazione del fascicolo.

Il tasto "Crea", numera il fascicolo all'interno della classifica prescelta mentre con la funzione "Crea e Stampa" si produce anche la stampa della copertina del fascicolo con i dati principali inseriti di anno, numero fascicolo, descrizione, classifica di appartenenza, date di validità e unità di competenza.

A seguito della numerazione del fascicolo vengono riportati nell'intestazione della pagina i dati identificativi di classificazione, anno e numero. Lo spostamento di alcuni campi compilati manualmente (classificazione e anno fascicolo) è dovuto ad una scelta di maggior ergonomia in fase di inserimento di un nuovo fascicolo.



A seguito della creazione del fascicolo viene reso disponibile il menù "Funzionalità", posto in basso sulla sinistra della pagina, che rende disponibili agli utenti abilitati le seguenti funzioni:

- Nuovo: permette la creazione di un nuovo fascicolo
- Sub: genera un sub-fascicolo del fascicolo su cui si è posizionati
- Duplica: copia su una nuova pagina i dati del fascicolo aperto per generarne uno nuovo
- Stampa Copertina: permette di stampare i dati principali del fascicolo
- Stampa documenti in fascicolo: produce l'elenco dei documenti contenuti nel fascicolo.

Le pagine successive abilitate a seguito della numerazione, contengono le informazioni relative ai documenti contenuti nel fascicolo, l'elenco dei sotto-fascicoli esistenti, le eventuali relazioni con altri fascicoli, la storicizzazione delle modifiche dei dati, e l'eventuale situazione di scarto archivistico.

3.3.1 Documenti in fascicolo

Questo folder mostra l'elenco di tutti i documenti fascicolati che fanno riferimento all'affare o al procedimento identificato dal fascicolo.

Dati		Documenti in fascicolo	Elenco Sub	Relazioni	Storico modifiche	Scarto
<< < 1 / 1 > >>     Ordinamento: Crescente per Anno e Data						
	Documento	File				
	Protocollo: 2020 / 43 del 19/02/2020 11:35:16 Fascicolo: 2 / 2017 - Classificazione: 01-07 Contratto: 2 / 2020 - Data stipula: 19/02/2020 12:00:00 - CIG: Z7774JJJF Oggetto: LAVORI DI AMPLIAMENTO DELLA ROTONDA VIA SANT'ARTEMIO					
	Protocollo Generale - 2017 / 31 del 14/02/2017 15:02:00 Modalità: ARRIVO Oggetto: INVIO DOCUMENTAZIONE UTENTE					
	Documento del 28/03/2017 15:06:06 Oggetto: COSTO CANONI MANUTENZIONE					
	Protocollo Generale - 2017 / 271 del 10/11/2017 11:24:06 Modalità: ARRIVO Oggetto: CONCORSO PARTECIPAZIONE					
	DETERMINAZIONI - Proposta 2018 / 21 - Atto 5 / 2018 Oggetto: REGOLAMENTAZIONE UTILIZZO POSTA ELETTRONICA AZIENDALE Tipologia: Esecutiva dal: 12/02/2018 - Pubblicata dal 12/02/2018 al 27/02/2018 Protocollo: 42 del 12/02/2018 10:41:45					
	PROTOCOLLO GENERALE - 2019 / 318 del 28/10/2019 13:25:34 Modalità: PARTENZA Oggetto: INVIO TRACCIATI					
	PROTOCOLLO GENERALE - 2020 / 163 del 03/06/2020 10:41:49 Modalità: PARTENZA Oggetto: INVIO DOCUMENTAZIONE RICHIESTA					

In corrispondenza di ciascuna riga in elenco sono visibili icone e dati specifici differenti che contraddistinguono le varie tipologie di documento.

È possibile consultare velocemente il file principale o allegati eventualmente presenti sul documento, attraverso un click sull'icona posta sulla destra di ogni riga . In qualunque momento, sarà possibile entrare in modifica su ogni documento dell'elenco, qualora se ne abbiano le competenze, con l'icona  o con doppio click sul documento desiderato.

La parte superiore della maschera contiene l'abituale navigatore per muoversi tra le pagine, il pulsante di aggiornamento delle informazioni presenti, ed un menu a tendina che permette di ordinare i documenti secondo diversi criteri. L'impostazione di base mostra i documenti ordinati per anno e data di creazione in ordine crescente (Crescente per Anno e Data), è possibile modificare l'ordinamento selezionando uno degli altri criteri disponibili: Decrescente per Anno e crescente per Data oppure Decrescente per Anno e Data.

Ulteriori due pulsanti sono abilitati a seguito della selezione di uno o più documenti dell'elenco, e sono necessari per modificare  la posizione archivistica o per aggiungere  una posizione archivistica secondaria.

3.3.2 Elenco Sub

I sotto fascicoli eventualmente presenti sul fascicolo che si sta consultando vengono elencati in questo folder.

L'apertura in modifica sui sub fascicoli selezionati avviene tramite l'icona  oppure con doppio click sulla registrazione desiderata.

01/03 - STATUTO
2020 / 1

RE NICOLA
A04.01 - AFFARI GENERALI
Creato da il 07/01/2020

Dati | Documenti in fascicolo | Elenco Sub | Relazioni | Storico modifiche | Scarlo

<< < 1 / 1 > >>

Fascicolo

- 2020/1.1 Stato: CORRENTE Anno Archiviazione: 2020
Oggetto: VERBALI 2020
- 2020/1.2 Stato: CORRENTE Anno Archiviazione: 2020
Oggetto: MONITORAGGIO PRATICHE
- 2020/1.3 Stato: CORRENTE Anno Archiviazione: 2020
Oggetto: RICHIESTE INOLTRE
- 2020/1.4 Stato: CORRENTE Anno Archiviazione: 2020
Oggetto: ATTESTATI DI FREQUENZA CORSI

3.3.3 Relazioni

01-03 - ARCHIVIO GENERALE
2020 / 1

RE NICOLA
AREA AFFARI GENERALI
Creato da TRABUCCHI LAURA il 29/02/2020

Dati | Documenti in fascicolo | Elenco Sub | Relazioni | Storico modifiche | Scarlo

Classifica: 01-03 - ARCHIVIO GENERALE Fascicolo: 2019 / 1 - PROGETTO FORNITURA SISTEMA DI PROTOCOLLO INFORMA

Relazione: Relazione Passiva Tipo relazione: Fascicolo Precedente/Seguente

Oggetto	Classifica	Anno	Numero	Tipo Relazione
RETE INFORMATICA	01-07	2018	1	Collegamento
PROGETTO FORNITURA SISTEMA DI PROTOCOLLO INFORMATICO	01-03	2019	1	Precedente/Seguente

Con questa funzione è possibile mettere in relazione fascicoli tra loro, in modo da avere dei collegamenti rapidi all'interno degli stessi. Tramite i campi di ricerca posti nella parte superiore è possibile ricercare il fascicolo da mettere in relazione; è poi possibile scegliere se la reazione sia attiva o passiva, tra il fascicolo che si sta modificando e il fascicolo con il quale si sta creando la relazione. Una relazione attiva sul fascicolo in modifica verrà mostrata come passiva sul fascicolo relazionato, e viceversa. Sono poi possibili due diverse tipologie di relazione; un generico collegamento tra fascicoli, e relazioni di questa tipologia sono possibili in numero illimitato, e la tipologia più specifica precedente/seguito è possibile solo una volta per fascicolo e con un solo fascicolo; questa ultima tipologia può essere utilizzata, ad esempio, per fascicoli a cadenza annuale, per legare tra loro annualità diverse.

Inserite le informazioni, si inserisce la relazione cliccando sul pulsante . Il valore viene immesso in maschera, ed è possibile aprire il fascicolo inserito come relazione con le abituali modalità. Il fascicolo legato con relazione attiva sarà evidenziato dall'icona  mentre la relazione passiva viene contrassegnata con l'icona .

3.3.4 Storico Modifiche

Questa funzione mostra l'elenco delle modifiche intervenute sul fascicolo, sarà possibile consultare non solo la data/ora e utente di modifica, ma anche il campo interessato alla modifica, il nuovo valore inserito ed anche il valore precedentemente presente.

**01-03 - ARCHIVIO GENERALE**
2020 / 1.1

RE NICOLA
AREA AFFARI GENERALI
Creato da RE NICOLA il 13/10/2020

Dati | Documenti in fascicolo | Elenco Sub | Relazioni | **Storico modifiche** | Scarfo

Ricerca storico dal: 13/10/2020 Ricerca storico al:

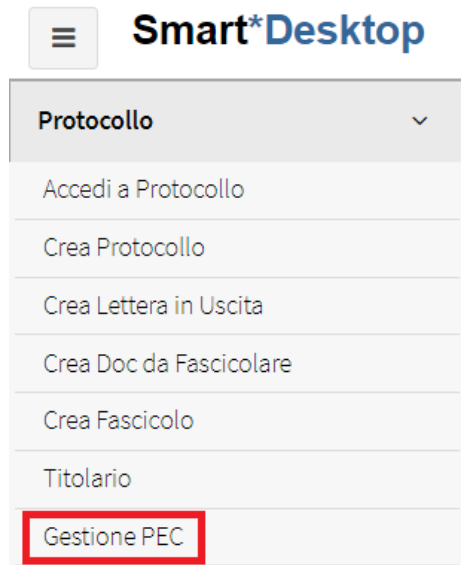
Data	Utente	Campo	Valore
13/10/2020 10:25:01	RE NICOLA	 Oggetto	VERBALI SECONDO SEMESTRE 2020
		 Responsabile	
		 Riservato	N
		 Digitale	N
		 Stato Fascicolo	CORRENTE
		 Topografia	
		 Note	
		 Data Apertura	13/10/2020
		 Data Archiviazione	
		 Anno Archiviazione	2020
		 Unità Competente	
13/10/2020 10:38:10	RE NICOLA	 Oggetto	NOTIFICA VERBALI PRIMO SEMESTRE 2020

Funzionalità...

4 Gestione PEC

Nella versione in oggetto, coerentemente con le altre funzionalità applicative, anche l'area di lavoro per la gestione della posta elettronica in ingresso relativa alle caselle integrate nel sistema di protocollo è stata completamente ridisegnata, semplificandone la gestione da parte degli utenti.

La nuova funzionalità si avvale delle medesime competenze gestite in precedenza, sarà quindi accessibile ai soli utenti abilitati, selezionando il link "Gestione PEC" presente nel menu della sezione Protocollo disponibile su Smart*Desktop



In alternativa, nell'area di lavoro Protocollo del sistema di Gestione Documentale, è disponibile il nuovo collegamento.

La nuova area di lavoro è caratterizzata da 2 sezioni che racchiudono le funzionalità presenti nella precedente gestione: "Messaggi in arrivo" e "Da Protocollare".

4.1 Messaggi in Arrivo

In questa sezione sono visibili tutti i messaggi ricevuti sulla casella selezionata e per cui l'utente ha competenza.



La parte superiore della pagina contiene il consueto navigatore per spostarsi tra le eventuali pagine presenti, ed una serie di campi di ricerca. Nel dettaglio, è possibile filtrare i messaggi presenti per:

- **Casella:** permette di scegliere per quale casella visualizzare i messaggi; la quantità di voci al suo interno dipende strettamente dalle configurazioni del sistema e dalle abilitazioni del singolo utente;
- **Data:** "Dal", "Al" è possibile indicare le date di ricezione per le quali eseguire la ricerca: in apertura viene sempre proposta la data odierna, ma è possibile cambiare il valore scrivendo direttamente nel campo o scegliendo il valore dal calendario;
- **Tipo:** è possibile scegliere tra i messaggi provenienti da mittenti aventi caselle di posta certificate, non certificate, o messaggi di tipo "ricevuta", in apertura viene sempre proposta l'opzione "Tutti".
- **"Oggetto" e "Mittente":** sono campi liberi che possono essere utilizzati per ricerche specifiche per

parole chiave o per parti più ampie dell'oggetto come anche per mittente; i due campi permettono la ricerca anche attraverso parti di parole, senza necessità di inserire nessun carattere aggiuntivo;

- *Esito*: è possibile filtrare i messaggi in base allo stato del processo di acquisizione e protocollazione; gli stati identificano se il messaggio in arrivo non ancora lavorato proviene da altri enti in regime di interoperabilità o da altri mittenti e, sui messaggi già lavorati, cosa effettivamente ne sia stato fatto. Oltre al valore di default "Tutti", può assumere tramite selezione dall'apposito menu a tendina i valori:
 - o *Da Gestire*: identifica i messaggi in arrivo provenienti da mittenti non in regime di interoperabilità, quindi privati, aziende o simili. Non distingue se il mittente è una casella certificata o meno (per questo è presente il filtro nel campo "Tipo"). A seconda delle operazioni compiute sul singolo messaggio, lo stato cambierà nei successivi.
 - o *Da protocollare (con Segnatura)*: è lo stato specifico dei messaggi arrivati da altri enti in regime di interoperabilità: in questi casi, il sistema leggendo la segnatura prepara in automatico delle bozze di protocollazione, reperibili anche nella sezione "**Da Protocollare**". Questo stato identifica quindi i messaggi provenienti da PEC con segnatura predisposti per la protocollazione ma non ancora numerati nel registro generale.
 - o *Da protocollare (senza Segnatura)*: come lo stato precedente, ma riguarda i messaggi provenienti da mail non certificate e da mail certificate ma senza la segnatura, quindi non provenienti in regime di interoperabilità da altri enti, sui quali è già stata però espressa la volontà di procedere alla protocollazione.
 - o *Gestito*: viene indicato sui messaggi automatici PEC e di interoperabilità (accettazione, consegna, conferma, ecc).
 - o *Generata Eccezione*: indica i messaggi arrivati in interoperabilità sui quali è stato scelto di inviare al mittente una notifica di eccezione
 - o *Non protocollato*: identifica i messaggi per i quali si è scelto l'inserimento a sistema senza procedere alla protocollazione, ma gestendone lo smistamento e/o la fascicolazione.
 - o *Protocollato*: identifica i messaggi sui quali è stata completata l'operazione di attribuzione del numero di protocollo.
 - o *Scartato*: indica i messaggi per i quali è stata eseguita l'apposita funzionalità "Scarta" dalla maschera del singolo messaggio.
- *Mostra messaggi automatici*: la selezione di questo campo permette di scegliere se visualizzare anche i messaggi automatici proprio della gestione PEC, ovvero accettazioni, consegne; questi messaggi non vengono mostrati nella ricerca di base in quanto solitamente gestiti in automatico dal sistema.

Per eseguire la ricerca dopo aver predisposto gli opportuni filtri occorre cliccare sull'icona "Ricerca" (). Di default, la nuova sezione all'accesso presenta i messaggi del giorno indipendentemente dal tipo e dallo stato, escludendo i messaggi automatici.

Posta Elettronica Certificata								
Messaggi in arrivo Da Protocollo								
Casella: AOO GRUPPO FINMATICA (demo.affarigenerali@legalmail.it) Dal: 20/10/2020 Al: 21/10/2020								
Tipo: (Tutti)	Oggetto:	Mittente:	Esito: (Tutti)	Mostra messaggi automatici				
Stato	Data Spedizione	Scaricato il	Mittente	Destinatari	Oggetto	Tipo	Allegati	
Da Protocollo con Segnatura	20/10/2020 10:10:33	20/10/2020 11:10:41	demo.affarigenerali@legalmail.it	demo.affarigenerali@legalmail.it	(Rif. 2020/371 PROT) RICHIESTA INTEGRAZIONE PRATICA VIA PIAVE	Pec		
Da Protocollo con Segnatura	20/10/2020 11:10:33	20/10/2020 11:10:37	demo.affarigenerali@legalmail.it	demo.affarigenerali@legalmail.it	(Rif. 2020/331 PROT) AUTORIZZAZIONE	Pec		
Da Protocollo con Segnatura	21/10/2020 10:10:33	21/10/2020 10:10:39	demo.affarigenerali@legalmail.it	demo.affarigenerali@legalmail.it	(Rif. 2020/377 PROT) RICHIESTA DOCUMENTAZIONE AGGIUNTIVA - PRATICA VIA PIAVE	Pec		
Da Protocollo con Segnatura	21/10/2020 15:10:37	21/10/2020 15:10:40	sigedo_test@pec.comune.fi.it	demo.affarigenerali@legalmail.it	(Rif. 2020/2286 PROT) PROGETTO AREA PEC	Pec		
Da Protocollo con Segnatura	21/10/2020 15:10:37	21/10/2020 15:10:38	demo.affarigenerali@legalmail.it	demo.affarigenerali@legalmail.it	(Rif. 2020/2287 PROT) INVIO DOCUMENTAZIONE WEBINAR	Pec		
Da Protocollo con Segnatura	21/10/2020 15:10:37	21/10/2020 15:10:40	demo.affarigenerali@legalmail.it	demo.affarigenerali@legalmail.it	(Rif. 2020/2288 PROT) COMUNICAZIONE INIZIO PROGETTO	Pec		
Da Gestire	21/10/2020 15:10:03	21/10/2020 15:10:38	C.Ceciliotti@ads.it	demo.affarigenerali@legalmail.it	ANOMALIA MESSAGGIO: Richiesta apertura fascicolo	Ordinario		

Per ogni messaggio presente nell'elenco sono visibili una serie di informazioni:

Stato del messaggio, in relazione ai possibili stati riportati poco sopra

Data Spedizione, data e ora di spedizione del messaggio originale da parte del mittente

Scaricato il, data e ora dell'effettivo scarico del messaggio nel sistema

Mittente, indirizzo mail del mittente

Destinatari del messaggio

Oggetto del messaggio

Tipo, messaggio proveniente da posta elettronica certificata ("PEC") o normale ("ordinario")

Allegati, cliccando sull'icona () "Apri Allegati" appare l'elenco degli allegati del messaggio ed è possibile scaricare e visualizzare il/i file/s.

L'icona identifica la presenza di una maschera di protocollo conseguente al singolo messaggio. Un protocollo collegato può essere effetto della procedura automatica che effettua il sistema sui messaggi provenienti in regime di interoperabilità, e quindi con presenza di segnatura: sono i messaggi identificati dallo stato "da protocollare con segnatura"; il sistema legge la segnatura e, sulla base di questa, procede con la preparazione di una bozza di protocollazione, contenente le informazioni dedotte, appunto, dalla segnatura. Cliccando l'icona quindi, si potrà accedere a questa bozza di protocollazione, e procedere con le operazioni necessarie. Una volta terminata la compilazione, e protocollato il documento, al rientro sulla pagina di gestione dei messaggi, lo stesso avrà lo stato cambiato in "Protocollato".

La presenza dell'icona relativa al protocollo collegato può essere effetto della procedura manuale di protocollazione dei messaggi ricevuti: per ogni messaggio infatti è possibile procederne alla protocollazione, anche passando da uno stato di bozza appunto. In questo caso, lo stato di questi messaggi sarà "Da protocollare senza segnatura", e il click sull'icona aprirà il documento collegato.

Eseguendo un doppio click in un qualunque punto della singola riga, o eseguendo un solo click e poi cliccando il consueto pulsante di accesso presente nella pulsantiera () "Modifica", sarà possibile entrare nella maschera di dettaglio del singolo messaggio.

Messaggio in arrivo
Da Gestire
Da posta elettronica ordinaria

Redattore: ANTONI FILIPPO
Unità:

Data Spedizione: 22/10/2020 09:46:59 Scaricato il: 22/10/2020 09:50:39

Mittente: M.Santini@ads.it

Destinatari: demo.affarigenerali@legalmail.it

CC:

BCC:

Oggetto: ANOMALIA MESSAGGIO: Invio documentazione richiesta
Si invia quanto in oggetto.
Cordiali saluti

Testo: Maurizio Santini

Classificazione: Fascicolo:

Allegati e Smistamenti

Allegati

- Prospetto Riepilogativo 2020.pdf p7m
- Documentazione a supporto - integrazione 2020.pdf

Smistamenti Correnti

Tipo	Trasmissione	Ufficio/Assegnante	Preso in carico	Assegnato	Eseguito
Nessuno smistamento presente					

Smistamenti Storici

Funzionalità...

Anche questa parte è stata riprogettata ed adeguata al nuovo standard previsto dal progetto Prisma 4.0, mantenendo l'impostazione della maschera precedente, ma introducendo una rinnovata veste grafica e le funzionalità presenti sulle nuove maschere già viste. In particolare, nella parte superiore sinistra troviamo l'indicazione dello stato del messaggio e del tipo di messaggio; sulla parte destra, oltre al nominativo dell'utente che ha lanciato la funzione, troviamo utente e unità di prima gestione.

Nella sezione immediatamente inferiore, trovano posto i dati di dettaglio del messaggio, data di spedizione originale e data di download nel sistema ("Scaricato il:"), mittente e destinatari diretti, copia conoscenza, e copia conoscenza nascosta. Seguono l'oggetto del messaggio, e il testo.

Come anticipato in precedenza, è possibile gestire a sistema il messaggio anche senza protocollarlo, potendolo inserire ad esempio in un fascicolo: a questo proposito sono presenti i campi dedicati alla posizione archivistica, nei quali è possibile agire come consuetudine per campi di questo tipo:

- Cliccando sull'icona contraddistinta dalla lente d'ingrandimento, verrà aperto l'elenco delle voci di classificazione disponibili: l'elenco è scorrevole e diviso in pagine, navigabili con gli appositi pulsanti. È sufficiente quindi cliccare sul valore desiderato per inserirlo in maschera; è anche possibile muoversi nell'elenco tramite le frecce giù e su della tastiera, premendo il tasto invio una volta selezionato il valore necessario.
- Posizionandosi nel campo, e cominciando a scrivere il codice o una parola della descrizione, il sistema comincerà a cercare tra i valori presenti, proponendoli nell'elenco. Identificato il valore desiderato, ancora è possibile selezionarlo cliccando con il mouse, o muovendosi nell'elenco con le frecce della tastiera, premendo invio una volta evidenziato il valore.

Inserito il valore di classifica, nel campo del fascicolo i valori saranno già filtrati in base al valore scelto nel campo precedente. Come sulla maschera di protocollo, tramite l'icona () "Ricerca Fascicolo", è possibile accedere ad una maschera di ricerca e, se l'utente è abilitato, alla creazione di un nuovo fascicolo.

La parte inferiore della maschera è divisa in sezioni, identificate dalle icone presenti sul lato sinistro. Nella prima sezione troviamo l'elenco degli allegati presenti nel messaggio, con possibilità di aprire i files e verificarne il contenuto, agendo sul pulsante dedicato. A lato, trova posto la parte dedicata agli smistamenti: infatti, oltre che poter fascicolare un messaggio senza protocollarlo, è anche possibile smistarlo, di modo da recapitarlo sulle Smart*Desktop dei componenti delle unità selezionate. L'inserimento dello smistamento è del tutto simile a quanto presente sulla maschera di protocollo.

4.2 “Da Protocollare”

La sezione “da protocollare”, contiene le bozze di protocollazione dei messaggi ricevuti, create automaticamente dal sistema o manualmente dagli utenti.

Posta Elettronica Certificata					
Messaggi in arrivo Da Protocollare					
Casella: (Tutte) Dal: 22/10/2020 Al: 22/10/2020 Tipo: (Tutti) Mittente:					
Modalità	Ultima Modifica	Oggetto	Classifica	Mittente	
ARRIVO	22/10/2020 12:06	DOCUMENTO DI RICONOSCIMENTO CC	/	C.Ceciliot@ads.it	
ARRIVO	22/10/2020 10:25	COMUNICAZIONE DI MANIFESTAZIONE CON COSAP	/	istituzionaleads@pec.it	
ARRIVO	22/10/2020 14:10	INVIO RICHIESTA PARTECIPAZIONE CORSO FORMAZIONE	/	cristian.ceciliot@postecert.it	

Per ogni messaggio presente nell’elenco viene indicato:

Modalità, ARRIVO

Data Spedizione, data e ora di spedizione del messaggio da parte del mittente

Oggetto del messaggio

Mittente, indirizzo mail del mittente

Allegati, cliccando sull'icona () “Apri Allegati” appare l’elenco degli allegati del messaggio ed è possibile scaricare e visualizzare il/i file/s

Nel dettaglio, è possibile filtrare i messaggi presenti per:

- **Casella**: permette di scegliere per quale casella visualizzare i messaggi; la quantità di voci al suo interno dipende strettamente dalle configurazioni del sistema e dalle abilitazioni del singolo utente.
- **Data**: “Dal”, “Al” è possibile indicare le date di ricezione per le quali eseguire la ricerca: in apertura viene sempre proposta la data odierna, ma è possibile cambiare il valore scrivendo direttamente nel campo o scegliendo il valore dal calendario.
- **Tipo**: è possibile scegliere tra i messaggi provenienti da mittenti aventi caselle di posta certificate, non certificate, o messaggi di tipo “ricevuta”, in apertura viene sempre proposta l’opzione “Tutti”.
- I campi “Oggetto” e “Mittente” sono campi liberi che possono essere utilizzati per ricerche specifiche per parole chiave o per parti più ampie dell’oggetto come anche per mittente; i due campi permettono la ricerca anche attraverso parti di parole, senza necessità di inserire nessun carattere aggiuntivo.

Da questa sezione è possibile visualizzare il dettaglio della maschera pre-compilata della registrazione a protocollo del documento selezionato con doppio click.

4.3 Ricezione e gestione dei messaggi

Se il messaggio proviene da una casella di posta elettronica certificata e tra gli allegati è incluso un file denominato Segnatura.xml conforme, l’applicazione, in base all’esito della verifica, predispone la maschera di protocollo su cui l’utente abilitato effettua l’accesso per la visualizzazione, piuttosto che in modifica per la registrazione a protocollo del documento contenuto nel messaggio ricevuto oppure l’invio della Notifica Eccezione al sistema informatico mittente.

Nella sezione “**Messaggi in arrivo**”, come descritto nel punto 4.1, questo è evidenziato dalla presenza dell'icona () “Apri Protocollo”:

Posta Elettronica Certificata							
Messaggi in arrivo Da Protocollare							
Casella: (Tutte) Dal: 20/10/2020 Al: 22/10/2020 Tipo: (Tutti) Oggetto: Mittente: Esito: Da Protocollore con Segr ☐ Mostra messaggi automatici							
Stato	Data Spedizione	Scaricato il	Mittente	Destinatari	Oggetto	Tipo	Allegati
Da Protocollore con Segnatura	21/10/2020 10:10:33	21/10/2020 10:10:39	demo.affarigenerali@legalmail.it	demo.affarigenerali@legalmail.it	(Rif. 2020/377 PROT) RICHIESTA DOCUMENTAZIONE AGGIUNTIVA - PRATICA VIA PIAVE	Pec	

La maschera pre-compilata di registrazione a protocollo del messaggio selezionato si presenta come segue:

Se l'utente compila la maschera di registrazione nei suoi dati mancanti e usa il pulsante **"Protocollo"**, il sistema assegna un numero di protocollo cronologico per l'anno solare ed il documento protocollato, ricevuto dalla posta elettronica, viene contrassegnato nel documentale con l'icona @ (✉).

Da notare che nella maschera di registrazione a protocollo dei messaggi ricevuti da protocollare, è visibile una sezione **"Dati Interoperabilità"** che raggruppa informazioni di sintesi sulla gestione interoperabilità.

Se il messaggio proviene da una casella PEC e non presenta tra gli allegati un file Segnatura.xml, o proviene da mail non certificate, nella sezione **"Messaggi in arrivo"** il messaggio si presenta nello stato **"Da gestire"**:

Posta Elettronica Certificata								
Messaggi in arrivo Da Protocollare								
<< >> 1 / 1 Casella: (Tutte) Dal: 19/10/2020 Al: 19/10/2020								
Tipo: (Tutti) Oggetto: Mittente: Stato: Da Gestire Mostra messaggi automatici								
Stato	Data Spedizione	Scaricato il	Mittente	Destinatari	Oggetto	Tipo	Allegati	
Da Gestire	19/10/2020 13:01:23	19/10/2020 13:06:00	cristian.ceciliot@postecert.it	ADS <istituzionaleads@cert.legalmail.it>	Invio documentazione per formazione	Pec		

Dopo aver selezionato il messaggio, con doppio click sullo stesso o agendo sull'icona (✎) **"modifica"**, l'applicativo presenta una maschera sulla quale, l'utente abilitato, può accedere in visualizzazione del contenuto del messaggio, ovvero procedere alla creazione della maschera di protocollazione se lo ritiene opportuno:

Messaggio in arrivo
Da Gestire
Da posta elettronica certificata (2033113)

Redattore: CECILIOT CRISTIAN
Unità: AFFARI GENERALI ISTITUZIONALI E FINANZIARI

Data Spedizione: 19/10/2020 14:48:39
Mittente: cristian.ceciliot@postecert.it
Destinatari: ADS <istituzionaleads@cert.legalmail.it>
CC:
CCR:
Oggetto: Invio documentazione per formazione
Testo: XXXX

Scaricato il: 19/10/2020 14:51:01

Classificazione: Fascicolo:

Allegati e Smistamenti

Allegati: test_ads.pdf

Smistamenti Correnti

Tipo	Trasmesso	Ufficio/Assegnante	Preso in carico	Assegnato	Eseguito
Nessuno Smistamento presente					

Smistamenti Storici

Crea Protocollo
Scarta
Visualizza messaggio di posta (emi)

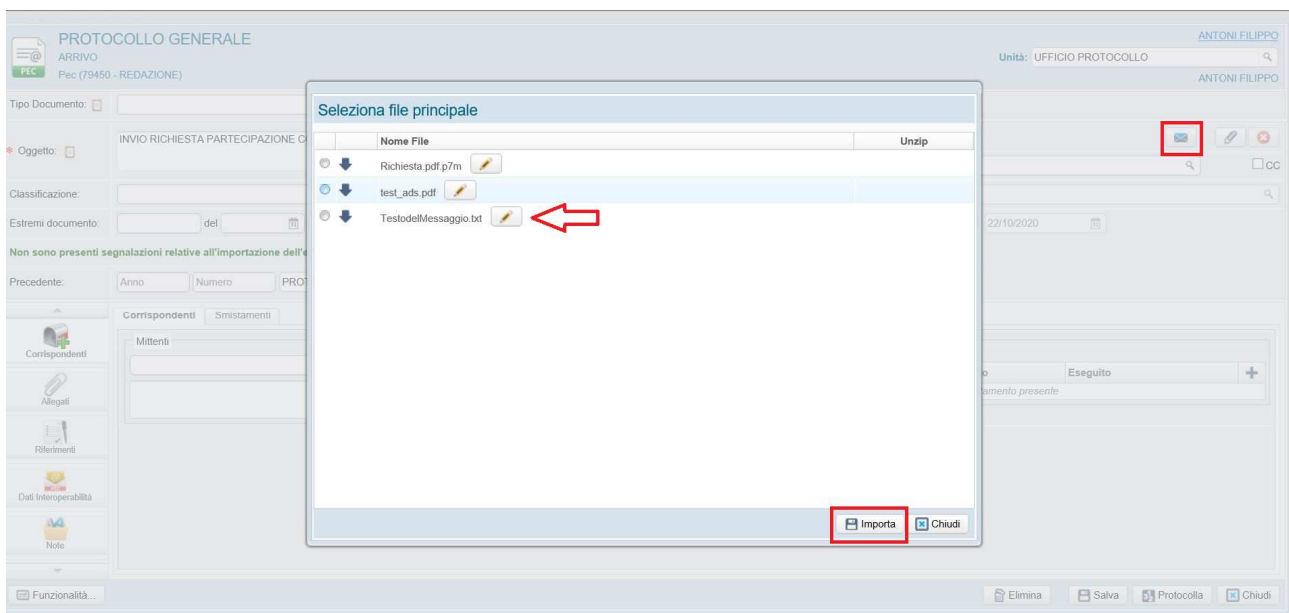
Salva Chiudi

Agendo sulla voce **“Crea Protocollo”** nel menu **“Funzionalità”**, in basso a sinistra nella maschera del messaggio, il sistema ribalta le informazioni del messaggio su una nuova maschera di protocollo, di modo che sia possibile protocollarne il contenuto.

Lo stato del messaggio cambia da **“Da Gestire”** in **“Da protocollare senza Segnatura”** e sarà visibile anche nella sezione **“Da Protocollare”**.

Le informazioni riportate sono meno puntuali rispetto ai messaggi ricevuti in interoperabilità, nei quali la maggioranza delle informazioni sono codificate nella segnatura. Di conseguenza, verranno riportati l'oggetto e il mittente, con possibilità chiaramente di modifica. Per quanto riguarda gli allegati, il sistema non è in grado di stabilire quale debba essere il file principale, mentre l'informazione è specificata in presenza di segnatura.

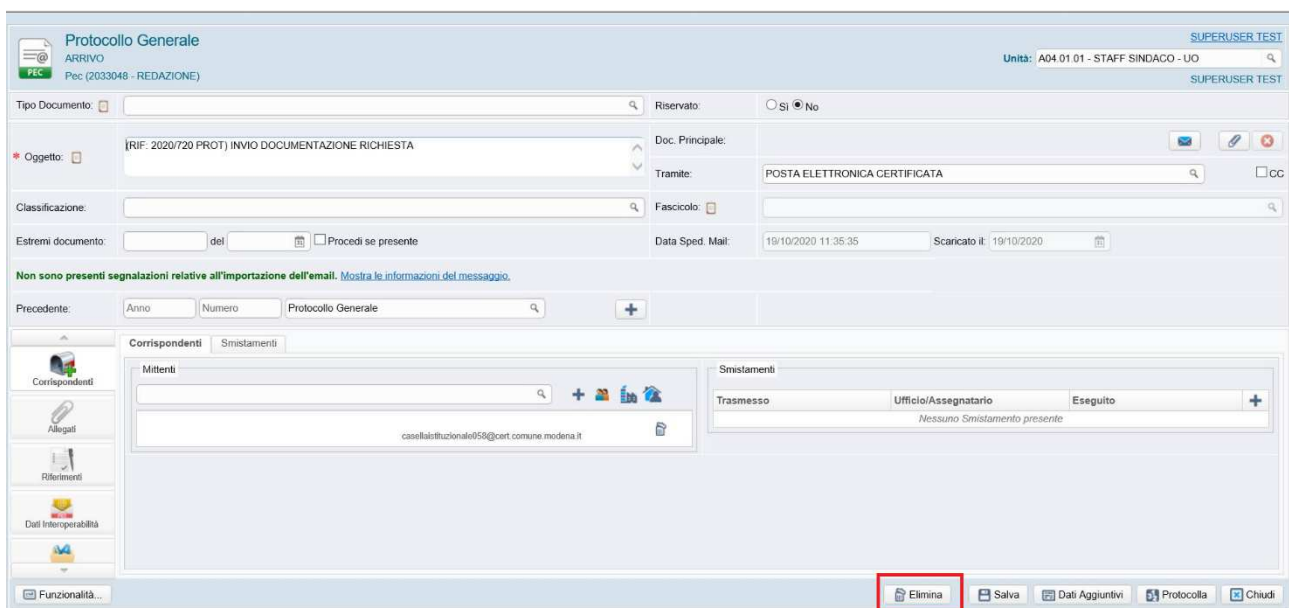
Di conseguenza, è necessario agire sul pulsante () **“Importa PEC”** presente alla destra di **“Doc. Principale”**, per comunicare al sistema quale dei file sia da considerare come principale, con possibilità anche in questa fase di prenderne visione, o di modificarne il nome. Scelto il file principale, gli altri verranno automaticamente inseriti come allegati secondari. Per questa tipologia di messaggio, il sistema crea sempre un allegato che contiene sempre il testo del messaggio originario, di modo che, se necessario, sia possibile indicarlo come allegato principale della registrazione di protocollo. Il formato di questo file viene deciso a livello di configurazione.



Inserendo quindi le ulteriori informazioni necessarie alla protocollazione, ed effettuata la protocollazione, tornando sull'elenco dei messaggi chiudendo il nuovo protocollo, troveremo aggiornato lo stato del messaggio appena gestito, da "Da protocollare senza Segnatura" in "Protocollato".

4.3.1 Messaggi indesiderati

E' presente una funzionalità apposita per la gestione dei messaggi ricevuti via PEC che non si ritiene di dover conservare. Come visto precedentemente, sul singolo messaggio è possibile indicare lo stato "Scartato", attraverso l'apposita voce del menu funzionalità "Scarta". È altresì possibile procedere tramite apposito pulsante "Elimina" da maschera di registrazione protocollo non ancora numerata, ma generata da un "Crea Protocollo" che in realtà non era necessario:



4.3.2 Consultazione messaggio protocollato e riferimenti

I messaggi ricevuti e protocollati, seguono i flussi di smistamenti che gli utenti abilitati predispongono e sono ricercabili e consultabili dal sistema documentale utilizzando le query predisposte nell'Area di lavoro **"Protocollo"** (ad esempio Ricerca Protocollo).

Per visualizzare la maschera del messaggio ricevuto utilizzare icona **"Elenco di collegamenti e riferimenti al documento"** presente nel blocco di visualizzazione del documento protocollato da gestione documentale e successivamente accedere alla sezione **"Riferimenti"**.

E' possibile consultare i messaggi protocollati nell'Area di Lavoro **"Posta Elettronica Certificata"**, valorizzando nella sezione **"Messaggi in arrivo"** lo stato "Protocollato"

Posta Elettronica Certificata								
Messaggi in arrivo Da Protocollare								
Casella: COMUNE DI SAN DONATO MILANESE (istituzionaleads@cert.legali) Dat: 11/10/2020 Al: 19/10/2020								
Tipo: (Tutti)	Oggetto:	Mittente:	Stato: Protocollato	Mostra messaggi automatici				
Stato	Data Spedizione	Scaricato il	Mittente	Destinatari	Oggetto	Tipo	Allegati	
Protocollato	14/10/2020 17:19:39	14/10/2020 17:22:02	M.Santini@ads.it	istituzionaleads@cert.legalmail.it	ANOMALIA MESSAGGIO: Invio di test per verifica funzionamento	Ordinario		
Protocollato	19/10/2020 13:02:15	19/10/2020 13:06:02	C.Ceciliotti@ads.it	istituzionaleads@cert.legalmail.it	ANOMALIA MESSAGGIO: Progetto ricerca PEC	Ordinario		

Per visualizzare il dettaglio del messaggio ricevuto effettuare doppio click sul messaggio selezionato.

Agendo sull'icona (📎) "Apri Protocollo" a destra di ogni singolo messaggio protocollato è possibile, come già indicato, visualizzare la maschera di dettaglio protocollazione.

Nella sezione **"Riferimenti"** del messaggio ricevuto protocollato vengono proposti l'elenco dei messaggi automatici di ritorno (annullamento o conferma).

Collegamenti Riferimenti Catena Documentale Posizioni Archivistiche Secondarie				
Documenti collegati				
Collegati	Anno	Numero	Registro	Protocollo Generale
Numero	Anno	Tipo Registro	Tipo Collegamento	Oggetto
			Collegamento fra messaggio in arrivo e protocollo	(Rif: 2020/1414 PROT) INVIO PEC RICHIESTA INFORMAZIONI ADS
			Collegamento fra protocollo e messaggio in arrivo per messaggio conferma ricezione	(Rif: 2020/1415 PROT) INVIO PEC RICHIESTA INFORMAZIONI ADS CONFERMA.XML

Agendo sull'icona (📎) "Apri Documento" (oppure doppio click sul riferimento selezionato) è possibile visualizzare a sua volta i riferimenti associati al messaggio automatico inviato: accettazione/consegna prodotti dal sistema di posta PEC.

PEC

Messaggio inviato

SENTOK (2031539)

SUPERUSER TEST

Data Spedizione:

16/10/2020 16:12:49

Mittente:

istituzionaleads@cert.legalmail.it

Destinatari:

ISTITUZIONALEADS@CERT.LEGALMAIL.IT

CC:

CCR:

Oggetto:

(Rif: 2020/1415 PROT) INVIO PEC RICHIESTA INFORMAZIONI ADS CONFERMA.XML

Testo:

Allegati

Riferimenti

Destinatari

Riferimenti

Documenti collegati

Numero	Anno	Tipo Registro	Tipo Collegamento	Oggetto
1415	2020	PROT	Collegamento fra protocollo e messaggio in arrivo per messaggio conferma ricezione	INVIO PEC RICHIESTA INFORMAZIONI ADS
			Collegamento fra messaggio inviato e messaggio ricevuto	ACCETTAZIONE: (Rif: 2020/1415 PROT) INVIO PEC RICHIESTA INFORMAZIONI ADS CONFERMA.XML
			Collegamento fra messaggio inviato e messaggio ricevuto	CONSEGNA: (Rif: 2020/1415 PROT) INVIO PEC RICHIESTA INFORMAZIONI ADS CONFERMA.XML

Chiusura

MANUALE DI CONSERVAZIONE

<i>Codice documento</i>	ManualeConservazione
<i>Versione</i>	6.0

	<i>Data</i>	<i>Nominativo</i>	<i>Funzione</i>
<i>Redazione</i>	23/07/2020	Giovanni Galazzini	Consulente
		Cristiano Casagni	Responsabile sviluppo e manutenzione del sistema
<i>Verifica</i>	08/09/2020	Gabriele Bezzi	Responsabile funzione archivistica di conservazione
<i>Approvazione</i>	09/09/2020	Marco Calzolari	Responsabile del servizio

Il presente documento è rilasciato sotto la licenza

Attribuzione-Non commerciale

delle Creative Commons.



REGISTRO DELLE VERSIONI

Versione	Variazioni	Data
1.0	Prima emissione	27/11/2012
2.0	Revisione completa per adeguamento alle nuove Regole tecniche	09/10/2014
2.5 <i>[versione non pubblicata]</i>	Revisione per migrazione dell'infrastruttura tecnologica ed evoluzione applicativa. Correzione errori ortografici e/o di impaginazione e aggiornamento riferimenti Sono stati specificamente aggiornati: • Introduzione – Definizioni: aggiunta definizioni • Sezione 2: precisazione rapporti tra responsabili (par. 2.2) e struttura organizzativa (par. 2.3); aggiornamento denominazione aree • Sezione 5: revisione completa • Sezione 6: modifica denominazione	27/11/2015
2.9 <i>[versione non pubblicata]</i>	Adeguamento all'indice del manuale predisposto da AGID	28/01/2016
3.0	Adeguamento ai criteri di accessibilità richiesti da AGID e aggiornamento organigramma IBACN a luglio 2016	25/07/2016
4.0	Aggiornamento organizzazione interna di ParER e organigramma IBACN a luglio 2017 e revisione dell'architettura tecnica con aggiornamento glossario e revisione refusi.	27/10/2017
5.0 <i>[versione non pubblicata sul sito di AgID]</i>	Aggiornamento organizzazione interna di ParER e organigramma IBACN alla data dell'aggiornamento Aggiornamento per l'introduzione della nuova architettura di Business Continuity Aggiornamento per l'introduzione delle nuove tecnologie di storage con aggiornamento glossario Aggiornamento per l'adeguamento alle norme ISO 28017 e 27018 Aggiornamento per l'adeguamento alla norma ISO 9001 Aggiornamento per recepire i cambiamenti applicativi intercorsi dalla pubblicazione della versione 4.0 Aggiornamento per l'adeguamento al GDPR	26/09/2019
6.0	Aggiornamento organizzazione interna di ParER Aggiornamento per la sostituzione del gestore dell'infrastruttura di Disaster Recovery	09/09/2020

SOMMARIO

1	SCOPO E AMBITO DEL DOCUMENTO	7
2	TERMINOLOGIA (GLOSSARIO, ACRONIMI).....	8
3	NORMATIVA E STANDARD DI RIFERIMENTO	19
3.1	Normativa di riferimento	19
3.2	Standard di riferimento.....	20
4	RUOLI E RESPONSABILITÀ.....	23
4.1	Modello organizzativo	23
4.2	Produttore	26
4.3	Utente	28
4.4	Ente conservatore	29
4.5	Organismi di tutela e vigilanza.....	31
5	STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	34
5.1	Organigramma dell'IBACN.....	34
5.2	Struttura organizzativa del Servizio Polo Archivistico (ParER).....	35
6	OGGETTI SOTTOPOSTI A CONSERVAZIONE	42
6.1	Oggetti conservati.....	42
6.1.1	Unità archivistiche e Unità documentarie.....	46
6.1.2	Formati.....	47
6.1.3	Metadati.....	48
6.2	Pacchetto di versamento (SIP).....	49
6.3	Pacchetto di archiviazione (AIP)	50
6.4	Pacchetto di distribuzione (DIP)	51
7	PROCESSO DI CONSERVAZIONE	52
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	52
7.1.1	Preacquisizione	54
7.1.2	Acquisizione	55
7.2	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti.....	55
7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	56
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie.....	57
7.4.1	Monitoraggio	57
7.4.2	Gestione delle anomalie	59
7.5	Preparazione e gestione del Pacchetto di archiviazione.....	60
7.6	Preparazione e gestione del Pacchetto di distribuzione (DIP) ai fini dell'esibizione.....	63
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	64
7.8	Scarto dei pacchetti di archiviazione	65
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori ..	65

8	IL SISTEMA DI CONSERVAZIONE.....	67
8.1	Componenti logiche.....	67
8.2	Componenti tecnologiche	69
8.2.1	SacER.....	70
8.2.2	Verso	73
8.2.3	PING	73
8.2.4	DPI.....	74
8.2.5	Interfacce di Acquisizione e di Recupero (Web Service)	74
8.2.6	TPI	74
8.2.7	DIPS.....	75
8.2.8	SIAM	75
8.2.9	Sacerlog	76
8.2.10	Componenti di supporto	76
8.3	Componenti fisiche.....	78
8.3.1	Schema generale	78
8.3.2	Caratteristiche tecniche dei Sistemi	80
8.4	Procedure di gestione e di evoluzione	84
8.4.1	Gestione dell'Esercizio.....	84
8.4.2	Gestione delle utenze	84
8.4.3	Gestione dei Malfunzionamenti.....	85
8.4.4	Gestione degli Incidenti di Sicurezza	86
8.4.5	Evoluzione pianificata	88
8.4.6	Richieste di Cambiamento	88
8.4.7	Progettazione e Realizzazione di Software Applicativo	90
8.4.8	Gestione dei Rilasci	91
8.4.9	Gestione e conservazione dei Log	92
9	MONITORAGGIO E CONTROLLI.....	93
9.1	Procedure di monitoraggio	93
9.2	Funzionalità per la verifica e il mantenimento dell'integrità degli archivi	93
9.3	Soluzioni adottate in caso di anomalie	94
9.4	Verifica periodica di conformità a normativa e standard di riferimento.....	96
9.5	Audit e gestione delle Non Conformità	96
9.6	Controlli di sicurezza	98
10	TRATTAMENTO DEI DATI PERSONALI.....	99
11	DOCUMENTI DI RIFERIMENTO E ALLEGATI	102

INDICE DELLE FIGURE

<i>Figura 1 - Sistema e attori</i>	<i>26</i>
<i>Figura 2 - Organigramma IBACN</i>	<i>34</i>
<i>Figura 3 - Struttura organizzativa di ParER</i>	<i>38</i>
<i>Figura 4 - Modello di ordinamento di archivio derivato da ISAD</i>	<i>42</i>
<i>Figura 5 - Pacchetto informativo (da OAIS)</i>	<i>45</i>
<i>Figura 6 - Struttura dell'Unità documentaria</i>	<i>46</i>
<i>Figura 7 - Schema logico del Sistema di conservazione</i>	<i>67</i>
<i>Figura 8 - Flussi di dati nel Sistema di conservazione</i>	<i>69</i>
<i>Figura 9 - Schema Tecnologico del Sistema di conservazione</i>	<i>70</i>
<i>Figura 10 - Schema Infrastrutturale del Sistema di conservazione</i>	<i>79</i>
<i>Figura 11 - Schema dei Sistemi di ParER</i>	<i>81</i>
<i>Figura 12 - Schema del Sito Primario</i>	<i>82</i>
<i>Figura 13 - Procedura di Gestione utenze</i>	<i>85</i>
<i>Figura 14 - Procedura di Gestione richieste e malfunzionamenti</i>	<i>86</i>
<i>Figura 15 - Procedura di Gestione incidenti di sicurezza</i>	<i>87</i>
<i>Figura 16 - Procedura di Gestione richieste di cambiamento</i>	<i>89</i>
<i>Figura 17 - Procedura di Progettazione e realizzazione di software applicativo</i>	<i>90</i>
<i>Figura 18 - Procedura di Gestione dei rilasci</i>	<i>91</i>
<i>Figura 19 - Procedura di Audit del SGI</i>	<i>97</i>
<i>Figura 20 - Gestione delle Non Conformità</i>	<i>97</i>
<i>Figura 21 - Procedura di Verifiche Tecniche e VA/PT</i>	<i>98</i>

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il *Manuale di conservazione* (d'ora in poi Manuale) che descrive il sistema di conservazione applicato dall'Istituto per i beni artistici, culturali e naturali della Regione Emilia-Romagna (d'ora in poi IBACN) in quanto Conservatore. E' predisposto dal Servizio Polo archivistico dell'Emilia-Romagna (d'ora in poi ParER), che realizza e gestisce il *processo di conservazione*.

In particolare, il presente Manuale descrive il modello organizzativo della conservazione adottato e illustra nel dettaglio l'organizzazione della struttura che realizza il *Processo di conservazione*, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di *conservazione*. Descrive inoltre il processo, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del *Sistema di conservazione*.

Gli elementi illustrati e descritti sono validi e rilevanti per tutti gli enti per i quali IBACN svolge la funzione di *conservazione* e realizza e gestisce il *processo di conservazione* ai sensi della normativa nazionale e regionale, secondo il modello organizzativo descritto al paragrafo 4.1. Tali enti sono in primo luogo la Regione Emilia-Romagna, gli enti e gli organismi regionali, quali le agenzie, aziende e istituti e le aziende del Servizio Sanitario Regionale, oltre che gli enti del territorio regionale appositamente convenzionati. Inoltre, il presente Manuale è valido e rilevante anche per gli enti fuori dal territorio regionale, con cui sono stati stipulati appositi accordi.

Per le tipologie degli oggetti sottoposti a *conservazione* e i rapporti con i *Produttori* il presente Manuale deve essere integrato con il **Disciplinare tecnico** specifico per ogni *Produttore*, che definisce le specifiche operative e le modalità di descrizione e di versamento nel *Sistema di conservazione* digitale dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* oggetto di *conservazione*.

La documentazione di riferimento sia tecnica (p.e. specifiche tecniche di versamento, modelli di *pacchetti informativi*) che amministrativa (p.e. schemi di convenzione o accordo) ed altra eventuale documentazione di analisi di interesse generale sono pubblicate nel sito di ParER: <http://parer.ibc.regione.emilia-romagna.it/>.

[\[Torna al Sommario\]](#)

2 TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Per i termini utilizzati nel presente Manuale si rimanda al Glossario di cui all'Allegato 1 delle Regole Tecniche e alle definizioni del D.lgs. 82/2005 e del DPR 445/2000 e loro successive modificazioni e integrazioni. In generale la terminologia utilizzata si riferisce alle norme citate o a standard nazionali e internazionali.

Le definizioni riportate in ordine alfabetico in questo capitolo riguardano termini impiegati ripetutamente nel testo non presenti nelle citate fonti di cui si ritiene necessario fornire una definizione. Inoltre, sono riportate le definizioni sintetiche usate nel testo per citare la normativa e gli standard di riferimento, con la descrizione completa della fonte citata.

Nel testo del Manuale sono riportati in *corsivo* i termini riferiti al Glossario delle Regole tecniche e in ***corsivo grassetto*** i termini contenuti nel presente capitolo.

Allegato: **Documento** che compone l'**Unità documentaria** per integrare le informazioni contenute nel **Documento principale**. È redatto contestualmente o precedentemente al **Documento principale**.

Annesso: **Documento** che compone l'**Unità documentaria**, generalmente prodotto e inserito nell'**Unità documentaria** in un momento successivo a quello di creazione dell'**Unità documentaria**, per fornire ulteriori notizie e informazioni a corredo del **Documento principale**.

Annotazione: **Documento** che compone l'**Unità documentaria** riportante gli elementi identificativi del **Documento** e del suo iter documentale (un tipico esempio di Annotazione è rappresentato dalla segnatura di protocollo).

Applet: programma che viene eseguito come "ospite" nel contesto di un altro programma, detto per questo container, su un computer client [...]. In altre parole, un applet è un programma progettato per essere eseguito all'interno di un programma-container; ne consegue che l'applet non può essere eseguito indipendentemente da un altro programma. (Fonte: Wikipedia)

Appliance: particolare dispositivo elettronico hardware provvisto di un software integrato con funzione di sistema operativo, utilizzato per eseguire particolari complesse e massicce funzioni applicative software. La differenza sostanziale con i normali server o le normali apparecchiature di rete è che l'appliance non è progettato per essere flessibile alle modifiche del software o dell'hardware successive alla configurazione e installazione fatta per la sua specifica funzione applicativa. (Fonte: Wikipedia)

Application server: tipologia di server che fornisce l'infrastruttura e le funzionalità di supporto, sviluppo ed esecuzione di applicazioni nonché altri componenti server in un contesto distribuito. Si tratta di un complesso di servizi orientati alla realizzazione di applicazioni ad architettura multilivello ed enterprise, con alto grado di complessità, spesso orientate per il web (applicazioni web). (Fonte: Wikipedia)

Archiving: processo di spostamento di dati che non sono utilizzati frequentemente su un dispositivo che ne garantisce la memorizzazione nel lungo periodo.

Autenticazione forte: procedura basata sull'utilizzo di due o più dei seguenti elementi [...] (i) qualcosa che solo l'utente conosce, p.e. una password [...] (ii) qualcosa che solo l'utente possiede, p.e. [...] un telefono cellulare (iii) qualcosa che caratterizza l'utente, p.e. [...] un'impronta digitale. (Fonte: Traduzione di citazione di Wikipedia inglese di un testo della Banca Centrale Europea)

Backup: replicazione, su un qualunque supporto di memorizzazione, di materiale informativo archiviato nella memoria di massa dei computer, al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali. (Fonte: Wikipedia)

Bilanciamento di carico: tecnica informatica che consiste nel distribuire il carico di elaborazione di uno specifico servizio tra più server. Si aumentano in questo modo la scalabilità e l'affidabilità dell'architettura nel suo complesso. (Fonte: Wikipedia)

BLOB: acronimo per Binary Large object; tipo di dato usato nei database per la memorizzazione di dati di grandi dimensioni in formato binario. (Fonte: Wikipedia)

Business intelligence (BI): un'applicazione di BI è uno strumento software che, acquisendo e manipolando masse di dati presenti su database o anche archivi de-strutturati, fornisce report, statistiche, indicatori, grafici costantemente aggiornati, facilmente adattabili e configurabili. (Fonte: Wikipedia)

Client: componente che accede ai servizi o alle risorse di un'altra componente detta server. Il termine client indica anche il software usato sul computer client per accedere alle funzionalità offerte dal server. (Fonte: Wikipedia)

Cloud computing: paradigma di erogazione di servizi offerti su richiesta da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita. (Fonte: Wikipedia)

Cloud Marketplace di AgID: piattaforma che espone i servizi e le infrastrutture qualificate da AgID secondo quanto disposto dalle Circolari AgID n. 2 e n.3 del 9 aprile 2018. A decorrere dal 1 aprile 2019, le Amministrazioni Pubbliche possono acquisire esclusivamente servizi qualificati da AgID e pubblicati nel Cloud Marketplace. (Fonte: AgID)

Cluster: insieme di dispositivi di elaborazione connessi in maniera più o meno stretta che operano insieme in modo tale da poter essere considerati un unico sistema. (Fonte: Wikipedia)

Componente: elemento che compone il **Documento**. Generalmente è un file, ma può essere anche composto solo da *metadati*.

Comunità di riferimento: un gruppo ben individuato di potenziali *Utenti* che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La Comunità di riferimento può essere composta da più comunità di *Utenti*. [da **OAIS**]

Contenuto informativo: l'insieme delle informazioni che costituisce l'obiettivo originario della *conservazione*. E' composto dall'**Oggetto-dati** e dalle **Informazioni di rappresentazione**. [da **OAIS**]

Continuità Operativa (Business Continuity): capacità di un'organizzazione di continuare a erogare prodotti o servizi a livelli predefiniti accettabili a seguito di un incidente. Si tratta di una disciplina di gestione che consente all'organizzazione - privata o pubblica che sia - di diventare più resiliente agli incidenti che potrebbero causarne l'interruzione delle attività o addirittura minacciarne l'esistenza. [...] Erroneamente, viene spesso confusa con il **Disaster Recovery** che è solo una parte specifica della business continuity, relativa in particolare ai processi informatici. La continuità operativa ha un campo di applicazione più ampio e prevede riflessioni anche su persone, siti, risorse e fornitori dell'organizzazione.

Convenzione: accordo tra il *Produttore* e ParER, che regola i rapporti di servizio, e più precisamente: la natura dei servizi offerti, la responsabilità delle parti e le condizioni economiche, oltre agli strumenti di consultazione e controllo. Con il termine Convenzione si intendono sia le convenzioni propriamente dette, sottoscritte con gli Enti del territorio dell'Emilia-Romagna, sia gli accordi di collaborazione sottoscritti con Enti di altri territori nazionali.

Data Center: struttura utilizzata per ospitare computer e componenti associati quali dispositivi di telecomunicazioni e di **storage**, in generale con adeguati livelli di prestazioni e di sicurezza. (Fonte: Wikipedia)

Data Breach: Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. (Fonte: GarantePrivacy)

Data Guard: estensione del database Oracle che consente di mantenere dei database secondari allineati ad un database primario. (Fonte: Wikipedia)

DICOM (Digital Imaging and COmmunications in Medicine): standard che definisce i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni di tipo biomedico quali ad esempio immagini radiologiche. (Fonte: Wikipedia)

Disaster recovery: insieme delle misure tecnologiche e logistico / organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività. (Fonte: Wikipedia)

Disciplinare tecnico: documento redatto con ogni *Produttore*, che definisce le specifiche operative e le modalità di descrizione e di versamento nel *Sistema di conservazione* digitale dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* oggetto di *conservazione*.

DNS (Domain Name System): sistema utilizzato per la risoluzione di nomi dei nodi della rete in indirizzi IP e viceversa. (Fonte: Wikipedia)

Documenti di conservazione: evidenze informatiche prodotte nel corso del processo di conservazione o da altri *sistemi di conservazione*.

Documento: nell'uso del presente Manuale, elemento dell'**Unità documentaria**. Si distingue in **Documento principale**, **Allegato**, **Annesso**, **Annotazione**. Si tratta comunque di un **Documento archivistico (Record)**.

Documento archivistico (Record): Informazioni memorizzate su qualsiasi supporto o tipologia documentaria, prodotte o ricevute e conservate da un ente o da una persona nello svolgimento delle proprie attività o nella condotta dei propri affari. [fonte: **ISAD**]

Documento principale: Documento che deve essere obbligatoriamente presente nell'**Unità documentaria**, della quale definisce il contenuto primario.

EJB (Enterprise JavaBean): componenti software che implementano, lato server, la logica di business di un'applicazione web all'interno della piattaforma **J2EE**. (Fonte: Wikipedia)

Elenco di versamento: documento in formato XML in cui sono indicati i *Documenti informatici* e le *Aggregazioni documentali informatiche* acquisiti dal *Sistema di conservazione* e una serie di informazioni relative alle verifiche a cui sono stati sottoposti durante il processo di acquisizione e *presa in carico*.

Esito versamento: documento in formato XML prodotto al termine delle verifiche in fase di **versamento**, memorizzato nel *Sistema di conservazione* ed inviato al sistema versante.

File system: meccanismo con il quale i file sono posizionati e organizzati o su un dispositivo di archiviazione o su una memoria di massa, come un disco rigido o un CD-ROM e, in casi eccezionali, anche sulla RAM. (Fonte: Wikipedia)

Firma detached: firma digitale che è tenuta separata dai dati firmati, a differenza della firma digitale completa che è inglobata nel file stesso. Ciò permette di poter lavorare con il file originale senza dover aprire un file firmato digitalmente, ma ovviamente una qualsiasi modifica al file originale interrompe lo stretto legame con la firma, nel senso che un file differente non possiederà la medesima firma. (Fonte: Wikipedia)

Firewall: componente di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più tronconi di rete, garantendo dunque una protezione in termini di sicurezza informatica della rete stessa. (Fonte: Wikipedia)

Framework di sviluppo: architettura logica di supporto su cui un software può essere progettato e realizzato, spesso facilitandone lo sviluppo da parte del programmatore. (Fonte: Wikipedia)

FTP (File Transfer Protocol): protocollo per la trasmissione di dati tra host (client) e server, particolarmente adatto al trasferimento di file di grandi dimensioni. (Fonte: Wikipedia)

FTPS (File Transfer Protocol Secure): estensione del protocollo **FTP** con utilizzo di protocolli crittografici. (Fonte: traduzione di Wikipedia inglese)

FTP server: programma che permette di accettare connessioni in entrata e di comunicare con un **client** attraverso il protocollo **FTP**. (Fonte: Wikipedia)

GDPR: Regolamento (UE) del 27 aprile 2016, n. 679, del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), noto con l'acronimo GDPR (General Data Protection Regulation).

Grant: istruzione SQL utilizzata per fornire a uno specifico utente o ruolo o a tutti gli utenti i privilegi necessari per eseguire delle azioni su oggetti di data base. (Fonte: tradotto da Oracle inglese)

HSM (Hardware Security Module): dispositivo fisico che garantisce e gestisce chiavi digitali per l'**autenticazione forte** e realizza processi di crittografia. Questi moduli in generale hanno la forma di una scheda o di un dispositivo esterno che si connette a un computer o a un server di rete (Fonte: tradotto da Wikipedia inglese)

HTTP (HyperText Transfer Protocol): principale protocollo utilizzato per la trasmissione d'informazioni sul web. (Fonte: Wikipedia)

HTTPS (HyperText Transfer Protocol over Secure Socket Layer): risultato dell'applicazione di un protocollo di crittografia al protocollo di trasmissione **HTTP**. (Fonte: Wikipedia)

IdP (Identity Provider): strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un sistema. Ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza. (Fonte: Wikipedia)

Incidente di sicurezza delle informazioni: Evento o serie di eventi relativo alla sicurezza delle informazioni, non voluti o inattesi, che hanno una probabilità significativa di compromettere le attività istituzionali o di affari e di minacciare la sicurezza delle informazioni. (Def. 2-36 STD ISO27000:2014).

Indice dell'AIP: file XML che contiene tutti gli elementi del *Pacchetto di archiviazione*, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal *Produttore*, sia da quelle generate dal *Sistema di conservazione* nel corso del *processo di conservazione*.

Indice del SIP: file XML che contiene i *metadati* e la struttura del *Sistema di versamento*, nonché i riferimenti ai file dei **Componenti**.

Indirizzo IP: etichetta numerica che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete. (Fonte: Wikipedia)

Informazioni descrittive: descrivono il *pacchetto informativo* e consentono di ricercarlo nel *sistema di conservazione*. In base alle caratteristiche della tipologia di oggetto contenuto nel Pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel *pacchetto informativo*, possono coincidere o possono anche essere diverse.

Informazioni sulla conservazione (PDI): informazioni necessarie a conservare il **Contenuto informativo** e a garantire che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da *metadati* che definiscono la provenienza, il contesto, l'identificazione e l'integrità del **Contenuto informativo** oggetto della *conservazione*. [da **OAIS**]

Informazioni sulla rappresentazione: informazioni che associano un **Oggetto-dati** a concetti più significativi. [da **OAIS**]

Informazioni sull'impacchettamento (PI): informazioni che consentono di mettere in relazione nel *Sistema di conservazione*, in modo stabile e persistente, il **Contenuto informativo** con le relative **Informazioni sulla conservazione**. [da **OAIS**]

ISAD: ICA - ISAD (G): General International Standard Archival Description - Second Edition - Adopted by the Committee on Descriptive Standards Stockholm, Sweden, 19-22 September 1999.

Istanza: copia dell'applicativo dedicata ad uno scopo specifico.

JAVA: piattaforma software che ha come caratteristica peculiare il fatto di rendere possibile la scrittura e l'esecuzione di applicazioni scritte in linguaggio Java che siano indipendenti dall'hardware sul quale poi sono eseguite. (Fonte: Wikipedia)

J2EE (Java Platform, Enterprise Edition): specifica le cui implementazioni vengono principalmente sviluppate in linguaggio di programmazione Java e ampiamente utilizzata nella programmazione Web. Ha come scopo la separazione delle funzionalità relative alla visualizzazione delle pagine web da quelle per la gestione della logica di business e del salvataggio delle informazioni sulla base dati. (Fonte: Wikipedia)

Lepida: rete delle Pubbliche Amministrazioni dell'Emilia-Romagna istituita dalla legge regionale n. 11/2004, principalmente costituita da collegamenti in fibra ottica ed estesa nel territorio appenninico attraverso dorsali radio in tecnologia Hyperlan. (Fonte: sito di Lepida SpA)

Magic number: sequenza di bit, normalmente posta prima della sequenza di dati, che serve per definire il formato in cui i dati sono memorizzati. [...] Oggi la maggior parte dei formati del file hanno un magic number, costituito da un numero di byte variabile (solitamente da 2 a 10). I file immagine GIF, per esempio, cominciano sempre con la stringa ASCII GIF87a o GIF89a che definisce lo standard al quale il file aderisce. [...] I file PDF iniziano con "%PDF". (Fonte: Wikipedia)

Marca temporale: sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione della marca temporale è detta *timestamping*. (Fonte: Wikipedia)

Massimario di scarto: vedi **Piano di Conservazione**.

Microservizi: approccio architetturale alla realizzazione di applicazioni caratterizzata dalla suddivisione dell'applicazione nelle sue funzioni di base. Ciascuna funzione, denominata servizio,

può essere compilata e implementata in modo indipendente. Pertanto, i singoli servizi possono funzionare, o meno, senza compromettere gli altri (Fonte: RedHat)

Migrazione: procedimento atto a trasformare il software, l'hardware, oppure i dati nell'ambito di un sistema informativo o nel passaggio da un sistema ad un altro.

Mimetype: identificatore standard utilizzato su internet per indicare il tipo di dati contenuti in un file. I mimetype sono definiti in un Registro ufficiale gestito dalla Internet Assigned Numbers Authority (IANA). (Fonte: Wikipedia)

Multi-tenant: architettura software in cui una singola istanza del software è eseguita da un server ed è fruita da diverse organizzazioni che, ciascuna con le sue peculiarità ambientali che costituiscono concettualmente uno specifico tenant, vedono il software come a loro utilizzo esclusivo. (Fonte: Wikipedia)

Near-line: termine usato in informatica per descrivere un tipo intermedio di archiviazione dati che rappresenta un compromesso tra lo storage on-line (con accesso ai dati frequente, molto rapido) e storage/archiviazione off-line (usato ad esempio per i backup, con accesso infrequente ai dati). (Fonte: Wikipedia)

NOC (Networking Operations Center): sito (o insieme di siti) da cui viene effettuato il controllo dell'operatività di una rete di apparecchiature informatiche e di server (Fonte: tradotto da Wikipedia inglese)

NTP (Network Time Protocol): protocollo per sincronizzare gli orologi dei computer all'interno di una rete. (Fonte: Wikipedia)

OAIS: ISO 14721:2012: Space data and information transfer systems -- Open archival information system - Reference model, OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.

Object storage: architettura di calcolatori dedicati alla memorizzazione di dati, che gestisce i dati come oggetti, anziché come gerarchia di file, come fanno i file system; ogni oggetto contiene i dati, una quantità variabile di metadati e un identificatore univoco. (Fonte: tradotto da Wikipedia inglese)

Oggetto-dati o Oggetto digitale: un oggetto composto da un insieme di sequenze di bit. [da **OAIS**]

Raccolta di archiviazione (AIC): Un Pacchetto di archiviazione (AIP), il cui contenuto informativo è costituito da un insieme di altri Pacchetti di archiviazione, in particolare aggregazione di AIP delle singole unità documentarie appartenenti all'aggregazione. [da **OAIS**]

PACS: acronimo anglosassone di Picture Archiving and Communication System (Sistema di archiviazione e trasmissione di immagini). Consiste in un sistema hardware e software dedicato all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali. (Fonte: Wikipedia)

Partitioning: suddivisione di un database o dei suoi costituenti in parti indipendenti; viene utilizzata per ragioni di performance, gestibilità e disponibilità dei dati. (Fonte: tradotto da Wikipedia inglese)

Penetration test: processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato. (Fonte: Wikipedia)

Persistenza: possibilità di far sopravvivere delle strutture dati all'esecuzione di un singolo programma, salvando i dati in uno storage non volatile, come su un *file system* o su un database. (Fonte: Wikipedia)

Piano di conservazione: L'art. 68 del DPR 445/2000 (Disposizioni per la conservazione degli archivi), prevede la dotazione da parte dell'ente di un piano di conservazione degli archivi, che deve consentire di selezionare i documenti destinati alla conservazione permanente oppure di identificare quelli passibili di scarto, secondo quanto indicato nel Massimario di Scarto, nel rispetto delle disposizioni vigenti in materia di tutela dei beni culturali

Protocollo di rete: descrizione a livello logico del processo di comunicazione (meccanismi, regole o schema di comunicazione) tra terminali e apparati preposto al funzionamento efficace della comunicazione in rete. (Fonte: Wikipedia)

Proxy: un server proxy è un server (inteso come sistema informatico o applicazione) che funge da intermediario per le richieste da parte dei client alla ricerca di risorse su altri server, disaccoppiando l'accesso al web dal browser. Un client si connette al server proxy, richiedendo qualche servizio (ad esempio un file, una pagina web o qualsiasi altra risorsa disponibile su un altro server), e quest'ultimo valuta ed esegue la richiesta in modo da semplificare e gestire la sua complessità. (Fonte: Wikipedia)

RAC: In un ambiente Oracle RAC due o più computer, ognuno con un'istanza del software accedono contemporaneamente allo stesso database. Ciò consente a un'applicazione o a un utente di connettersi a ambedue i computer. mantenendo un accesso coordinato ai dati. (Fonte: tradotto da Wikipedia inglese)

Regole tecniche: Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Release: specifica versione di un software resa disponibile ai suoi utenti finali. La release è univocamente identificata da un numero in modo da distinguerla dalle precedenti e future altre release del software. Convenzionalmente si distinguono release maggiori, dette *major release*, quando le differenze dalla release precedente riguardano sostanziali evoluzioni delle funzionalità del software, e release minori, dette *minor release*, quando le differenze riguardano principalmente correzioni di malfunzionamenti del software. (Fonte: Wikipedia)

ReST (REpresentational State Transfer): insieme di principi di architetture di rete, i quali delineano come le risorse sono definite e indirizzate. Il termine è spesso usato nel senso di descrivere ogni semplice interfaccia che trasmette dati su **HTTP** senza un livello opzionale. (Fonte: Wikipedia)

S3: Servizio di **Object storage** accessibile via web fornito da Amazon; per l'accesso al servizio da parte degli applicativi Amazon mette a disposizione funzionalità di interfaccia che sono diventate uno standard de facto, accettato da molti dei sistemi di **Object storage** presenti sul mercato.

SCP (Secure Copy): protocollo per trasferire in modo sicuro un file tra un computer locale ed un host remoto o tra due host remoti. (Fonte: Wikipedia)

Serie: Unità Archivistiche o Unità Documentarie ordinate secondo un *sistema di classificazione* o conservati insieme perché:

- sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività;
- appartengono ad una specifica **tipologia documentaria**;
- a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso.

(fonte: **ISAD**)

SaaS (Software as a Service): modello di distribuzione del software applicativo dove un produttore di software sviluppa, opera e gestisce un'applicazione web che mette a disposizione dei propri clienti via Internet; spesso si tratta di un servizio di **cloud computing**. (Fonte: Wikipedia)

Servlet container: componente di un web server che interagisce con i servlet, ovvero con programmi in linguaggio Java atti alla generazione dinamica di pagine web. (Fonte: tradotto da Wikipedia inglese)

SGI: Sistema di Gestione Integrato, che armonizza il Sistema di Gestione della Qualità (SGQ) e il Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

SICTR (Servizio ICT - Information and Communication Technology Regionale): struttura organizzativa della Regione Emilia-Romagna deputata, in base a quanto previsto dalle Delibere di Giunta n. 270/2016 e 622/2016, a gestire le infrastrutture informatiche, a fissare gli standard informatici e di rete, a progettare, sviluppare e gestire i sistemi informativi "centrali", a gestire la sicurezza informatica degli strumenti informatici ed apparati di rete utilizzati per le attività della Regione e degli Enti / Agenzie che fruiscono a vario titolo dei servizi informatici e di rete regionali

SIEM (Security Information and Event Management): le soluzioni rientranti in questa categoria di sistemi sono contraddistinte dalla capacità di effettuare analisi real-time degli allarmi di sicurezza generati dagli apparati hardware di rete e dalle applicazioni software di gestione e monitoraggio.

Le soluzioni SIEM sono anche impiegate per effettuare il log delle informazioni di sicurezza e generare dei report funzionali alle tematiche di rispetto delle norme e degli standard. (Fonte: Wikipedia)

SOC (Security Operation Center): centro da cui vengono forniti servizi finalizzati alla sicurezza dei sistemi informativi dell'azienda stessa o di clienti esterni.

Un SOC fornisce tre tipologie di servizi:

- di gestione: tutte le attività di gestione delle funzionalità di sicurezza legate all'infrastruttura IT (rete, sistemi ed applicazioni) sono centralizzate dal SOC;
 - di monitoraggio: l'infrastruttura IT e di Sicurezza vengono monitorate in tempo reale al fine di individuare tempestivamente tentativi di intrusione, di attacco o di uso malevolo dei sistemi;
 - proattivi: sono servizi finalizzati a migliorare il livello di protezione dell'organizzazione.
- (Fonte: Wikipedia)

Sotto componente: *Componente* di un *Componente*. Per esempio, sono *Sotto componenti* la **marca temporale** (se detached) o la Firma digitale (sempre se detached) di un determinato *Componente*.

Storage: dispositivo per memorizzare i dati in formato digitale; sono considerati storage sia i dispositivi a cassette che i dispositivi a disco.

Struttura versante (o Struttura): ripartizione dell'Ente produttore identificativa della specifica area di produzione dei documenti versati, in genere coincidente con l'*area organizzativa omogenea*.

Tape library: sistema automatico composto da alloggiamenti contenenti cassette magnetiche, dispositivi di lettura/scrittura delle cassette stesse e dispositivi di riconoscimento automatico delle cassette. (Fonte: Wikipedia)

Tempo UTC (Tempo coordinato universale): fuso orario di riferimento da cui sono calcolati tutti gli altri fusi orari del mondo. Esso è derivato dal tempo medio di Greenwich (in inglese Greenwich Mean Time, GMT), con il quale coincide a meno di approssimazioni infinitesimali, e perciò talvolta è ancora chiamato, sia pure impropriamente, GMT. (Fonte: Wikipedia)

Tipologia documentaria: categoria di documenti omogenei per natura e funzione giuridica, modalità di registrazione o di produzione, che hanno comuni caratteristiche formali e/o intellettuali; nel sistema SacER, che fa riferimento al più complesso concetto di *Unità Documentaria*, anziché di Documento, si preferisce parlare di "Tipo di Unità Documentaria"

Trouble ticket: sistema informatico che gestisce e registra delle liste di richieste di assistenza o di problemi, organizzato secondo le necessità di chi offre il servizio. [...] Un ticket o biglietto, serve per tenere il filo di una richiesta. Ad ogni biglietto corrisponde un identificativo univoco, che ne consente l'archiviazione e la consultazione in qualunque momento, da parte del personale coinvolto nella sua chiusura. I biglietti vengono 'creati' o 'aperti', all'atto della ricezione di una nuova richiesta, e l'obiettivo è di 'chiuderli' o 'risolverli', fornendo la soluzione al problema segnalato. (Fonte: Wikipedia)

Unità archivistica: insieme organizzato di *Unità documentarie* o *Documenti* raggruppati dal *Produttore* per le esigenze della sua attività corrente in base al comune riferimento allo stesso oggetto, attività o fatto giuridico. Può rappresentare una unità elementare di una *Serie*. [da **ISAD**]

Unità di archiviazione (AIU): Un **Pacchetto di archiviazione** (AIP) elementare, il cui contenuto informativo non è ulteriormente decomposto in altri contenuti informativi. Definisce un AIP di Unità documentaria. .[da **OAIS**]

Unità documentaria (*item*): aggregato logico costituito da uno più **Documenti** che sono considerati come un tutto unico. Costituisce l'unità elementare in cui è composto l'*archivio*, cioè l'unità minima, concettualmente non divisibile, di cui è composto un archivio o in altri termini, la più piccola distinta unità di **Documenti** gestita come entità. Può contenere componenti, come ad esempio una e-mail con allegati; comunque i componenti dell'Unità documentaria sono gestiti come una singola entità nel sistema. [da **ISAD e da ISO 23081**]

Versamento: azione di *trasferimento* di SIP dal *Produttore* al *Sistema di conservazione*.

Versamento anticipato: **versamento** nel *Sistema di conservazione* di *Documenti informatici* che si trovano ancora nella fase attiva del loro ciclo di vita.

Versamento in archivio: **versamento** nel Sistema di *Aggregazioni documentali informatiche* nella loro forma stabile e definitiva (principalmente Fascicoli chiusi e **Serie** annuali complete), ovvero che hanno esaurito il loro ciclo di vita attivo per entrare in quello semi-attivo.

Vulnerabilità: componente di un sistema, in corrispondenza della quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole del sistema e consente a un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema. (Fonte: Wikipedia)

Vulnerability assessment: processo che porta a identificare, quantificare, valutare la priorità (o l'importanza) delle **vulnerabilità** in un sistema. (Fonte: tradotto da Wikipedia inglese)

Web Server: applicazione software che, in esecuzione su un server, è in grado di gestire le richieste di trasferimento di pagine web di un client, tipicamente un web browser, tramite il protocollo **HTTP** o eventualmente la versione sicura **HTTPS**. (Fonte: Wikipedia)

Web Service: un sistema software progettato per supportare l'*interoperabilità* tra diversi sistemi in una medesima rete oppure in un contesto distribuito. (Fonte: Wikipedia)

ZIP: formato di compressione dei dati molto diffuso nei computer con sistemi operativi Microsoft e supportato di default nei computer con sistema operativo Mac OS X. Supporta vari algoritmi di compressione. (Fonte: Wikipedia)

[\[Torna al Sommario\]](#)

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Le normative in vigore nei luoghi dove sono conservati i documenti, cioè normativa europea, nazionale italiana e regionale dell'Emilia-Romagna e gli standard di riferimento sono riportati in modo più dettagliato e secondo la gerarchia delle fonti nell'Allegato 1 "Normativa e standard di riferimento" che viene mantenuto costantemente aggiornato e pubblicato on-line sul sito di ParER.

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica.

Legge del 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Decreto Legislativo 10 agosto 2018, n. 101 che ha dettato disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.

Decreto Legislativo del 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali.

Decreto Legislativo del 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio.

Decreto Legislativo del 7 marzo 2005 n. 82 e s.m.i – Codice dell'amministrazione digitale (CAD).

Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71.

Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - “Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005”.

Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

Circolare AGID del 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Circolare AgID del 9 aprile 2018, n. 2 – Criteri per la qualificazione dei Cloud Service Provider per la PA

Circolare AgID del 9 aprile 2018, n. 3 – Criteri per la qualificazione di servizi SaaS per il Cloud della PA

[\[Torna al Sommario\]](#)

3.2 Standard di riferimento

ICA - ISAD (G): General International Standard Archival Description - Second Edition -Adopted by the Committee on Descriptive Standards Stockholm, Sweden, 19-22 September 1999. Traduzione italiana a cura di Stefano Vitali, con la collaborazione di Maurizio Savoja, Firenze 2000. Standard dell'ICA (International Council on Archives – Conseil International des Archives) che fornisce delle norme generali per l'elaborazione di descrizioni archivistiche.

ISO 14721:2012 – Open Archival Information System (OAIS) – Reference model (CCSDS 650.0-M-2, Recommend Practice, Magenta Book June 2012): definisce concetti, modelli e funzionalità inerenti agli archivi digitali e ciò che è richiesto per garantire una conservazione permanente, o per un lungo termine indefinito, di informazioni digitali. Questa versione sostituisce la prima (ISO 14721:2003 - CCSDS 650.0-B-1 – Blue Book, January 2002) di cui è disponibile una traduzione in italiano (Sistema informativo aperto per l'archiviazione: traduzione italiana: *OAIS. Sistema informativo aperto per l'archiviazione*, a cura di Giovanni Michetti, Roma, ICCU 2007).

ISO 16363:2012 - Space data and information transfer systems - Audit and certification of trustworthy digital repositories (CCSDS 652.0-M-1 Recommend Practice, Magenta Book September 2011).

ISO 15836:2009 - Information and documentation – The Dublin Core metadata element set. Sistema di metadati del Dublin Core (questa versione sostituisce la precedente: ISO 15836:2003).

ISO 23081-1:2006 - Information and documentation – Records management processes – Metadata for records – Part 1- Principles. Quadro di riferimento per lo sviluppo di un Sistema di metadati per la gestione documentale.

ISO/TS 23081-2:2007: - Information and documentation – Records management processes – Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione.

ISO 23081-2:2009: - Information and documentation – Managing Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione.

LTO6: LTO (Linear Tape Open) è uno standard "open" sviluppato alla fine del 1990 come tecnologia di storage dei dati su nastro. La versione 6 è stata definita alla fine del 2012.

PREMIS: Data Dictionary for Preservation Metadata. Risultato dell'attività di un gruppo di lavoro transnazionale costituito nel 2003, definisce l'insieme essenziale di metadati necessari per tracciare il processo di conservazione. La versione 3.0 è stata definita nel giugno del 2015 e rivista nel novembre 2015.

SQL: (Structured Query Language) è un linguaggio standardizzato per database basati sul modello relazionale (RDBMS).

UNI 11386:2010: - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI SInCRO): Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali: definisce la struttura dell'insieme di dati a supporto del processo di conservazione; in particolare, precisa e integra alcune disposizioni contenute nella Deliberazione CNIPA 19 febbraio 2004, n. 11, individuando gli elementi informativi necessari alla creazione dell'indice di conservazione e descrivendone sia la semantica sia l'articolazione per mezzo del linguaggio formale XML. L'obiettivo della norma è di consentire agli operatori del settore di utilizzare una struttura-dati condivisa al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, grazie all'adozione dello Schema XML appositamente elaborato.

UNI ISO 15489-1:2006: Informazione e documentazione – Gestione dei documenti di archivio – Principi generali sul record management.

UNI ISO 15489-2:2007: Informazione e documentazione – Gestione dei documenti di archivio – Linee guida sul record management.

ISO/IEC 9001:2015: requisiti per la realizzazione all'interno di un'organizzazione di un sistema di gestione della qualità.

ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems -- Requirements. Requisiti di un ISMS (Information Security Management System).

ISO/IEC 27017:2015: Codice di condotta per i controlli di sicurezza delle informazioni per i servizi in cloud.

ISO/IEC 27018:2014: - Codice di condotta per la protezione delle informazioni di identificazione personale (PII) in cloud pubblici.

ISO 22301:2012: Societal security -- Business continuity management systems --- Requirements.

ETSI TS 101 533-1 v1.3.1 (2012-04) - Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management. Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

ETSI TR 101 533-2 v1.3.1 (2012-04) - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors. Linee guida per valutare sistemi sicuri e affidabili per la conservazione delle informazioni.

[\[Torna al Sommario\]](#)

4 RUOLI E RESPONSABILITÀ

4.1 Modello organizzativo

La Regione Emilia-Romagna con la legge regionale 24 ottobre 2013 n. 17¹, che ha apportato modifiche alle leggi regionali 11/2004 (Sviluppo regionale della società dell'informazione) e 29/1995 (Riordinamento IBACN), ha definito la propria declinazione del modello organizzativo per la conservazione stabilendo, all'art. 2 comma 4bis, che:

*La Regione, anche in collaborazione con le altre pubbliche amministrazioni interessate, favorisce altresì lo sviluppo integrato della conservazione digitale dei documenti informatici e, nel rispetto dei principi di efficacia, efficienza ed economicità, svolge le funzioni di archiviazione e conservazione digitale dei documenti informatici secondo quanto disposto dall'articolo 2, comma 1 lettera f bis) della legge regionale 10 aprile 1995, n. 29 [art. 2 comma 4 bis L.R. 11/2004]*²

A sua volta il citato articolo 2, comma 1 lettera f bis della L.R. 29/1995 nella sua nuova versione stabilisce che l'Istituto per i beni artistici culturali e naturali (IBACN):

"svolge le funzioni di archiviazione e conservazione digitale dei documenti informatici anche a rilevanza fiscale, con le modalità previste dalle disposizioni vigenti, prodotti o ricevuti dalla Regione e dagli altri soggetti di cui all'articolo 19, comma 5, lettera a) della legge regionale 24 maggio 2004, n. 11 nonché, mediante apposita convenzione, dei documenti informatici prodotti o ricevuti dai soggetti di cui all'articolo 19, comma 5, lettera b) della medesima legge e da altri soggetti pubblici"

I soggetti indicati al citato articolo 19 sono rispettivamente:

- a) *la Regione, gli enti e gli organismi regionali, le loro associazioni e consorzi, quali le agenzie, le aziende e gli istituti, anche autonomi, nonché gli enti e le aziende del Servizio sanitario regionale, ed inoltre gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria dai soggetti precedenti*
- b) *gli Enti locali, i loro enti e organismi, le loro associazioni, unioni e consorzi, quali le aziende e gli istituti, anche autonomi, le istituzioni, gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria da tali soggetti, ed inoltre gli istituti di istruzione scolastica e universitaria presenti e operanti nel territorio regionale*

I soggetti elencati al punto a), ai sensi del comma 3 dell'art. 16 della L.R. 11/2004³ sono "obbligati" ad utilizzare le funzioni di archiviazione e conservazione digitale dei documenti informatici svolte da IBACN ai sensi del citato articolo della L.R. 29/1995. Invece quelli elencati al punto b) hanno la facoltà di utilizzare le funzioni di conservazione svolte da IBACN.

Riassumendo si può dire che il modello organizzativo definito dalla Regione Emilia-Romagna è che **IBACN svolge le funzioni di archiviazione e conservazione digitale per la Regione e gli altri enti sopracitati, in particolare gli enti e le aziende del Servizio sanitario**

¹ Pubblicata nel BURERT n. 313 del 24 ottobre 2013

² Modifica apportata dall'articolo 2 della L. R. 17/2013

³ Così come modificato dall'articolo 9 della L.R. 17/2013

regionale, nella logica di sviluppo integrato della conservazione digitale dei documenti informatici nel rispetto dei principi di efficacia, efficienza ed economicità.

Il modello rientra in quanto previsto dalle vigenti **Regole tecniche** alla lettera b) del comma 2 dell'articolo 5, ma si tratta di un modello rafforzato da una norma di legge regionale ed inserito in una più ampia visione di sistema regionale allargato. Infatti per garantire risparmi ed efficienza si concentra in un soggetto specializzato una funzione complessa come quella della conservazione degli oggetti digitali.

IBACN, ai sensi del citato art. 2 comma 4bis della L.R. 11/2004 e dell'art. 1 comma 1 bis della L.R. 29/1995, introdotto con l'art. 38 della L.R. n. 9/2015,⁴ può inoltre collaborare con pubbliche amministrazioni interessate di tutto il territorio nazionale.

L'idea progettuale di realizzare centri di conservazione digitale, cioè "strutture dedicate alla conservazione della memoria digitale di più soggetti *Produttori*, dotate di personale archivistico e informatico altamente qualificato" era già presente nel progetto DOCAREA presentato ed attuato nell'ambito del piano nazionale di e-government su iniziativa e coordinamento della Provincia di Bologna⁵.

All'interno di tale progetto si era infatti maturata l'idea che il complesso delle attività da svolgere, i requisiti giuridici da soddisfare e le competenze professionali necessarie per la corretta conservazione degli *archivi informatici* non fossero alla portata della maggior parte delle pubbliche amministrazioni, richiedendo risorse – finanziarie, umane e strumentali – troppo elevate per ogni singola organizzazione. Di qui la concezione di un polo di conservazione digitale, concepito come archivio unico di concentrazione servente più *Produttori*, che si proponesse di offrire una soluzione condivisa, affidabile e tempestiva al problema della conservazione dei documenti informatici delle pubbliche amministrazioni.

Questa struttura, inizialmente pensata a livello provinciale e denominata Archive Service Center (ASC), già durante lo svolgimento del progetto DOCAREA venne portata, proprio per il livello di complessità e di risorse richieste, ad una dimensione regionale assumendo la denominazione di Polo archivistico regionale dell'Emilia-Romagna (ParER).

Al termine della fase di progettazione nel luglio 2009 il Polo archivistico è stato costituito come struttura operativa presso l'Istituto dei Beni artistici, culturali e naturali della Regione Emilia-Romagna (IBACN)⁶. La legge regionale n. 17 del 29/10/2008 ha attribuito, infatti, all'Istituto la funzione di archiviazione e conservazione dei documenti informatici prodotti dalla Regione e,

⁴ Il citato comma 1bis dell'art. 1 della L. R. 29/1995 ora recita: *L'istituto, per lo svolgimento delle attività di cui all'articolo 2, nel rispetto dei principi di sussidiarietà e partecipazione, può promuovere accordi e intese, favorire progetti strutturati in rete nei territori, prestare consulenza e collaborare, anche mediante convenzioni, con le istituzioni nazionali ed europee, le altre Regioni, gli enti pubblici e privati, gli enti locali e le loro forme associative, le imprese, gli enti di ricerca e formativi, e anche con il coinvolgimento attivo dei cittadini. Può altresì istituire comitati scientifici che siano di ausilio all'esercizio delle funzioni di cui all'articolo 2.* L'articolo 2, relativo alle attribuzioni, come ricordato prevede espressamente alla lettera f bis) le funzioni di archiviazione e conservazione digitale dei documenti informatici.

⁵ Una scheda sul progetto si trova nella Appendice B di S. Pigliapoco, *La memoria digitale delle amministrazioni pubbliche*, cit., p. 225 - 236

⁶ Delibera di Giunta regionale Emilia-Romagna del 22 giugno 2009, n. 877, che «autorizza l'IBACN a istituire, per la gestione delle funzioni assegnate dalla L.R. 17/2008 in materia di conservazione digitale [...], una struttura dirigenziale a livello di Servizio denominata "Polo archivistico regionale"».

mediante apposita convenzione, dei documenti prodotti da Province, Comuni e altri soggetti pubblici⁷.

La scelta di affidare la realizzazione di ParER a IBACN è stata assunta in ragione delle caratteristiche di autonomia organizzativa, gestionale e tecnico-scientifica di cui l'Istituto gode⁸, delle specifiche funzioni che esso ricopre nell'ambito della valorizzazione dei beni culturali e dell'esperienza maturata nel coordinamento degli enti sul territorio. Deriva inoltre dalla scelta fondamentale assunta su precisa posizione della Soprintendenza archivistica per l'Emilia-Romagna della necessità che il Polo dovesse essere una struttura pubblica, tecnico-specialistica, indipendente e autonoma a livello direttivo e decisionale.

ParER ha tutte le caratteristiche istituzionali, giuridiche e tecniche indispensabili al corretto svolgimento del proprio ruolo di *archivio* cioè, per utilizzare i termini di **OAIS**, una struttura organizzata di persone e sistemi che accetta la responsabilità di conservare documenti informatici e renderli disponibili ad una **Comunità di riferimento**.

Infatti, IBACN è un soggetto pubblico, con personalità giuridica e quindi ente terzo rispetto a tutti i *Produttori*⁹, e ha dotato il Servizio Polo Archivistico di una specifica struttura tecnologica ed un organico con professionalità qualificate che assommano conoscenze di natura archivistica, informatica, organizzativa e giuridica¹⁰.

In particolare, in ParER si ritiene fondamentale promuovere l'incontro tra le professionalità archivistiche e informatiche, in quanto la collaborazione tra archivisti e informatici rappresenta e si rivela sempre più una risorsa strategica e una condizione se non sufficiente sicuramente necessaria per affrontare le sfide poste dalla conservazione digitale.

Le logiche organizzative di ParER e i suoi rapporti con i *Produttori* fanno riferimento come modello concettuale alle risultanze del progetto internazionale sulla conservazione InterPARES e al modello Open Archival Information System (**OAIS**), certificato standard ISO 14721 nel 2003 e recentemente aggiornato (ISO 14721:2012).

⁷ Legge regionale 29 ottobre 2008, n. 17 («Misure straordinarie in materia di organizzazione»), art. 8.

⁸ Come da Statuto (approvato con Delibera di Giunta regionale del 10 giugno 1997, n. 942), IBACN ha personalità giuridica, autonomia statutaria e finanziaria e opera con autonomia scientifica, organizzativa, amministrativa e contabile. È quindi un soggetto pubblico, ente terzo rispetto agli Enti produttori che conferiscono i propri documenti al Polo.

⁹ Si può quindi definire una terza parte neutrale cioè, secondo la definizione data all'interno del progetto di ricerca internazionale InterPARES: una persona giuridica che non ha interesse nel contenuto dei documenti e non ha ragione di alterare i documenti sotto la sua custodia, che inoltre cercherà di non permettere a nessuno di alterare i documenti sia accidentalmente che di proposito.

¹⁰ Tra le competenze del Servizio, così come ridefinite dalla delibera di Giunta regionale del 5 dicembre 2011, n. 1803, figurano: «la responsabilità dello svolgimento dei processi di conservazione sostitutiva e di riversamento sostitutivo dei Documenti informatici della Regione e degli altri enti convenzionati; la cura delle modalità di trasferimento, accesso e fruizione del patrimonio documentario e informativo conservato in ParER; la promozione dell'adesione degli enti del sistema regionale a ParER; il supporto all'azione dei responsabili del protocollo informatico presso gli Enti produttori per la messa a punto degli strumenti archivistici, organizzativi e software per le esigenze di produzione e conservazione dei documenti digitali, nonché per l'adeguamento al *Sistema di conservazione* digitale di ParER; l'evoluzione tecnologica (hardware, software, formati elettronici, ecc.) e l'aggiornamento o **migrazione** dei sistemi di ParER; la gestione ed erogazione di servizi per il trattamento dei Documenti informatici (e dei documenti multimediali) per la Regione e gli enti convenzionati; il coordinamento dell'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione delle pubbliche amministrazioni previste dal Codice dell'amministrazione digitale presso l'Istituto, in raccordo con la Direzione generale competente della Giunta regionale».

Il *Sistema di conservazione* opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale.

Seguendo quanto indicato dalle **Regole tecniche** vigenti e sulla base dello stesso modello **OAIS** si possono identificare i seguenti ruoli fondamentali: *Produttore* (o Ente produttore), *Utente*, *Responsabile*.

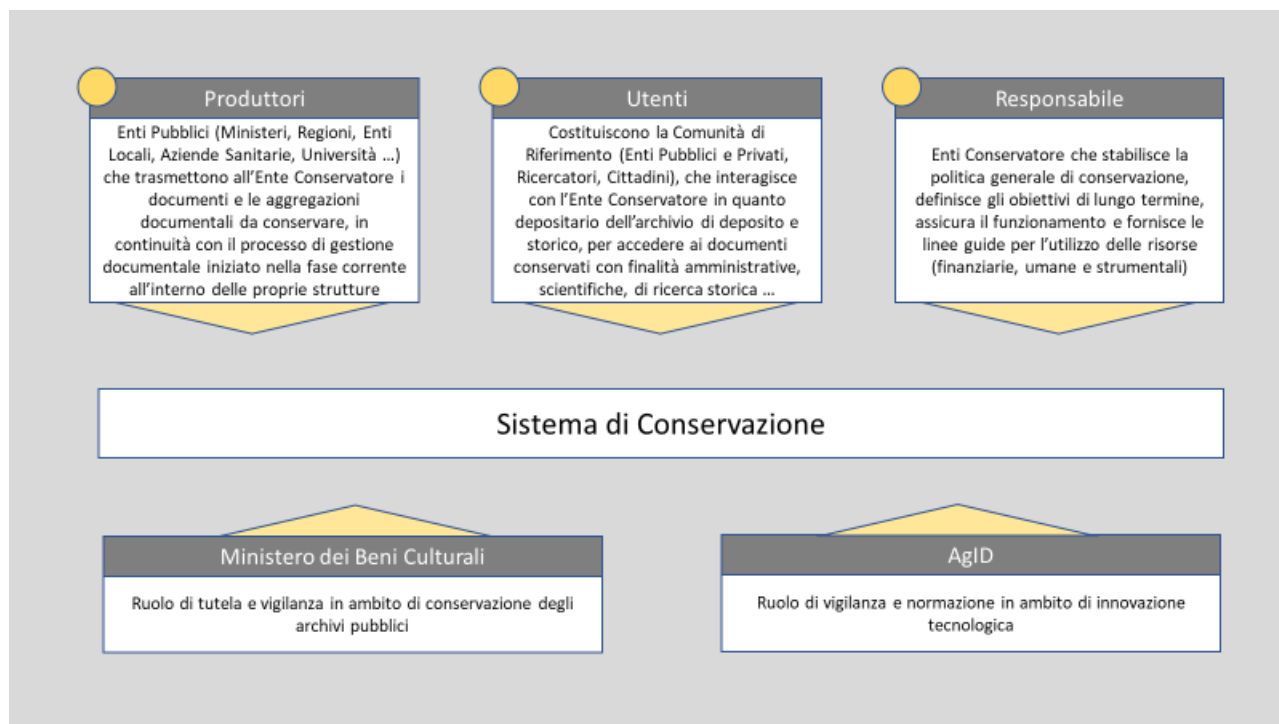


Figura 1 - Sistema e attori

[\[Torna al Sommario\]](#)

4.2 Produttore

È il soggetto che affida la conservazione dei propri documenti informatici a IBACN, denominato nella **Convenzione** Ente Produttore.

Nel ruolo del *Produttore* possono essere definiti tutti gli enti pubblici convenzionati, che versano i *Documenti informatici* e le *Aggregazioni documentali informatiche* da conservare con gli opportuni *metadati*, in continuità con il processo di gestione documentale iniziato nella fase corrente all'interno delle strutture di produzione.

I rapporti tra IBACN, tramite ParER, e i *Produttori* vengono formalizzati e regolati per mezzo di due documenti fondamentali: la **Convenzione** e il **Disciplinare tecnico**¹¹.

¹¹ Per il dettaglio delle operazioni preliminari all'avvio in produzione di un ente, sia dal punto di vista amministrativo sia tecnico-operativo si vedano le pagine del sito di ParER specificamente dedicate alla attività di conservazione per gli enti; lo schema di Convenzione è approvato con apposita delibera del Consiglio Direttivo dell'IBACN e periodicamente aggiornato; i Disciplinari Tecnici specifici sono presenti nel sistema di conservazione per ogni produttore.

La **Convenzione**, o accordo, regola i rapporti di servizio tra il *Produttore* e ParER, e più precisamente la natura dei servizi offerti, la responsabilità delle parti e le condizioni economiche. Precisa, inoltre, quali sono i servizi offerti da ParER e definisce gli strumenti di consultazione e controllo. Le attuali **Convenzioni** prevedono l'erogazione dei servizi di conservazione dei documenti informatici a titolo gratuito per gli enti dell'Emilia-Romagna (enti locali, Aziende sanitarie, Università) e a titolo oneroso per gli enti di altre regioni.

Il *Produttore*, secondo quanto previsto nella **Convenzione**, si impegna a depositare i *Documenti informatici* e le loro *Aggregazioni documentali informatiche* nei modi e nelle forme definite da IBACN, tramite ParER, garantendone l'autenticità e l'integrità nelle fasi di produzione e di archiviazione corrente, effettuata nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente. Si impegna inoltre a depositare e mantenere aggiornati, nei modi e nelle forme definite tramite ParER da IBACN, gli strumenti di ricerca e gestione archivistica elaborati a supporto della formazione dei documenti e della tenuta degli *archivi*.

Il *Produttore* mantiene la titolarità e la proprietà dei documenti depositati.

Le **tipologie documentarie** da trasferire, le modalità di versamento e i *metadati* sono concordati e specificati nel **Disciplinare tecnico**.

Il responsabile di riferimento del *Produttore* è di norma il *Responsabile della gestione documentale*, il *Responsabile della conservazione* o il responsabile di specifici sistemi di produzione documentale, quali quelli di produzione di documentazione sanitaria. Se nominato, può essere anche il *Coordinatore della gestione documentale*.

Come indicato dall'art.11 del DPCM 13 novembre 2014 il *Responsabile della gestione documentale* o, se nominato, il *Coordinatore della gestione documentale*, provvede a generare i pacchetti di versamento e stabilisce, per le diverse **tipologie documentarie**, i tempi di versamento o trasferimento in conservazione, in conformità con le norme vigenti in materia, il sistema di classificazione e il piano di conservazione. Infine, verifica il buon esito della operazione di versamento in particolare tramite la verifica della produzione del *rapporto di versamento* da parte del sistema di conservazione.

Il *Produttore* resta il responsabile del contenuto del *Pacchetto di versamento* (d'ora in poi SIP) ed è obbligato a trasmetterlo al servizio di conservazione secondo le modalità operative descritte genericamente nel presente Manuale e in dettaglio nel **Disciplinare tecnico** e nella documentazione tecnica di riferimento.

Nel sistema di conservazione il soggetto che materialmente versa i SIP nel sistema di conservazione è identificato con il termine "Versatore". Normalmente coincide con il Produttore, ma in alcuni casi, generalmente per motivi tecnico-organizzativi, quest'ultimo può incaricare un altro Produttore di versare in conservazione i suoi documenti.

Se il Versatore non è un Produttore (e in questo caso prende il nome di Versatore esterno), non può versare i SIP direttamente nel sistema - in quanto non può essere titolare di una Struttura versante - ma può versare oggetti per conto del Produttore nel sistema di preacquisizione (vedi paragrafo 7.1.1).

Il Produttore, nella sua attività di produzione e versamento in conservazione dei SIP, può essere coadiuvato da utenti esterni appartenenti ad altre organizzazioni, definite "Fornitori esterni", che sono normalmente le software house che gestiscono i sistemi di produzione e/o versamento dei documenti.

Il personale dei Fornitori esterni può operare sul Sistema per finalità di supporto tecnico e organizzativo alle attività di conservazione su esplicita autorizzazione del Produttore

Come indicato nel paragrafo 4.3, il *Produttore* ha l'accesso presso la propria sede al *Sistema di conservazione* per la parte relativa alla sua documentazione conservata.

[\[Torna al Sommario\]](#)

4.3 Utente

In base alla definizione del glossario allegato alle vigenti **Regole tecniche** si indentifica come *Utente* una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione dei *Documenti informatici* al fine di fruire delle informazioni di interesse.

L'*Utente* richiede al *Sistema di conservazione* l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il *Sistema di conservazione* permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai *Documenti informatici* conservati e consente la produzione di un *Pacchetto di distribuzione* direttamente acquisibile dai soggetti autorizzati.

In termini **OAIS** la comunità degli *Utenti* può essere definita come **Comunità di riferimento**

Nel ruolo dell'*Utente* si possono definire al momento solo specifici soggetti abilitati dei *Produttori*, in particolare gli operatori indicati dal *Produttore* che possono accedere esclusivamente ai documenti versati dal *Produttore* stesso o solo ad alcuni di essi secondo le regole di visibilità e di accesso concordate tra ParER e il *Produttore*

L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione utenze indicate nel *Piano della sicurezza del sistema di conservazione* e nel rispetto delle misure di sicurezza previste negli articoli da 31 a 36 del D.lgs. 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1 e dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B del medesimo decreto.

In prospettiva si possono definire *Utenti* potenzialmente tutti coloro che potranno interagire con ParER, quale conservatore e custode di archivi di deposito e storici, per accedere ai documenti conservati per finalità amministrative, scientifiche e di ricerca storica in relazione alle **tipologie documentarie** conservate e nel rispetto delle normative vigenti in materia di tutela dei beni culturali e di tutela dei dati personali.

[\[Torna al Sommario\]](#)

4.4 Ente conservatore

In base alla normativa vigente il *Responsabile della conservazione* per le pubbliche amministrazioni è identificato con un dirigente o un funzionario formalmente designato e può identificarsi con il *Responsabile della gestione documentale* o, se nominato, con il *Coordinatore della gestione documentale*.

Il modello organizzativo precedentemente descritto, ai sensi dell'articolo 5, comma 2, lettera b) delle vigenti **Regole tecniche**, prevede che il soggetto produttore affidi la conservazione e il processo di conservazione ad un soggetto conservatore esterno specificamente individuato nell'IBACN.

La responsabilità del *Sistema di conservazione* e del servizio di conservazione come soggetto che svolge attività di *conservazione* è in capo a IBACN, nato nel 1974 come organo tecnico-scientifico e strumento della programmazione regionale nel settore dei beni artistici, culturali e naturali. L'Istituto ha personalità giuridica, autonomia statutaria e finanziaria ed opera con autonomia scientifica, organizzativa, amministrativa e contabile.

L'Istituto promuove e svolge attività conoscitiva ed operativa, di indagine e di ricerca, per la valorizzazione ed il restauro del patrimonio storico ed artistico, nonché per lo svolgimento di ogni funzione relativa ai beni artistici, culturali e naturali, prestando in tali campi la propria consulenza alla Regione ed agli Enti locali. Tra le altre, svolge le funzioni di archiviazione e *conservazione* digitale dei *Documenti informatici* anche a rilevanza fiscale, con le modalità previste dalle disposizioni vigenti, prodotti o ricevuti dalla Regione e dagli altri soggetti obbligati, nonché dei *Documenti informatici* prodotti o ricevuti dai soggetti convenzionati.

Il ruolo di IBACN come responsabile del servizio di conservazione e del *Sistema di conservazione* va inquadrato alla luce dell'art. 2 della L.R. 11/2004, ossia nel contesto di un più generale impegno, da parte della Regione Emilia-Romagna – nel rispetto delle competenze dello Stato e di concerto con il sistema degli Enti locali – per assicurare a cittadini, imprese ed enti condizioni di sviluppo delle loro attività e relazioni, promuovendo le potenzialità delle tecnologie informatiche nella prestazione di servizi e nell'accessibilità e scambio di dati. In particolare, la Regione persegue lo sviluppo delle reti strumentali, organizzative ed operative e lo sviluppo integrato dei servizi attivi sulla rete della pubblica amministrazione attraverso la collaborazione con le amministrazioni periferiche dello Stato, il sistema delle autonomie locali e, più in generale, tutti i soggetti pubblici e privati e le organizzazioni sociali operanti sul territorio.

Nello specifico, la Regione, anche in collaborazione con le altre pubbliche amministrazioni interessate, favorisce lo sviluppo integrato della *conservazione* dei *Documenti informatici* e, nel rispetto dei principi di efficacia, efficienza ed economicità, svolge le funzioni di archiviazione e *conservazione* digitale dei *Documenti informatici* secondo quanto disposto dall'articolo 2, comma 1, lettera f bis) della legge regionale 10 aprile 1995, n. 29.

In quanto soggetto responsabile IBACN si occupa delle politiche complessive del *Sistema di conservazione* e ne determina l'ambito di sviluppo e le competenze. A tal fine, in coerenza con **OAIS**, provvede alla pianificazione strategica, alla ricerca dei finanziamenti, alla revisione periodica dei risultati conseguiti e ad ogni altra attività gestionale mirata a coordinare lo sviluppo del sistema. Non risulta invece coinvolto nelle operazioni quotidiane di amministrazione del

sistema che sono a carico del soggetto incaricato della sua gestione, cioè il Servizio Polo Archivistico Regionale, comunemente noto come ParER, il cui dirigente è specificamente individuato come Responsabile del servizio di conservazione.

La missione di ParER è essere l'*archivio informatico* della Pubblica Amministrazione in Emilia-Romagna per la conservazione e l'accesso dei *Documenti informatici* e in generale di ogni oggetto digitale a supporto dei processi di innovazione e semplificazione amministrativa, con gli obiettivi di:

- garantire la conservazione, archiviazione e gestione dei Documenti informatici e degli altri oggetti digitali;
- erogare servizi di accesso basati sui contenuti digitali conservati
- fornire supporto, formazione e consulenza ai Produttori per i processi di dematerializzazione.¹²

Di fatto, quindi (come definito dal testo della **Convenzione**, art. 3, comma 1), IBACN, tramite ParER, si impegna alla *conservazione* dei documenti trasferiti e ne assume la funzione di Responsabile del servizio di conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione, e svolge, tramite la struttura organizzativa e di responsabilità di ParER, l'insieme delle attività elencate nell'articolo 7 comma 1 delle **Regole tecniche**, in particolare quelle indicate alle lettere a), b), c), d), e), f), g), h), i), j), k) e m).

I ruoli specificamente individuati sono riportati nella seguente tabella:

RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO	DELEGHE
Responsabile del servizio di conservazione	Marco Calzolari	vedi cap. 5	da luglio 2009	-
Responsabile Sicurezza dei sistemi per la conservazione	Marco Calzolari	vedi cap. 5	da luglio 2009	-
Responsabile funzione archivistica di conservazione	Gabriele Bezzi	vedi cap. 5	da novembre 2009	-
Responsabile trattamento dati personali (attuatore)	Marco Calzolari	vedi cap. 10	da dicembre 2019	
Responsabile protezione dati personali (DPO)	Sergio Duretti	Vedi cap. 10	da gennaio 2020	

¹² Da Relazione sulle attività realizzate per gli anni 2009 – 2012 approvata dalla Delibera di Giunta regionale Emilia-Romagna del 01 ottobre 2012, n. 1428.

RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO	DELEGHE
Responsabile sistemi informativi per la conservazione	Maurizio Coppari	vedi cap. 5	da dicembre 2019	-
Responsabile sviluppo e manutenzione del sistema di conservazione	Cristiano Casagni	vedi cap.5	da luglio 2009	-

Per la descrizione nel dettaglio della struttura organizzativa e di responsabilità si veda il capitolo 5 e per i dati dei soggetti che nel tempo hanno assunto la responsabilità del *Sistema di conservazione* l'Allegato 2 "Registro dei responsabili".

Nell'Allegato, che verrà mantenuto opportunamente aggiornato, sono riportati i dati delle persone fisiche che, in base ai loro ruoli in IBACN, nel tempo hanno esercitato la rappresentanza del conservatore tramite specifiche azioni e/o eventuali sottoscrizioni. In particolare il Direttore di IBACN, quale delegato alla firma delle **Convenzioni** e alla rappresentanza generale di IBACN (oltre che di *Responsabile del trattamento dei dati personali*); il Dirigente Responsabile del Servizio Polo archivistico regionale dell'Emilia-Romagna (ParER), quale Responsabile del servizio di conservazione e delegato alla firma delle **Convenzioni**; il titolare della Posizione organizzativa di presidio della funzione archivistica di conservazione, a cui sono assegnate in particolare le funzioni di sottoscrizione previste nell'ambito del *processo di conservazione* e le funzioni di rappresentanza nei rapporti con il MiBACT e gli altri enti di vigilanza per quanto di competenza.

In taluni casi la **Convenzione** può prevedere che, per semplificare le attività di avviamento e di gestione ordinaria del servizio di conservazione, il rapporto tra il Produttore e il Conservatore sia mediato da un ente, chiamato nel sistema di conservazione "Ente gestore", che, pur non assumendo la responsabilità diretta del processo di conservazione, che resta in capo al conservatore, agisce come facilitatore del processo medesimo, svolgendo attività di gestione (quali configurazioni di sistema, definizione di modalità comuni di versamento, monitoraggio) e coordinamento (gestione delle utenze, formazione, supporto di primo livello) rispetto ad un gruppo definito di Produttori.

Il ruolo di Gestore è concordato tramite apposito accordo da una parte con il Conservatore, dall'altra parte con i Produttori: il Gestore stipula con il conservatore un accordo generale, cui gli enti Produttori possono aderire, semplificando notevolmente i processi amministrativi di adesione al servizio, anche se è comunque necessaria la stipula di un accordo formale anche tra Produttore e Conservatore, riferito all'accordo generale con il Gestore. Il ruolo di gestore viene normalmente svolto da enti territoriali, che svolgono servizi per gli enti del proprio territorio.

[\[Torna al Sommario\]](#)

4.5 Organismi di tutela e vigilanza

Il Ministero per i beni e le attività culturali (MiBACT) esercita funzioni di tutela e vigilanza dei sistemi di conservazione degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente importante e autorizza le operazioni di *scarto* e trasferimento della documentazione conservata ai sensi del D.Lgs 42/2004¹³.

La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiBACT, tramite le Soprintendenze archivistiche competenti per territorio.

"Lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art. 21, c. 1, lettera b).

Anche "Il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art. 21, c. 1, lettera e).

La disposizione si applica anche:

- all'affidamento a terzi dell'archivio (outsourcing), ai sensi del D.lgs 22 gen. 2004, n. 42, art. 21, c. 1, lettera e)
- al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico.¹⁴

La Soprintendenza archivistica può, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli archivi e può emettere prescrizioni per la tutela degli archivi.

Secondo quanto disposto dall'art. 36, comma 2 lettera a) del recente regolamento di organizzazione del MiBACT (DPCM 29 agosto 2014, n. 171), il Soprintendente archivistico "svolge, sulla base delle indicazioni e dei programmi definiti dalla competente Direzione generale, attività di tutela dei beni archivistici presenti nell'ambito del territorio di competenza nei confronti di tutti i soggetti pubblici e privati, ivi inclusi i soggetti di cui all'articolo 44-bis del Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni", cioè i conservatori accreditati.

Il Dm 27 novembre 2014 ha ridisegnato la distribuzione degli istituti periferici accorpando, in cinque casi, le Soprintendenze di due regioni sotto un'unica direzione: Abruzzo e Molise, Calabria e Campania, Puglia e Basilicata, Umbria e Marche, Veneto e Trentino Alto-Adige, che si sommano alla già esistente Piemonte e Valle d'Aosta.

In particolare, la Soprintendenza archivistica per l'Emilia-Romagna (ora Soprintendenza Archivistica e Bibliografica dell'Emilia-Romagna) svolge un ruolo di vigilanza del *Sistema di conservazione* di IBACN per verificare che il *processo di conservazione* avvenga in modo conforme alla normativa e ai principi di corretta e ininterrotta custodia, senza però accedere a informazioni personali/sensibili contenute nei documenti o nel sistema.

L'IBACN l'11 maggio 2010 ha stipulato un accordo di collaborazione con la Soprintendenza archivistica dell'Emilia-Romagna, rinnovato fino al 2016 che prevede tra i punti più qualificanti:

- la semplificazione delle procedure di autorizzazione al trasferimento mediante l'approvazione preventiva dello schema di **Convenzione**;
- l'agevolazione dell'attività ispettiva;

¹³ Si fa riferimento in particolare agli art. 4, 10, 18 e 21 del citato Decreto legislativo. Il mantenimento delle competenze del MiBAC in materia di tutela dei sistemi di conservazione degli archivi pubblici è ribadito dall'art. 6 comma 9 e dall'art. 9 comma 2 delle Regole Tecniche

¹⁴ Dal sito della Soprintendenza archivistica per l'Emilia-Romagna, <http://www.sacro.archivi.beniculturali.it/index.php?id=21>

- il supporto e consulenza ai *Produttori*.

Alla scadenza dell'accordo citato, in data 10 aprile 2017 è stato stipulato un nuovo accordo con la Soprintendenza archivistica e bibliografica dell'Emilia-Romagna che ha scadenza il 31 dicembre 2033 e che ha riconfermato i punti sopra indicati.

In base a tale accordi e secondo quanto indicato nella **Convenzione**, ParER consente alla Soprintendenza archivistica e bibliografica dell'Emilia-Romagna l'accesso ai propri sistemi per rendere possibile e operativo lo svolgimento della funzione di vigilanza e tutela prevista dalla legge ed effettuare le opportune verifiche sul corretto svolgimento dell'attività di *conservazione*, in particolare lo svolgimento dell'attività ispettiva, finalizzata ad accertare lo stato di conservazione e di custodia degli archivi, ai sensi e nel rispetto di quanto previsto dall'articolo 19 del D.lgs. n. 42/2004, con *"modalità concordate che consentano lo svolgimento e la documentazione di tale attività in modalità interamente digitali all'interno del sistema di conservazione sviluppato da IBACN"*.

La profilazione dell'utente Soprintendente non consente l'accesso ai contenuti dei documenti conservati e ai dati personali/sensibili presenti nei documenti e nei metadati.

IBACN ha attualmente sottoscritto accordi anche con la Soprintendenza archivistica del Veneto e Trentino Alto-Adige e con quella del Piemonte e Valle d'Aosta.

Bisogna ricordare che, ai sensi del DPR del 1 novembre 1973 n. 690, le attribuzioni degli organi centrali e periferici dello Stato in materia di ordinamento, tutela, vigilanza, conservazione, custodia e manutenzione del patrimonio storico artistico e popolare sono esercitate, per il rispettivo territorio, dalle province autonome di Trento e di Bolzano. Per la provincia di Trento tali attribuzioni riguardano anche gli archivi e i documenti della provincia, dei suoi enti funzionali, dei comuni e degli altri enti locali, degli altri enti pubblici per le materie di competenza della provincia, nonché gli archivi e i documenti dei privati.

In base alle **Regole tecniche** i sistemi di conservazione delle pubbliche amministrazioni e i sistemi di conservazione dei conservatori accreditati sono soggetti anche alla vigilanza dell'AgID. Per tale fine il *Sistema di conservazione* di IBACN prevede la materiale conservazione dei dati e delle Copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede del *Produttore*.

AgID vigila inoltre sulla corretta applicazione delle regole del **Cloud marketplace**, che ParER ha adottato per fornire il servizio di conservazione ai Produttori nella forma di **SaaS** (Software as a service).

[\[Torna al Sommario\]](#)

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma dell'IBACN

L'Organigramma di IBACN è illustrato in figura.

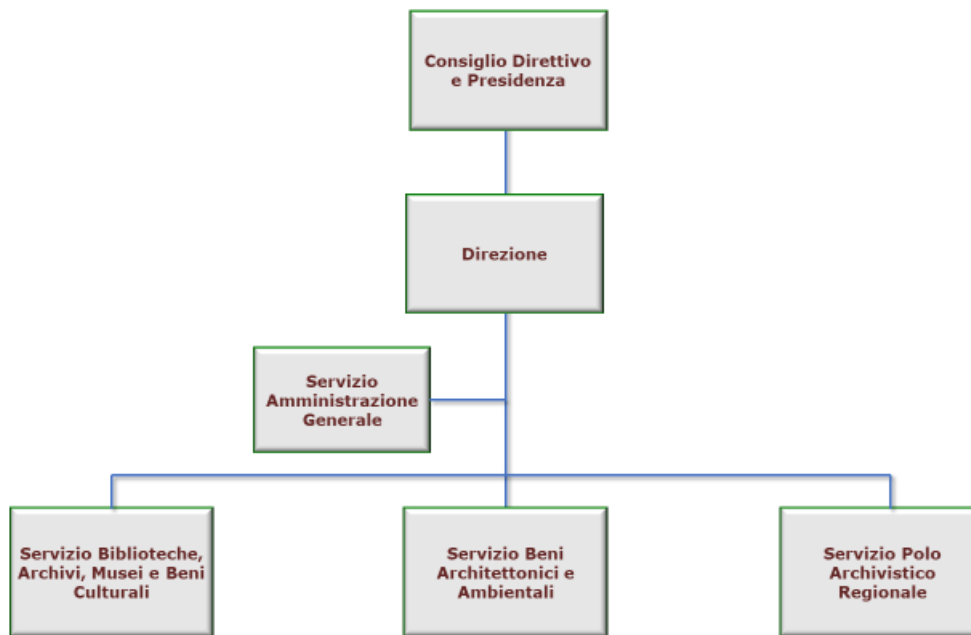


Figura 2 - Organigramma IBACN

In seno a IBACN, la gestione del *Sistema di conservazione* è in carico a uno dei Servizi in cui si articola l'Istituto: con Del. Giunta 877/2009, infatti, la Regione Emilia-Romagna ha attivato il Servizio Polo archivistico regionale dell'Emilia-Romagna (ParER) come struttura dirigenziale a livello di Servizio di IBACN.

A ParER sono state attribuite, da ultimo con la Delibera di Giunta 1803/2011, diverse competenze, tra le quali in primis la responsabilità dello svolgimento del *processo di conservazione* dei *Documenti informatici* della Regione e degli altri enti convenzionati, e la cura delle modalità di trasferimento, *accesso* e fruizione del patrimonio documentario e informativo conservato.

ParER cura inoltre l'evoluzione tecnologica e l'aggiornamento o la **migrazione** del *Sistema di conservazione*.

In una prospettiva di promozione della dematerializzazione e della conservazione digitale, ParER coordina l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione delle pubbliche amministrazioni previste dal Codice dell'amministrazione digitale presso l'Istituto, in raccordo con la Direzione generale competente della Giunta regionale; supporta l'azione dei responsabili della gestione documentale presso i *Produttori*, in particolare in vista

dell'adeguamento dei sistemi al *Sistema di conservazione*; promuove l'adesione degli enti del sistema regionale; si raccorda con analoghe iniziative a livello nazionale ed europeo.

5.2 Struttura organizzativa del Servizio Polo Archivistico (ParER)

All'interno di ParER, si situano le responsabilità relative al Servizio di Conservazione di seguito dettagliate.

Responsabile del Servizio: dirigente con responsabilità dei procedimenti / processi / progetti di ParER. E' il dirigente responsabile del Servizio Polo archivistico regionale (ParER). È responsabile dei progetti e delle attività di ParER, della definizione e attuazione delle politiche complessive del Sistema di conservazione, nonché del governo della gestione del Sistema di conservazione e della gestione amministrativa del personale assegnato, con responsabilità sulle differenti posizioni organizzative afferenti al servizio e sulla relativa definizione del personale e delle risorse di cui avvalersi per l'attuazione delle attività, sulla pianificazione annuale delle attività assegnate e dell'organizzazione del lavoro all'interno del servizio. Ha l'obbligo di definire i fabbisogni professionali ordinari e straordinari, le proposte di piani di sviluppo del personale e le conseguenti azioni e valutazioni dei risultati. È responsabile della definizione dei requisiti e delle specifiche del Sistema di conservazione, sulla base della normativa vigente, e dell'erogazione del servizio ai *Produttori*, oltre che della gestione delle Convenzioni.

Responsabile della sicurezza dei sistemi per la conservazione: è il soggetto al quale compete la definizione delle soluzioni tecniche e organizzative in attuazione delle disposizioni in materia di sicurezza, nonché la verifica del rispetto e il monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. È tenuto a segnalare eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

Responsabile della funzione archivistica di conservazione: è il funzionario titolare della Posizione Organizzativa responsabile del presidio della funzione archivistica di conservazione ed opera a stretto contatto con il Responsabile del Servizio. Nella struttura organizzativa del paragrafo successivo va identificato con il Responsabile dell'Area funzione archivistica di conservazione. Rientrano tra le sue mansioni e responsabilità, come da specifica designazione:

- la definizione e gestione del processo di conservazione, incluse le modalità di trasferimento, descrizione archivistica, esibizione, accesso e fruizione del patrimonio documentario e informativo conservato;
- la verifica sistematica dell'aderenza del processo e del sistema di conservazione alla normativa e standard di riferimento e ai loro aggiornamenti;
- la definizione dei requisiti degli accordi e/o Convenzioni dal punto di vista archivistico, con la definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici, anche mediante l'analisi e l'identificazione dell'articolazione strutturale dei Produttori e delle modalità di registrazione e classificazione della documentazione da essi adottate;
- il monitoraggio del processo di conservazione con la verifica delle modalità di versamento e l'eventuale presenza di errori, la verifica di integrità e la descrizione archivistica dei documenti e delle Aggregazioni documentali informatiche trasferite;
- l'analisi archivistica per lo sviluppo di nuove funzionalità del Sistema di conservazione;

- la collaborazione con l'azione del responsabile della gestione documentale del Produttore ai fini del trasferimento in conservazione e della selezione;
- la gestione dei rapporti con gli enti convenzionati e con la Soprintendenza archivistica per l'Emilia-Romagna (ora Soprintendenza archivistica e bibliografica dell'Emilia-Romagna) e altre articolazioni del MiBACT per quanto di competenza;
- la sottoscrizione con firma digitale dei Pacchetti di archiviazione secondo le modalità descritte nel presente Manuale
- l'eventuale sottoscrizione di Pacchetti di distribuzione e di attestazioni di conformità di copie cartacee di Documenti informatici conservati.

Responsabile dei sistemi informativi per la conservazione: individuato nella struttura organizzativa del paragrafo successivo con il Responsabile dell'Area gestione servizi e infrastrutture di ParER. Rientrano tra le sue mansioni:

- la gestione dell'esercizio delle componenti hardware e software del Sistema di conservazione;
- la responsabilità della corretta erogazione dei servizi di conservazione, della verifica e del mantenimento dei relativi livelli di servizi;
- il monitoraggio, d'intesa con il Responsabile della Sicurezza del servizio di conservazione, della sicurezza fisica e logica dell'impianto tecnologico di ParER;
- il coordinamento tecnico dei rapporti con i fornitori di data center e supporto tecnologico ai progetti di conservazione digitale;
- la pianificazione, di concerto con i fornitori, dello sviluppo dell'architettura tecnologica a disposizione per le attività di conservazione e quelle di servizio;
- il controllo e verifica dei livelli di servizio erogati dai fornitori (SLA), la segnalazione delle eventuali difformità e la pianificazione delle necessarie contromisure;
- il coordinamento nell'assegnazione, nell'installazione e nella manutenzione delle attrezzature informatiche individuali, nonché nell'assistenza agli operatori, con il supporto dei collaboratori assegnati a tale attività;
- la collaborazione nelle attività inerenti alla protezione dei dati personali; la predisposizione delle procedure di acquisto di beni e servizi in area informatica;
- il supporto di rete telematica alle attività di ParER.

Responsabile dello sviluppo e della manutenzione del sistema di conservazione: individuato nella struttura organizzativa del paragrafo successivo con la Posizione Organizzativa di Capo Progetto dell'Area tecnologia e sviluppo sistemi di conservazione. E' responsabile del coordinamento e della gestione dei rapporti con i fornitori per le attività di pianificazione strategica e operativa finalizzate alla progettazione e allo sviluppo del *Sistema di conservazione* di ParER e per le attività di monitoraggio e di verifica delle operazioni di implementazione del *Sistema di conservazione* e di personalizzazione e implementazione di nuove funzionalità dei sistemi informatici. Tra i suoi compiti rientrano:

- il monitoraggio dello sviluppo dei progetti informatici e la cura della rispondenza allo standard dei parametri e dei requisiti definiti;
- il coordinamento delle attività di verifica e di implementazione dei progetti;
- l'analisi e la progettazione delle nuove procedure informatiche in base alle necessità dell'utenza, agli standard e alla rispondenza ai criteri di qualità e sicurezza individuati per l'insieme del sistema informativo regionale;

- l'interfaccia con i Produttori, in riferimento agli applicativi di gestione, ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;
- l'individuazione di soluzioni di personalizzazione e manutenzione delle soluzioni applicative in relazione alle diverse tipologie di Produttori e degli oggetti conservati o da conservare e alle esigenze di evoluzione tecnologica;
- la definizione delle caratteristiche e dei requisiti del Sistema di conservazione (componenti architetture, applicative, delle risorse e dei servizi);
- la progettazione e organizzazione del sistema (informativo, informatico, telematico) con riferimento ai diversi processi di sviluppo, di test e rilascio in produzione e di conduzione a regime;
- la gestione dell'intero ciclo di sviluppo di siti web e portali connessi al servizio di conservazione;
- il supporto alla verifica dell'aderenza del processo e del sistema di conservazione alla normativa e standard di riferimento e ai loro aggiornamenti.

Le figure sopracitate svolgono inoltre le azioni indicate nel Piano della Sicurezza in merito alla definizione ed alla attuazione degli indirizzi e delle attività necessarie per assicurare la sicurezza delle informazioni conservate.

Il **Responsabile del trattamento dei dati personali** è identificato nel capitolo 10 del presente Manuale.

ParER è organizzato secondo la struttura riportata in figura.

Le aree indicate svolgono le attività di seguito descritte in dettaglio; il Responsabile della Sicurezza coincide attualmente con il Responsabile del servizio e il Responsabile della Qualità coincide con il Responsabile dell'Area funzioni di supporto.

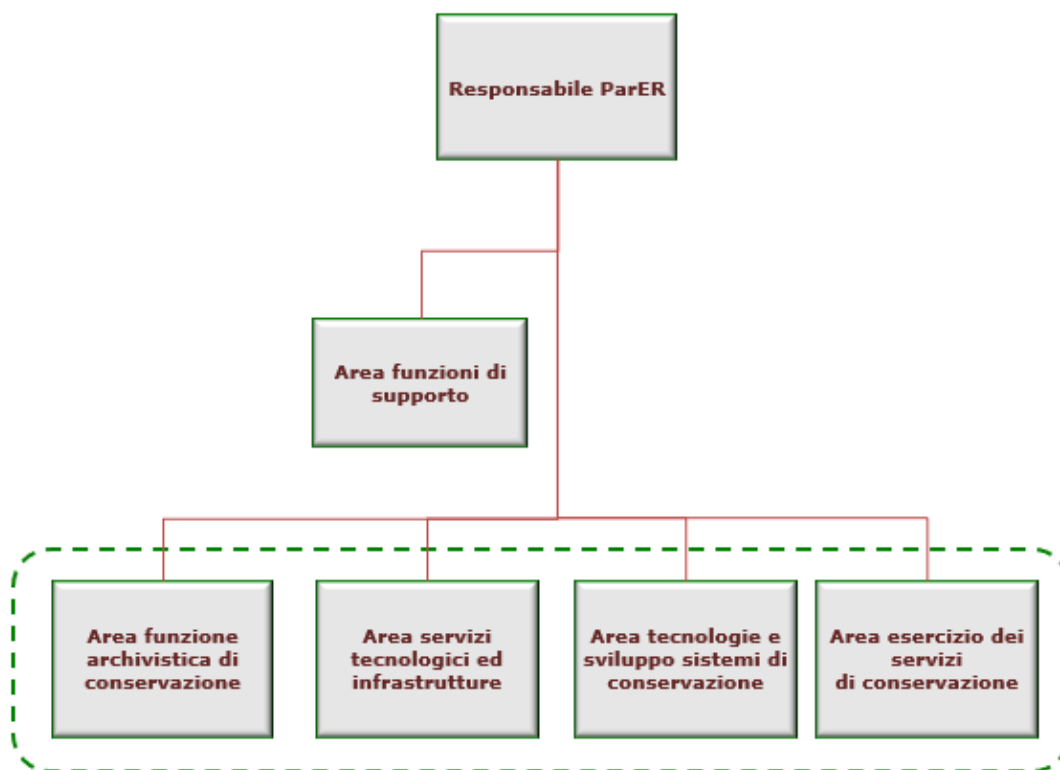


Figura 3 - Struttura organizzativa di ParER

AREA FUNZIONI DI SUPPORTO, per la gestione dei processi amministrativi interni al servizio. In particolare, è in capo a quest'area la responsabilità nella gestione dei rapporti giuridico-amministrativi e nella redazione degli atti di impegno e delle convenzioni con la pubblica amministrazione, degli atti di liquidazione e dei contratti con i fornitori e della gestione delle **Convenzioni** con gli enti per l'avvio del rapporto con ParER, l'analisi e gli adempimenti organizzativi relativi all'applicazione della normativa in materia di protezione dei dati personali; la gestione contabile dei capitoli di spesa di competenza di ParER e il relativo monitoraggio; la gestione della procedura amministrativa inerente le **Convenzioni** per la funzione di conservazione dei *Documenti informatici* da sottoscrivere con i *Produttori* (enti locali e vari enti pubblici), la gestione dei processi di certificazione e di accreditamento, le gestione della Qualità. Il Responsabile di quest'area è rappresentato dal **Responsabile di Gestione Qualità**, che ha il compito di verificare sia la redazione che l'aggiornamento dei documenti del Sistema di Gestione Integrato (**SGI**) rispettino i requisiti ISO 9001. Una volta definita, è responsabile della distribuzione della documentazione approvata, della definizione dei template e standard documentali, della loro revisione nel caso di cambiamenti e modifiche. Relativamente al suo ambito, è responsabile degli Audit al fine di verificare la corretta applicazione delle procedure e dei requisiti prescritti dalla normativa e analizzare le Non conformità di processo e di sistema in modo da evidenziare eventuali scostamenti, di conseguenza concorda con gli altri Responsabili l'applicazione di adeguate Azioni Correttive. Rileva gli indici di Qualità ed effettua il riesame per verificare l'adeguatezza e l'efficacia del sistema integrato, focalizzandosi sull'ambito della qualità.

AREA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE, con funzioni di gestione del protocollo, gestione e verifica della conservazione digitale, gestione dell'archivio di deposito e storico analogico della Regione Emilia-Romagna.

Quest'area ha la responsabilità generale del processo di conservazione, e in particolare garantisce l'aderenza del processo alla normativa e standard di riferimento e ai loro aggiornamenti.

Si occupa di fornire le linee guida su tutti gli aspetti archivistici del servizio e ne verifica l'applicazione; ciò si applica in particolare alle **Convenzioni**, ai **Disciplinari tecnici**, alla definizione dei modelli di *pacchetti informativi*, Alla definizione degli aspetti non operativi delle procedure, alla gestione della documentazione interna al servizio.

Quest'area si occupa inoltre del monitoraggio complessivo del processo di conservazione e ne garantisce la correttezza, provvedendo alla sottoscrizione digitale dei *pacchetti informativi*.

Dal punto di vista delle nuove applicazioni quest'area contribuisce alla definizione dei requisiti funzionali, garantendone la coerenza con le esigenze del processo di conservazione.

Infine, quest'area mantiene le relazioni con gli enti convenzionati e con gli organismi di sorveglianza e di indirizzo (MiBACT, Soprintendenze archivistiche, AgID), nonché con altri soggetti interessati a sviluppare azioni comuni nell'ambito della conservazione.

AREA SERVIZI TECNOLOGICI E INFRASTRUTTURE, con funzione di presidio della gestione dei servizi di conservazione e dell'infrastruttura informatica di ParER. Il Responsabile di tale area svolge le attività quale Responsabile dei sistemi informativi per la conservazione in base alle mansioni indicate in precedenza.

L'infrastruttura tecnologica che ospita il *Sistema di conservazione*, nonché tutti i servizi necessari al suo funzionamento, è in parte ospitata presso i **data center** della regione Emilia-Romagna uno contenente il sito primario e l'altro il sito di **disaster recovery**.

Ambedue i **data center**, descritti in dettaglio nel capitolo 8, sono situati sul territorio nazionale, per cui deve considerarsi applicabile la normativa nazionale.

AREA TECNOLOGIE E SVILUPPO DEI SISTEMI DI CONSERVAZIONE, con le funzioni di presidio dei sistemi informatici e di gestione dei rapporti con i fornitori dei servizi tecnologici agli enti, per l'interfacciamento di ParER.

In quest'area è prevista la figura di un Responsabile dello sviluppo e della manutenzione del *Sistema di conservazione*, con le mansioni e i compiti indicati in precedenza, per i quali è supportato dalle figure dell'Area.

Sono inoltre previste altre figure: analista informatico (o "analista di sistemi informativi"), analista funzionale (o "Analista di business") e tecnico informatico (o "Analista Programmatore"). L'analista informatico è il gestore delle relazioni con i fornitori degli enti che si vogliono interfacciare con ParER e del supporto tecnico per la definizione delle specifiche tecniche, la progettazione e la validazione delle funzionalità ed evoluzioni del software di conservazione, ivi incluse le problematiche di autenticazione e di sicurezza informatica.

L'analista funzionale è responsabile delle attività di analisi dei requisiti e delle funzionalità che il *Sistema di conservazione* deve garantire nel tempo per poter erogare il servizio richiesto, partecipando alle diverse fasi di progettazione delle funzionalità del *Sistema di conservazione* e delle sue evoluzioni, dallo studio di fattibilità alle fasi di analisi e realizzazione, rilascio e collaudo; la rilevazione e l'analisi critica delle esigenze di evoluzione del sistema; il coinvolgimento nella reingegnerizzazione dei processi legati alla conservazione e nella scelta dell'evoluzione dell'architettura e delle funzionalità del sistema.

I tecnici informatici sono i soggetti addetti allo sviluppo e all'evoluzione del *Sistema di conservazione*. Tra le loro mansioni figurano la traduzione delle analisi dei requisiti e delle

funzioni in specifiche tecniche del *Sistema di conservazione*; lo sviluppo delle evoluzioni software del *Sistema di conservazione*; la realizzazione dei test e della messa in esercizio delle nuove versioni dell'applicativo di conservazione; la realizzazione delle attività di verifica, manutenzione e aggiornamento del *Sistema di conservazione* in uso; lo sviluppo e la manutenzione delle componenti di sicurezza dell'applicativo di conservazione.

Il personale addetto allo sviluppo opera anche nella manutenzione del sistema in esercizio, quando se ne presente la necessità, in base a piani di lavoro che tengono conto sia delle esigenze di nuovi sviluppi che delle esigenze di manutenzione del sistema in esercizio.

AREA ESERCIZIO DEI SERVIZI DI CONSERVAZIONE, con funzioni di gestione operativa dei servizi di conservazione.

Prevede al suo interno la figura di un Responsabile, con mansioni di coordinamento delle attività operative a supporto del processo di conservazione. Il Responsabile si occupa di coordinare le attività delle risorse dell'area, in modo tale da garantire adeguati livelli di servizio agli Enti che conservano presso ParER. Oltre a gestire il ciclo di pianificazione, esecuzione e controllo delle attività, si occupa di definire i processi e le procedure operative del servizio, in coerenza con le linee guida emesse dall'Area Funzione Archivistica di Conservazione; nel caso di nuovi sviluppi applicativi fornisce i requisiti di massima del servizio e verifica i documenti prodotti dall'Area Tecnologia e Sviluppo dei Sistemi di Conservazione.

All'interno dell'area operano diversi archivisti, che si occupano di analizzare le problematiche specifiche delle diverse tipologie documentarie, e in particolare la modellizzazione dei *pacchetti informativi*, di avviare in conservazione nuovi Enti e di estenderne l'uso del servizio a nuove strutture e a nuove tipologie documentarie, di formare gli utenti all'utilizzo del servizio, di verificare l'andamento dei versamenti, di supportare gli utenti nella pratica quotidiana del servizio. A questo scopo parte del personale a turno opera come help desk per gli utenti, sia nelle attività preliminari all'avvio del servizio, che nelle attività di esercizio del servizio stesso; va sottolineato che l'help desk non è una struttura separata, ma un insieme di attività svolte da archivisti a supporto degli utenti, utilizzando procedure e strumenti standardizzati, formalizzati e condivisi con gli altri operatori dell'help desk. Gli archivisti infine contribuiscono allo sviluppo delle nuove applicazioni partecipando quando necessario all'analisi funzionale e ai test preliminari al passaggio in produzione

Nella tabella successiva è riportata la mappatura tra le attività principali del Servizio e le strutture interessate. Per la rappresentazione grafica è stato utilizzato lo schema RACI:

- R, Responsible: ha il compito di svolgere una particolare attività
- A, Accountable: è responsabile dei risultati dell'attività o ha un ruolo di approvatore
- C, Consulted: è coinvolto attivamente nel processo indirizzando le azioni da compiere o le decisioni da prendere
- I, Informed: è mantenuto informato sulle azioni da compiere o sulle decisioni prese. Il soggetto informato non può influenzare il risultato

Attività	Resp. Servizio	Resp. Sicurezza dei Sistemi	Resp. Funzioni di Supporto e Qualità	Resp. Funzione Archivistica Conservazione	Resp. Esercizio di conservazione	Resp. Servizi Tecnologici Infrastrutture	Resp. Tecnologie e Sviluppo dei Sistemi	Resp. Trattamento Dati Personali
Gestione delle Convenzioni	A		R	C	C			

Attività	Resp. Servizio	Resp. Sicurezza dei Sistemi	Resp. Funzioni di Supporto e Qualità	Resp. Funzione Archivistica Conservazione	Resp. Esercizio di conservazione	Resp. Servizi Tecnologici Infrastrutture	Resp. Tecnologie e Sviluppo dei Sistemi	Resp. Trattamento Dati Personali
Attivazione del servizio di conservazione	A			C	R			
Gestione del processo di conservazione				A	R			
Chiusura del servizio di conservazione	A			C	R			
Gestione Infrastruttura	I			I	I	A, R	I	
Sviluppo e manutenzione del sistema	I			I	I	I	A, R	
Monitoraggio del servizio di conservazione	A			R	R	R		
Gestione del Sistema di Qualità	C		A,R	C	C	C	C	C
Verifica di conformità a norme e std di conservazione			I	A, R		I	I	C
Gestione Sicurezza del sistema	I	A,R				I	I	
Gestione degli incidenti di sicurezza	I	A,R		I	I	C	C	I
Gestione del Cambiamento	A	C		C	C	C	R	
Gestione mal-funzionamenti	A			R	R	R	R	
Rapporti con le Autorità di vigilanza	I			A,R				
Amministrazione Processi di Certificazione	I	I	A,R	I	I	I	I	
Trattamento dei dati personali	I	I		R	R			A

[\[Torna al Sommario\]](#)

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

Il *Sistema di conservazione* gestito da ParER (Sistema), conserva *Documenti informatici*, in particolare documenti amministrativi informatici, con i *metadati* ad essi associati e le loro *Aggregazioni documentali informatiche*, che includono i Fascicoli informatici (Fascicoli). Inoltre il Sistema gestisce l'organizzazione e la descrizione dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* in **Serie**.

Tale modello riprende quello gerarchico di ordinamento di un *archivio*, illustrato in **Errore**. **L'origine riferimento non è stata trovata.**, derivata dallo schema dello standard **ISAD**.

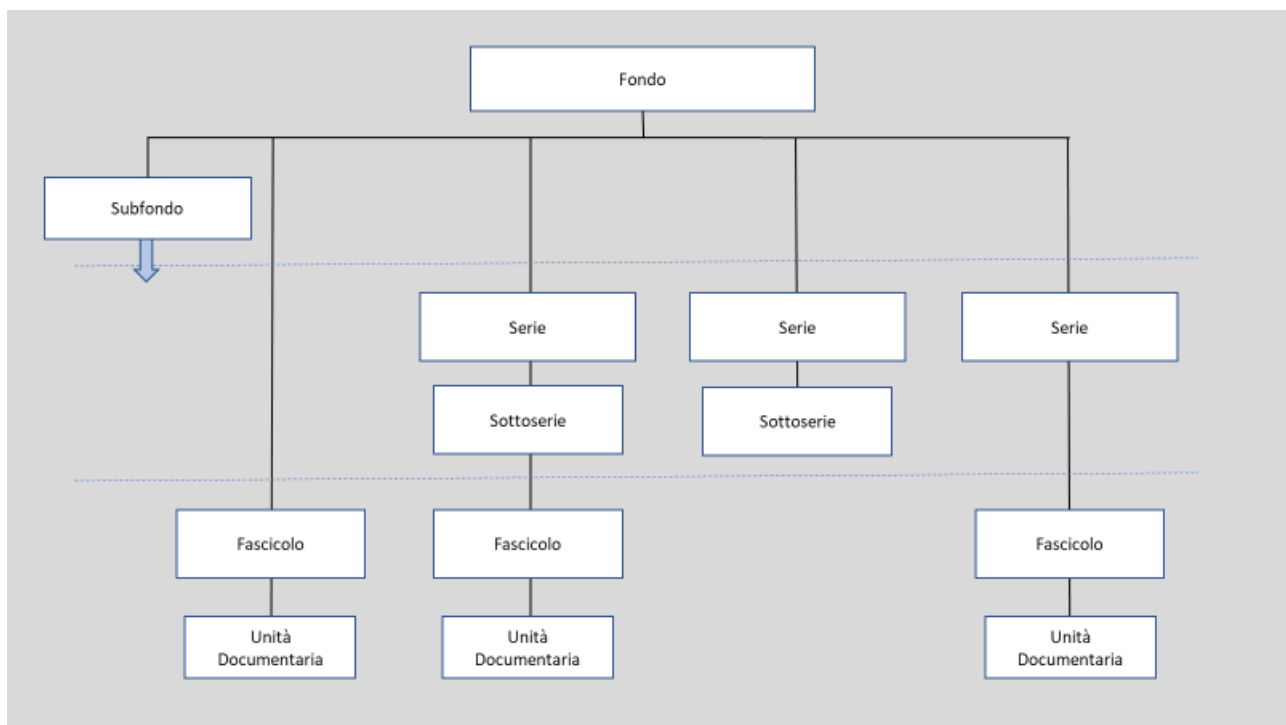


Figura 4 - Modello di ordinamento di archivio derivato da ISAD

I *Documenti informatici* e le loro *Aggregazioni documentali informatiche* (fascicoli) sono trattati nel sistema nella forma di **Unità documentarie** e **Unità archivistiche**, specificamente descritte nel paragrafo 6.1.1, e sono inviati in conservazione sotto forma di *Pacchetti di versamento* (SIP), che contengono sia i documenti che i relativi *metadati*.

Il Sistema gestisce gli oggetti sottoposti a conservazione in *archivi*, articolati in **Strutture** (generalmente, ma non necessariamente, corrispondenti alle Aree Organizzative Omogenee delle Pubbliche Amministrazioni) e distinti per ogni singolo *Produttore*.

Per mantenere anche nel Sistema le informazioni relative alla struttura dell'*archivio* e dei relativi vincoli archivistici, le **Unità documentarie** sono versate corredate di un set di *metadati* di Profilo archivistico che include gli elementi identificativi e descrittivi del Fascicolo, con riferimento alla

voce di *classificazione* e l'eventuale articolazione in sottofascicoli. Inoltre, è gestita la presenza di classificazioni, fascicoli e sotto-fascicoli secondari e collegamenti tra le diverse **Unità archivistiche** e documentarie presenti nel sistema.

Le **Unità archivistiche** e le **Serie** sono versate nel Sistema quando sono complete e dichiarate chiuse, descritte da un set di *metadati* che include obbligatoriamente, oltre alle informazioni di identificazione, *classificazione* e descrizione, anche il tempo di conservazione previsto. Nel caso delle **Serie** la chiusura avviene normalmente a cadenza annuale (o comunque secondo una definizione temporale definita dal *Produttore*) ed è da intendersi come chiusura della partizione periodica della Serie stessa (ad esempio, la partizione annuale della serie delle Determinazioni corrisponde alle determinazioni prodotte in un determinato anno e tale partizione va ad alimentare la relativa serie).

I *Documenti informatici* (**Unità documentarie**), e, in certi casi, i Fascicoli (**Unità archivistiche**) sono suddivisi in **tipologie documentarie** (definite nel sistema Tipi unità documentarie e Tipi fascicolo), che identificano gruppi documentali omogenei per natura e funzione giuridica, modalità di registrazione o di produzione. Tale suddivisione è funzionale all'individuazione, per ogni singola **tipologia documentaria**, di set di *metadati* standard e di articolazioni o strutture di composizione omogenee. Inoltre, le **tipologie documentarie** in molti casi individuano le **Serie** in cui si articola e organizza la produzione documentale del *Produttore*.

Per le principali **tipologie documentarie**, l'Area Funzione archivistica elabora e pubblica documenti di studio ed analisi (modelli degli AIP e dei SIP), che definiscono per ogni **tipologia documentaria**:

- il set dei *metadati* descrittivi che le caratterizzano, ritenuti essenziali per la corretta conservazione dei documenti e delle aggregazioni documentali informatiche (vedi più avanti paragrafo 6.1.3), in coerenza con quanto stabilito nell'Allegato 5 delle **Regole tecniche**;
- la struttura in base a cui sono articolate (vedi più avanti paragrafo 6.1.1).

A titolo esemplificativo, si riportano le principali macrocategorie di **tipologie documentarie** gestite e conservate:

- **Documentazione amministrativa:** documenti inerenti all'attività degli organi consiliari, contratti e accordi, decreti e ordinanze, deliberazioni, determinazioni, documentazione contabile, documenti protocollati, registri, strumenti urbanistici, ecc.;
- **Documentazione sanitaria:** referti e immagini diagnostiche;
- **Documentazione scolastica:** pagelle e registri didattici
- **Documentazione universitaria:** verbali di esame e altri documenti inerenti all'attività didattica;
- **Documenti di conservazione:** Evidenze informatiche prodotte da altri *sistemi di conservazione*.

Benché il Sistema operi primariamente su *Documenti informatici* originali e su Fascicoli informatici, al fine di mantenere la completezza e la consistenza dei fascicoli, e più in generale dell'*archivio* nel suo complesso, nel caso di Fascicoli ibridi è previsto l'invio al Sistema anche delle copie per immagini di originali analogici o dei soli *metadati* relativi a documenti in originale analogico.

Stante la natura eterogenea degli *archivi* conservati da ParER, diverse sono le attività svolte a garanzia non solo della integrità ma anche della fruibilità degli *archivi* stessi nel lungo periodo per mantenere la loro leggibilità e reperibilità, anche nella prospettiva della futura fruizione come archivi storici.

A tal fine le strategie adottate per la conservazione a cura di ParER prevedono le seguenti azioni:

- definire con precisione la **Comunità di riferimento** di ogni *archivio*, in accordo con i *Produttori*;
- analizzare le caratteristiche archivistiche e tecnologiche dei documenti conservati;
- mantenere attivo un osservatorio tecnologico sulla conservazione ed effettuare sperimentazioni sulle tecnologie disponibili, con particolare riguardo alle tecnologie open source ed ai progetti nazionali e internazionali nell'area della conservazione;
- collaborare attivamente con le autorità istituzionalmente preposte alla definizione del quadro normativo e delle regole operative per la conservazione documentale e con le autorità di sorveglianza.

In ragione dei diversi fattori che influiscono sulla fruibilità degli *archivi* nel lungo periodo, ParER adotta diverse misure per garantire la reperibilità e la *leggibilità* dei documenti conservati negli *archivi*. In particolare per quanto riguarda la reperibilità dei documenti si prevedono appropriate procedure di natura archivistica (creazione di **Serie** e fascicoli, arricchimento di *metadati*, collegamento tra documenti interrelati, ecc.), mentre per quanto riguarda la *leggibilità* si prevedono procedure di manutenzione dei *formati*, che possono variare in ragione della **Comunità di riferimento** e delle caratteristiche archivistiche e tecnologiche dei documenti stessi; p.e. nel caso di studi in standard **DICOM**, che vengono restituiti solo a sistemi **PACS**, non vengono operate trasformazioni di *formato*, mentre nel caso di formati proprietari o deprecati di documenti amministrativi destinati ad avere ampia diffusione, si possono operare attività di trasformazione verso formati standard aperti (p.e. pdf/A); l'adozione di trasformazioni dipende dalla vita utile del documento (p.e. non vengono trasformati documenti che saranno sottoposti a *scarto* nel breve periodo), dagli accordi con il *Produttore* e da considerazioni più generali di natura tecnologica ed archivistica. Quando necessario ParER sviluppa e mantiene nel tempo appositi sistemi di accesso per specifiche **tipologie documentarie**, a garanzia della fruibilità nel lungo periodo.

Gli oggetti sottoposti a conservazione, siano essi *Aggregazioni documentali informatiche*, *Documenti informatici*, o *metadati*, sono trasmessi dal *Produttore*, memorizzati e conservati nel Sistema e distribuiti agli *Utenti* sotto forma di *pacchetti informativi*. Il *pacchetto informativo*, a seconda sia utilizzato per versare, conservare o distribuire gli oggetti sottoposti a conservazione, assume la forma, rispettivamente, di *Pacchetto di versamento* (SIP), *Pacchetto di archiviazione* (AIP) e *Pacchetto di distribuzione* (DIP), descritti rispettivamente nei paragrafi 6.2, 6.3 e 6.4.

Il *pacchetto informativo* è un contenitore astratto che contiene due tipi di informazione: il **Contenuto informativo** (o Content information) e le **Informazioni sulla conservazione** (PDI – Preservation Description Information), la cui correlazione è identificata dalle **Informazioni sull'impacchettamento** (PI – Packaging information). Il *pacchetto informativo*, inoltre, è descritto e può essere ricercato nel Sistema grazie alle **Informazioni descrittive** (Descriptive information).

Una rappresentazione grafica del *pacchetto informativo*, ripresa dal Modello **OAIS**, è riportata in figura.

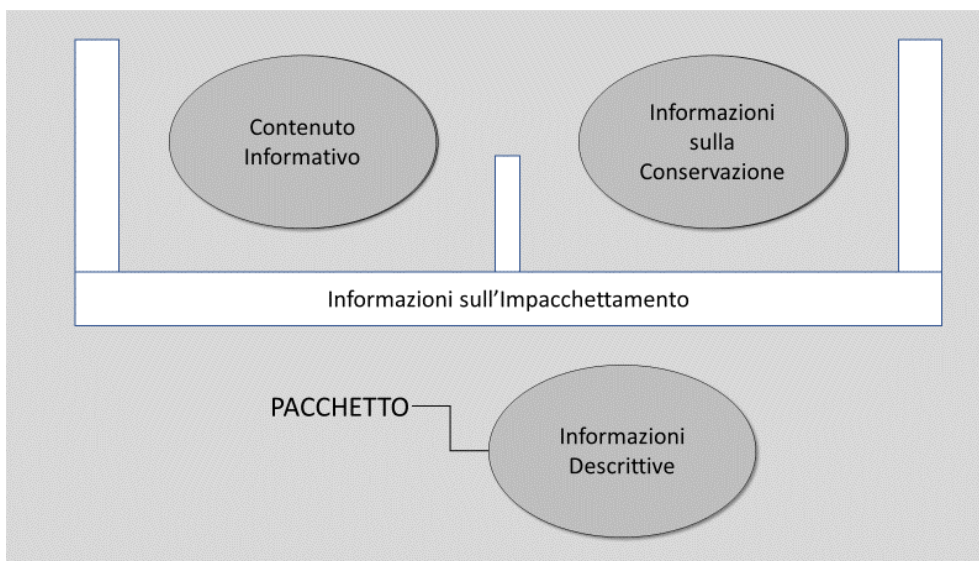


Figura 5 - Pacchetto informativo (da OAIS)

Il **Contenuto informativo** contiene le informazioni che costituiscono l'oggetto originario della conservazione ed è composto da due elementi:

- **Oggetto-dati:** può assumere la forma di sequenza di bit (tipicamente un file), qualora l'oggetto sia digitale, o solo da informazioni (*metadati*), qualora sia un oggetto materiale (ad esempio, un documento analogico);
- **Informazioni sulla rappresentazione:** costituiscono le informazioni necessarie a rendere comprensibile l'**Oggetto-dati** agli *Utenti*. Il caso tipico di **Informazioni sulla rappresentazione** è costituito dalle informazioni relative al *formato* con cui la sequenza di bit è codificata, informazioni che consentono al Sistema di decodificare opportunamente la sequenza di bit per essere correttamente rappresentata e resa intelligibile agli *Utenti* del Sistema.

Le **Informazioni sulla conservazione** sono le informazioni necessarie a conservare il **Contenuto informativo** e garantiscono che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da *metadati* che definiscono la provenienza, il contesto, l'identificazione e l'*integrità* del **Contenuto informativo** oggetto della conservazione.

Le **Informazioni sull'impacchettamento** sono informazioni che consentono di mettere in relazione nel Sistema, in modo stabile e persistente, il **Contenuto informativo** con le relative **Informazioni sulla conservazione**.

Le **Informazioni descrittive**, infine, descrivono il *pacchetto informativo* e consentono di ricercarlo nel Sistema. In base alle caratteristiche della tipologia di oggetto contenuto nel Pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel *pacchetto informativo*, possono coincidere o possono anche essere diverse.

[\[Torna al Sommario\]](#)

6.1.1 Unità archivistiche e Unità documentarie

Le **Unità archivistiche** contengono una o più **Unità documentarie**, secondo le logiche di *classificazione* e fascicolazione utilizzate dal *Produttore* per organizzare i documenti prodotti nel proprio *archivio* (vedi figura successiva).

L'**Unità documentaria** rappresenta l'unità minima elementare di riferimento di cui è composto un *archivio*, pertanto rappresenta il riferimento principale per la costruzione dei *pacchetti informativi* di cui ai paragrafi 6.2, 6.3 e 6.4..

Con riferimento a quanto indicato nello standard ISO 23081-2, l'**Unità documentaria**, rappresenta la più piccola "unit of records" individuabile e gestibile come una entità singola gestita nel Sistema, anche se al suo interno contiene elementi e **Componenti** come, ad esempio, un messaggio di posta elettronica con i suoi allegati.

All'**Unità documentaria** e agli elementi che la compongono sono associati set di *metadati* che li identificano e li descrivono, secondo le logiche e le articolazioni esposti al paragrafo 6.1.3.

Coerentemente con quanto sopra riportato l'Unità Documentaria è pertanto strutturata su tre livelli: Unità Documentaria, **Documento**, **Componente**, come rappresentato in figura.

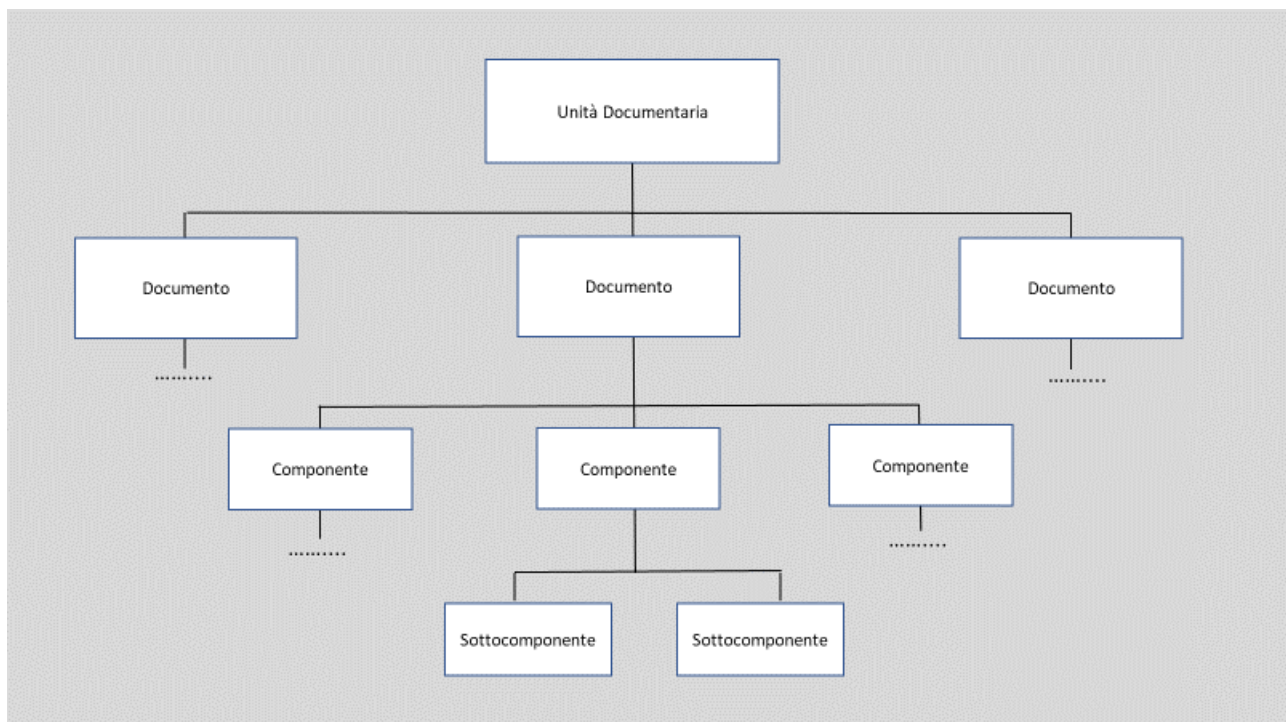


Figura 6 - Struttura dell'Unità documentaria

L'**Unità documentaria** fa sempre riferimento a una specifica **tipologia documentaria** che ne determina oltre ai *metadati* di riferimento anche la struttura, in termini di definizione ed articolazione in **Documenti** e **Componenti** in essa contenuti.

I **Documenti** sono gli elementi dell'**Unità documentaria** e sono identificati in base alla funzione che svolgono nel contesto dell'**Unità documentaria** stessa, ovvero:

- **Documento principale:** è il **Documento** che definisce il contenuto primario dell'**Unità documentaria**. È obbligatorio e deve essere sempre presente;

- **Allegato:** è un **Documento** redatto contestualmente o precedentemente al **Documento principale** ed unito a questo, come parte integrante, per memoria, prova, chiarimento o integrazione di notizie. È facoltativo;
- **Annesso:** è un **Documento**, generalmente prodotto e inserito nell'**Unità documentaria** in un momento successivo rispetto a quello del **Documento principale**, per fornire ulteriori notizie e informazioni a corredo del **Documento principale**. È facoltativo;
- **Annotazione:** può essere costituita da quegli elementi che tradizionalmente in ambiente cartaceo venivano apposti sullo stesso supporto del **Documento principale** come elementi identificativi del **Documento** e del suo iter documentale e che in ambito informatico si sono mutati in **Documenti** associati al **Documento principale** (un tipico esempio di Annotazione è rappresentato dalla segnatura di protocollo). È facoltativa.

I **Componenti** individuano il contenuto del **Documento**. Normalmente tale contenuto è digitale, ovvero costituito da una sequenza di bit, generalmente sotto forma di file, e i relativi *metadati*, tra cui quelli che identificano il *formato*. È possibile, però, che in taluni casi, il **Componente** sia espresso solo da *metadati* e sia quindi privo della sequenza di bit. Tipicamente questo avviene quando l'oggetto della conservazione non è digitale (ad esempio, documenti presenti solo in originale analogico).

Inoltre, esiste una particolare categoria di **Componenti** definiti **Sotto componenti**, che contengono elementi integrativi del **Componente** rappresentati da sequenze di bit distinte da quelle del **Componente** (ad esempio, *marche temporali detached* o *firma detached*). Il **Sotto componente** ha una struttura del tutto simile al **Componente** ed è associato logicamente al **Componente** cui fa riferimento.

[\[Torna al Sommario\]](#)

6.1.2 Formati

Il *Sistema* utilizza come *formati* di conservazione quelli elencati al punto 5 dell'Allegato 2 alle **Regole tecniche** e, inoltre, è in grado di trattare, su richiesta del *Produttore*, anche *formati* non compresi nel suddetto elenco ma che il *Produttore* utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i Formati gestiti sono elencati e descritti in un registro interno al Sistema denominato "Registro dei formati" in cui ogni *formato* è corredato da informazioni relative a estensioni e **mimetype**. Inoltre, ogni *formato* è classificato in base alla sua idoneità a essere conservato a lungo termine. Sulla base di questa suddivisione i *formati* si dividono in:

- **Formati idonei:** sono i *formati* che per le loro caratteristiche di standardizzazione, di apertura, di sicurezza, di portabilità, di *immodificabilità*, di *staticità* e di diffusione sono reputati idonei alla conservazione a lungo termine;
- **Formati gestiti:** sono i *formati* leggibili e accessibili ma potenzialmente soggetti a obsolescenza tecnologica e che, in caso di necessità, possono essere opportunamente migrati in Formati idonei con idonee procedure;
- **Formati deprecati:** sono *formati* ritenuti non idonei per la conservazione a lungo termine e che al contempo non possono essere migrati in Formati idonei, per i quali, quindi, non è possibile assicurare la conservazione a lungo termine.

Con ogni *Produttore* è concordato un elenco di Formati ammessi, che individua i *formati* che il Sistema può accettare da ogni *Produttore* e per ogni **tipologia documentaria** gestita. L'elenco dei Formati ammessi è riportato (e gestito) nelle funzionalità "Amministrazione strutture versanti" del Sistema ed è aggiornato continuamente in base alle esigenze del *Produttore*

Il Sistema identifica i *formati* al momento della ricezione del SIP (vedi paragrafo 7.2) mediante l'analisi dei **magic number** o del contenuto del file, in modo tale da consentire l'individuazione dello specifico **mimetype**.

L'informazione sul *formato* è parte dei *metadati* dei **Componenti** dell'**Unità documentaria** e costituisce elemento dell'Informazione sulla rappresentazione (vedi paragrafo 6.1).

[\[Torna al Sommario\]](#)

6.1.3 Metadati

I *metadati* gestiti dal Sistema sono individuati in coerenza con la normativa italiana e con gli standard e i modelli internazionali di riferimento. Più in dettaglio sono descritti ed analizzati per specifici oggetti da conservare e specifiche **tipologie documentarie** tramite i modelli di SIP pubblicati sul sito del ParER.

I *metadati* gestiti, in base alle funzioni cui assolvono, si dividono nelle seguenti macro classi:

- **Metadati di identificazione:** identificano in modo univoco le **Unità documentarie** e archivistiche. Includono i dati identificativi del *Produttore* e i dati di registrazione originari, nonché gli identificativi specifici di ogni elemento dell'**Unità documentaria** (**Documenti** e **Componenti**);
- **Metadati di struttura:** descrivono la struttura dell'**Unità archivistica o documentaria**, indicando nell'ultimo caso il numero e la tipologia di **Allegati**, **Annessi** e **Annotazioni** che la compongono, nonché, per ognuno di essi, il numero e la tipologia dei **Componenti**;
- **Metadati di profilo archivistico:** descrivono il Fascicolo e più in generale la collocazione dell'**Unità documentaria** nel contesto dell'*archivio* del *Produttore*. Ricomprendono anche i *metadati* che collegano l'**Unità documentaria** ad altre **Unità documentarie** conservate nel sistema (Collegamenti);
- **Metadati di profilo generali:** individuano gli elementi descrittivi essenziali comuni alle diverse tipologie di **Unità archivistiche**, **Unità documentarie** e relativi elementi;
- **Metadati di profilo specifici:** individuano elementi descrittivi ulteriori rispetto a quelli previsti nel profilo generale. Sono definiti per ogni tipologia di **Unità archivistica e documentaria** e per ogni *Produttore*;
- **Metadati di conservazione:** sono tipicamente generati dal Sistema nel corso del *processo di conservazione* e attengono tanto all'analisi e alle verifiche effettuate sugli oggetti conservati, che alla descrizione delle attività svolte dal Sistema. Tra i Metadati di conservazione rientrano anche i *metadati* associati alle **Unità archivistiche e documentarie** provenienti da altri *sistemi di conservazione* (Metadati specifici di migrazione) e che contengono le informazioni relative al *processo di conservazione* di cui le **Unità archivistiche e documentarie** sono state eventualmente oggetto prima di essere versate nel Sistema.

[\[Torna al Sommario\]](#)

6.2 Pacchetto di versamento (SIP)

I pacchetti di versamento (SIP) sono concordati per struttura e contenuto con il *Produttore* e contengono l'oggetto o gli oggetti da conservare. In base alle specifiche esigenze possono contenere una o più **Unità archivistiche**, una o più **Unità documentarie**, un **Documento** da aggiungere a un'**Unità documentaria** già versata o solo informazioni relative a un'**Unità documentaria** già conservata da aggiornare. Ogni SIP può generare uno o più *Pacchetti di archiviazione* così come più SIP possono costituire un unico *Pacchetto di archiviazione*.

I SIP sono composti dai file dei **Componenti** e dall'**Indice del SIP** (file XML che contiene i *metadati* e la struttura del pacchetto).

Per essere acquisiti e presi in carico dal Sistema i SIP devono rispettare una determinata struttura dati nell'ambito della quale viene concordato con il Produttore il contenuto informativo da portare in conservazione. La struttura dati è descritta nelle Specifiche tecniche dei servizi di versamento, mentre le procedure per la trasmissione e l'acquisizione dei SIP sono descritte nel capitolo 7.1.

I vari modelli di SIP gestiti dal Sistema, descritti in dettaglio nelle Specifiche dei Servizi di Versamento sono:

- SIP di un'**Unità archivistica**: è il SIP utilizzato per versare le *Unità archivistiche* (Fascicoli). Contiene i *metadati* descrittivi dell'**Unità archivistica** e l'elenco delle **Unità documentarie** in esso contenute. Genera un corrispondente *Pacchetto di archiviazione* relativo all'**Unità archivistica**;
- SIP di un'**Unità documentaria**: contiene un'**Unità documentaria** completa in tutti gli elementi presenti nei sistemi del *Produttore* al momento del versamento. Il versamento di un pacchetto contenente un'**Unità documentaria** genera un corrispondente *Pacchetto di archiviazione*;
- SIP di un **Documento**: è utilizzato per aggiungere un singolo **Documento** e i relativi *metadati* a un'**Unità documentaria** già presente nel Sistema. Il versamento di tale pacchetto genera l'aggiornamento del *Pacchetto di archiviazione* dell'**Unità documentaria** cui il **Documento** viene aggiunto. La necessità di aggiungere un **Documento** a un'**Unità documentaria** già presente si presenta tipicamente in due casi:
 - quando, per numerosità e dimensioni, è preferibile suddividere il versamento di un'**Unità documentaria** in più parti;
 - qualora uno o più **Documenti** appartenenti a un'**Unità documentaria** siano disponibili sul sistema del *Produttore* solo in un momento successivo a quello in cui l'**Unità documentaria** di cui fanno parte è stata versata nel Sistema;
- SIP di Aggiornamento metadati: è utilizzato per versare nel Sistema esclusivamente informazioni, tipicamente *metadati*, per integrare, modificare o sostituire quelle già presenti in un'**Unità documentaria** già conservata nel Sistema. Il versamento di tale pacchetto genera l'aggiornamento del *Pacchetto di archiviazione* dell'**Unità documentaria** i cui i metadati vengono aggiornati.

Nel caso in cui, per motivi tecnici o organizzativi, il *Produttore* non sia in grado di produrre o versare SIP nella struttura dati richiesta, può trasmettere i documenti sotto forma di generici **Oggetti** il cui contenuto e struttura è concordato con l'Ente conservatore. Tali **Oggetti** sono sottoposti alla procedura di Preacquisizione (descritta nel paragrafo 7.1.1) per essere trasformati in SIP ed essere così accettati dal Sistema.

[\[Torna al Sommario\]](#)

6.3 Pacchetto di archiviazione (AIP)

Il *Pacchetto di archiviazione* viene generato dal Sistema a conclusione del processo di acquisizione e *presa in carico* dei SIP (vedi paragrafo 7.5). È composto dagli **Oggetti-dati** (file), dall'**Indice dell'AIP**, un file XML che contiene tutti gli elementi del *pacchetto informativo*, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal *Produttore*, sia da quelle generate dal Sistema nel corso del *processo di conservazione* e dai Documenti di conservazione, ovvero i documenti ricevuti o prodotti nel corso del processo di conservazione (Indici dei SIP, Esiti versamenti, ecc.).

L'**Indice dell'AIP** generato dal Sistema è conforme alle specifiche definite nell'Allegato 4 delle **Regole tecniche** e agli specifici Standard individuati dall'Allegato 3.

La tabella seguente illustra come i vari elementi del *pacchetto informativo* sono presenti nell'AIP gestito dal Sistema.

Elemento del pacchetto informativo	Articolazione dell'elemento	Descrizione
Contenuto informativo	Oggetto-dati	È la sequenza di bit (tipicamente sotto forma di file) associata al Componente . Può coincidere con quella inviata nel SIP dal <i>Produttore</i> o essere stata generata, a partire da questa, dal Sistema nel caso di produzione di copie informatiche.
	Informazioni sulla rappresentazione	Sono contenute a livello di Componente nell' Indice dell'AIP e sono derivate sia da quelle contenute nel SIP di origine, sia da quelle generate dal Sistema. Includono i <i>metadati</i> relativi al <i>formato</i> .
Informazioni sulla conservazione	Metadati di provenienza, contesto, identificazione, integrità	Sono contenuti nell' Indice dell'AIP a livello di Unità archivistica, Unità documentaria, Documento e Componente e originano dai SIP ricevuti o dai documenti generati dal <i>processo di conservazione</i> .

Elemento del pacchetto informativo	Articolazione dell'elemento	Descrizione
Informazioni su l'impacchettamento	-	A livello di Unità archivistica sono contenute nell'Indice e includono i riferimenti alle Unità documentarie che la compongono. A livello di Unità documentaria sono contenute nei Metadati di struttura e a livello di Componente negli identificativi utilizzati per associare il Componente all'Oggetto-dati.

Il Sistema è in grado di gestire e produrre tre tipi di AIP, descritti in dettaglio nel documento Modelli di AIP:

- AIP di **Unità documentaria**: contiene gli **Oggetti-dati** e si configura come **Unità di archiviazione** (AIU) in quanto oggetto elementare conservato nel Sistema;
 - AIP di **Unità archivistica**: il caso tipico è il Fascicolo e si configura come una collezione di AIP o **Raccolta di archiviazione** (AIC) il cui contenuto informativo è costituito dagli AIP delle singole unità documentarie appartenenti al fascicolo;
- AIP di Serie: si divide a sua volta in AIP di Serie di Unità documentarie e in AIP di Serie di Unità archivistiche (fascicoli). Si configura anch'essa come una collezione di AIP.

[\[Torna al Sommario\]](#)

6.4 Pacchetto di distribuzione (DIP)

Il *Pacchetto di distribuzione* viene generato dal Sistema a partire dai *Pacchetti di archiviazione* conservati ed è finalizzato a mettere a disposizione degli *Utenti*, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione.

Il Sistema mette a disposizione degli *Utenti*, per tutti gli oggetti sottoposti a conservazione, un DIP coincidente con l'AIP, ma può gestire la produzione di DIP specifici in relazione a particolari esigenze. In relazione alle sue caratteristiche e agli utilizzi a cui è destinato, il *Pacchetto di distribuzione* può essere generato al momento della richiesta da parte di un *Utente* e non conservato nel Sistema.

Le modalità di *esibizione* dei DIP sono descritte al paragrafo 7.6.

[\[Torna al Sommario\]](#)

7 PROCESSO DI CONSERVAZIONE

Il *processo di conservazione* si attiva a seguito di sottoscrizione della **Convenzione** tra il *Produttore* e IBACN con le modalità indicate nella **Convenzione** stessa e dettagliate nel **Disciplinare tecnico**. La **Convenzione** medesima disciplina anche la chiusura del servizio in caso di recesso o scadenza della **Convenzione** stessa, con le modalità operative descritte nel paragrafo 7.9.

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Il *processo di conservazione* si basa su una logica di conservazione caratterizzata dal **versamento** da parte dei *Produttori* degli oggetti da conservare (*Documenti informatici e Aggregazioni documentali informatiche*) in due fasi: **Versamento anticipato** e **Versamento in archivio**.

Con **Versamento anticipato** si intende il **versamento** nel *Sistema di conservazione* di singoli *Documenti informatici* che possono trovarsi ancora nella fase attiva del loro ciclo di vita. Tale versamento avviene in un momento il più possibile prossimo a quello di effettiva produzione del documento ed è definito anticipato perché interviene in un momento antecedente a quello previsto normalmente dalla pratica archivistica, ovvero il versamento del Fascicolo chiuso, o della **Serie** completa (o di partizioni di essa) in archivio di deposito.

Il **Versamento anticipato** è finalizzato a mettere in sicurezza l'oggetto, prevedendo una serie di controlli tesi a verificarne i metadati, il *formato* e le eventuali firme digitali apposte, al fine di mettere in atto le opportune misure necessarie alla sua conservazione a lungo termine, ovvero:

- la rilevazione dell'eventuale obsolescenza dei formati dei file, in modo da attivare per tempo le misure necessarie a mantenerne la leggibilità;
- l'apposizione di un riferimento temporale certo e opponibile a terzi;
- la rilevazione di eventuali anomalie o errori nella produzione dei documenti, anche al fine di segnalare al *Produttore* le opportune contromisure per la loro risoluzione.

In questa fase è prevista l'acquisizione nel Sistema anche di *Documenti informatici* per i quali la normativa stabilisce tempi precisi di versamento come, ad esempio, il registro giornaliero di protocollo che deve essere "trasMESSO entro la giornata lavorativa successiva al *Sistema di conservazione*, garantendo l'*immodificabilità* del contenuto"¹⁵.

Con **Versamento in archivio** si intende il **versamento** nel Sistema delle *Aggregazioni documentali informatiche* nella loro forma stabile e definitiva, principalmente Fascicoli chiusi e partizioni annuali di **Serie** documentarie ¹⁶.

¹⁵ DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico...", art. 7 comma 5.

¹⁶ In ottemperanza a quanto previsto dall'art. 67 del DPR 445/2000, che al comma 1 prevede che "Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione".

Questa fase del *processo di conservazione*, assimilabile al versamento dall'archivio corrente all'archivio di deposito, assolve a un duplice obiettivo: da un lato portare nel Sistema le informazioni necessarie a costruire l'*archivio informatico* dell'ente; dall'altro aggiornare e fissare definitivamente, qualora si rendesse necessario, le informazioni di corredo relative alle **Unità documentarie** versate anticipatamente nel Sistema.

Il versamento in archivio di un'aggregazione documentale informatica avviene dopo che i singoli elementi che compongono l'aggregazione sono stati versati nel Sistema. Nel SIP dell'aggregazione sono elencati tutti gli elementi che la compongono e il versamento avviene solo se nel Sistema questi sono tutti presenti.

A tal fine, prima di procedere con il loro versamento in archivio, è consigliabile effettuare l'aggiornamento dei metadati relativi alle Unità documentarie versate in Versamento anticipato in modo da assicurare che i metadati conservati nel Sistema siano completi e definitivi.

In altri termini si può dire che con il **Versamento in archivio** viene completato, da parte del *Produttore*, il *processo di conservazione* iniziato con il **Versamento anticipato**, assicurando che gli oggetti digitali siano correttamente conservati a partire dal momento della loro produzione e resi accessibili per gli usi previsti (esibizione, accesso amministrativo, studio e ricerca). Al tempo stesso, il Sistema è messo in condizioni di acquisire, man mano che sono disponibili, le informazioni di contesto archivistico degli oggetti conservati e di assicurare in questo modo la corretta formazione dell'*archivio* del *Produttore*.

Il Sistema inoltre gestisce altre modalità di conservazione particolari:

- **Conservazione fiscale**, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari, in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze);
- **Migrazione**, che ha per oggetto *Documenti informatici e/o Aggregazioni documentali informatiche* provenienti da altri *sistemi di conservazione*. La peculiarità di questa conservazione risiede nella necessità di garantire il mantenimento della catena di custodia e si sostanzia nell'acquisizione, oltre che degli oggetti da sottoporre a conservazione, anche dei documenti e dei *metadati* prodotti dal *Sistema di conservazione* di provenienza; qualora il sistema di provenienza sia un *Sistema di conservazione* conforme alle **Regole tecniche** ai fini dell'*interoperabilità*, il SIP avrà le caratteristiche definite nelle **Regole tecniche** all'articolo 9 lettera h.

I SIP sono prodotti e versati nel Sistema sotto la responsabilità del *Produttore* con le modalità e le procedure descritte nei loro aspetti generali nel presente Manuale e, per gli aspetti operativi e specifici relativi a ogni *Produttore*, nei **Disciplinari tecnici**, dove sono illustrati i *Documenti informatici* e le *Aggregazioni documentali informatiche* oggetto di conservazione e le procedure operative per il loro **versamento** e acquisizione nel Sistema.

Al momento dell'acquisizione i SIP sono oggetto di una serie di verifiche automatiche. Nel caso in cui le verifiche abbiano successo, il **versamento** viene accettato, il SIP acquisito per la sua *presa in carico* e generato in modo automatico dal Sistema il *Rapporto di versamento*, che viene inviato al sistema che ha effettuato il **versamento** in un documento in formato XML denominato "**Esito versamento**". Qualora il SIP non abbia superato i controlli, l'**Esito versamento** riporta il dettaglio degli errori che hanno causato il fallimento del **versamento**.

I SIP presi in carico dal Sistema sono inseriti in ***Elenchi di versamento***, documenti in formato XML che vengono validati dal Responsabile della funzione archivistica di conservazione o automaticamente dal Sistema. La validazione dell'Elenco innesca la generazione dei *Pacchetti di archiviazione* (AIP) relativi ai SIP in Elenco.

Va ricordato che il Sistema è in grado di acquisire e prendere in carico automaticamente solo SIP che rispettano la struttura dati indicata nei Modelli di SIP e nelle Specifiche tecniche dei servizi di versamento (vedi paragrafo 6.2). Qualora il Produttore non sia in grado di versare i documenti come SIP, può trasmetterli sotto forma di Oggetti (di formato e struttura concordati con l'Ente conservatore) per sottoporli a un'elaborazione preliminare (Preacquisizione), svolta dal Sistema e finalizzata alla loro trasformazione in SIP.

In base a quanto appena illustrato, il processo di acquisizione e *presa in carico* dei SIP prevede le seguenti fasi:

1. Preacquisizione;
2. Acquisizione;
3. Verifica;
4. Rifiuto o accettazione;
5. Presa in carico e generazione del Rapporto di versamento;
6. Generazione del Pacchetto di archiviazione.

Nei paragrafi seguenti sono illustrate nel dettaglio le varie fasi del processo.

[\[Torna al Sommario\]](#)

7.1.1 Preacquisizione

La fase di Preacquisizione ha in input un Oggetto e in output uno o più SIP e si avvia con la trasmissione dell'Oggetto a cura del *Produttore* o di un *Versatore* esterno da lui incaricato (vedi paragrafo 4.2). L'Oggetto trasmesso deve essere conforme alle specifiche definite dall'Ente conservatore. Il *Produttore/Versatore* trasmette l'Oggetto interfacciando i propri sistemi o utilizzando il client di versamento manuale messo a disposizione dall'Ente conservatore. Non è prevista la trasmissione degli Oggetti su supporti fisici.

Qualora la trasmissione abbia esito positivo al *Produttore* viene attestata la corretta ricezione dell'Oggetto.

L'Oggetto ricevuto è sottoposto a una serie di controlli finalizzati a verificarne la conformità con le relative specifiche. Le eventuali non conformità rilevate durante i controlli possono essere bloccanti o non bloccanti. Nel primo caso il processo si interrompe; nel secondo caso, invece, si interviene sull'oggetto ricevuto in modo da eliminare le non conformità rilevate. L'oggetto così modificato, unitamente alla descrizione degli interventi che ha subito, viene versato nuovamente nel Sistema e sottoposto nuovamente ai controlli di cui sopra.

Nel caso in cui i controlli abbiano esito positivo, il Sistema procede alle elaborazioni necessarie a versare il SIP, ovvero:

- trasformazione dell'Oggetto in uno più SIP: ogni SIP generato contiene il riferimento all'Oggetto dal quale è stato generato;

- **versamento** dei SIP nel Sistema: i SIP vengono versati nel Sistema con le modalità descritte nel paragrafo 7.1.2.

Il *Produttore* può in ogni momento interrogare il Sistema per ottenere informazioni sullo stato di avanzamento del processo di preacquisizione e sugli esiti del versamento dei SIP così generati.

[\[Torna al Sommario\]](#)

7.1.2 Acquisizione

L'acquisizione avviene con il **versamento** di SIP nel Sistema esclusivamente mediante l'utilizzo dei servizi descritti nel paragrafo 8.2 ed in dettaglio nel documento "Specifiche tecniche dei servizi di versamento".

Per effettuare il **versamento** dei SIP il *Produttore* può interfacciare i propri sistemi o, in alternativa, utilizzare il client di versamento manuale messo a disposizione da ParER mediante il quale inserire i dati necessari a generare e versare il SIP nel Sistema.

Non è prevista la trasmissione di SIP su supporti fisici.

Al completamento della trasmissione, il Sistema avvia contestualmente il processo di verifica del pacchetto, descritto nel paragrafo seguente.

[\[Torna al Sommario\]](#)

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Il SIP acquisito viene sottoposto a una serie di verifiche automatiche da parte del Sistema, finalizzate ad evidenziare eventuali anomalie.

Le verifiche riguardano:

- l'identificazione del Versatore: queste verifiche, effettuate mediante il controllo delle credenziali comunicate dal sistema versante a ogni versamento, sono finalizzate a garantire l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione e/o dell'*area organizzativa omogenea* di riferimento ai sensi del art. 44, comma 1 lettera a) del CAD e a garantire il corretto inserimento nell'*archivio* del *Produttore* nella opportuna **Struttura** (vedi paragrafo 6.1.1);
- la conformità dell'**Indice del SIP** al modello dati stabilito (vedi paragrafo 6.2): queste verifiche sono finalizzate a controllare se l'**Indice del SIP** è conforme al modello concordato con il *Produttore* e configurato nel sistema;
- l'univocità degli identificativi degli oggetti contenuti nel SIP: il controllo è finalizzato a verificare che gli identificativi assegnati dal *Produttore* e contenuti nel SIP siano effettivamente univoci, verificando che gli stessi non siano già presenti nel Sistema;

- la consistenza dei Metadati di profilo e specifici (vedi paragrafo 6.1.3): questa verifica è finalizzata a controllare che i set di Metadati presenti nel pacchetto siano conformi (in termini di obbligatorietà, valori e formato) a quelli concordati tra *Produttore* e l'Ente conservatore. Tali set sono configurati nel Sistema mediante le funzionalità di Amministrazione delle Strutture versanti;
- il controllo sulle eventuali firme digitali apposte sugli **Oggetti-dati** (file) contenuti nel pacchetto. Le verifiche sono finalizzate a controllare la regolarità della firma digitale apposta in ordine a: formato di firma utilizzato, *integrità* del documento firmato (controllo crittografico), catena trusted, validità del certificato (scadenza e formato), presenza di eventuali revoche. I controlli sono effettuati alla data indicata dal *Produttore* nel SIP (che può essere quella contenuta nella firma, in una marca temporale o un riferimento temporale dichiarato nell'Indice SIP) o, in assenza di questa, alla data del versamento;
- l'ammissibilità dei **formati** degli **Oggetti-dati** (file) presenti nel pacchetto in base a quanto concordato con il *Produttore*: le verifiche si esplicano nel calcolo del **mimetype** dell'**Oggetto-dati** e nel confronto del valore così ottenuto sia con quello eventualmente dichiarato dal *Produttore* nel SIP, sia con i Formati ammessi, documentati e conservati nel Sistema nelle funzionalità di Amministrazione delle strutture versanti;
- **i controlli di coerenza e consistenza delle Aggregazioni documentali informatiche versate:** si tratta di controlli che vengono svolti in caso di **Versamento in archivio** di aggregazioni documentali informatiche e sono finalizzati a verificare la coerenza e la completezza di quanto versato.

La descrizione analitica delle verifiche automatiche e dei controlli a cui sono sottoposti i SIP, nonché le logiche con cui il Sistema opera in questo frangente, sono illustrati nel documento "Specifiche tecniche dei servizi di versamento".

[\[Torna al Sommario\]](#)

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Nel caso in cui tutte le verifiche abbiano avuto esito positivo, il SIP viene acquisito nel Sistema per la sua *presa in carico*, memorizzato nelle sue varie parti (**Indice del SIP** e **Oggetti-dati**), associato logicamente all'*archivio* del *Produttore* ed eliminato dall'area di lavoro temporanea.

In particolare, l'**Indice del SIP** e gli **Oggetti-dati** vengono memorizzati nella loro *integrità* e mantenuti nel Sistema anche ai fini del loro successivo inserimento nell'AIP (vedi paragrafo 7.5). Le operazioni di acquisizione si concludono con la *presa in carico* dei SIP accettati e la generazione automatica del relativo *Rapporto di versamento* che viene memorizzato nel Sistema e associato al SIP cui si riferisce.

Il *Rapporto di versamento* contiene l'Identificativo univoco del Rapporto, il *Riferimento temporale* relativo alla sua creazione (specificato con riferimento al **tempo UTC**), l'*impronta* dell'**Indice del SIP** e le *impronte* degli **Oggetti-dati** che ne fanno parte, oltre alla descrizione sintetica del contenuto del SIP acquisito. La descrizione analitica del *Rapporto di versamento* e la relativa struttura dati è contenuta nel documento "Specifiche tecniche dei servizi di versamento".

Il *Riferimento temporale* contenuto nel *Rapporto di versamento* è generato dal Sistema con le modalità descritte nel capitolo 8 ed è quindi da considerarsi opponibile ai terzi in base a quanto previsto dal comma 4, lettera b) dell'art. 41 del DPR 22 febbraio 2013.

Il *Rapporto di versamento* è reso disponibile al *Produttore* in varie modalità:

- è trasmesso in risposta al **versamento** del SIP nell'**Esito versamento**, un documento in formato XML che contiene, oltre al *Rapporto di versamento*, l'elenco analitico dei controlli eseguiti e dei relativi esiti, i parametri di configurazione del Sistema al momento del versamento e la data di versamento del SIP, descritto in dettaglio nel documento "Specifiche tecniche dei servizi di versamento";
- può essere richiesto utilizzando un apposito servizio, secondo le modalità descritte nel documento "Specifiche tecniche dei servizi di recupero";
- può essere visualizzato e scaricato dall'interfaccia web del Sistema dagli operatori abilitati utilizzando le apposite funzionalità del Sistema.

[\[Torna al Sommario\]](#)

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Nel caso in cui almeno una delle verifiche elencate al paragrafo 7.3 non vada a buon fine, il SIP viene rifiutato e il Sistema restituisce al *Produttore* gli errori riscontrati, inviando l'**Esito versamento**, un documento in formato XML, descritto in dettaglio nel documento Specifiche tecniche dei servizi di versamento, in cui sono contenute tutte le informazioni sui controlli effettuati e i relativi esiti, sia sintetici che analitici, nonché l'**Indice del SIP** rifiutato.

I Pacchetti rifiutati, ovvero l'Indice dei SIP e gli **Oggetti-dati** che ne fanno parte, unitamente ai relativi **Esiti versamento**, sono memorizzati in un'area temporanea del Sistema, logicamente esterna all'*archivio* vero e proprio, a cui sia il *Produttore* che ParER possono accedere utilizzando l'interfaccia web del Sistema, per eventuali ulteriori controlli e verifiche (vedi paragrafo 7.4.1).

I SIP rifiutati restano memorizzati nel Sistema per almeno sei mesi; trascorso questo periodo possono essere cancellati, interamente o per la sola parte di **Oggetti-dati**. La cancellazione è stabilita ed effettuata sulla base di valutazioni che tengono conto delle **tipologie documentarie** trattate, delle caratteristiche del *Produttore* e della quantità e qualità dei versamenti falliti. Eventuali specifiche modalità e tempistiche di cancellazione dei SIP rifiutati sono concordate con il Produttore e configurate nel Sistema.

[\[Torna al Sommario\]](#)

7.4.1 Monitoraggio

Il Sistema mette a disposizione specifiche funzionalità di monitoraggio relative alla gestione dei **versamenti** dei SIP e alla generazione e gestione degli AIP, oltre a statistiche e report su quanto presente nel Sistema.

Il monitoraggio consente di avere una vista complessiva, suddivisa per fasce temporali, sull'acquisizione dei SIP, sul rifiuto dei SIP, sui tentativi falliti di versamento e sulle eventuali anomalie, mettendo a disposizione degli operatori tutte le informazioni necessarie a verificare tanto le anomalie che hanno impedito il **versamento** dei SIP nel Sistema, quanto tutti gli elementi relativi ai SIP versati e agli AIP generati o aggiornati a seguito di tali **versamenti**.

In particolare, sono evidenziati, in tabelle sintetiche complessive o per singola **Struttura**:

- i **versamenti** di SIP svolti con successo, cioè che hanno generato un *Rapporto di versamento*;
- l'inserimento o meno dei SIP in **Elenchi di versamento**;
- i versamenti rifiutati;
- i tentativi di versamento falliti, che non hanno attivato il processo di acquisizione.

Tali informazioni di monitoraggio sono a disposizione degli utenti degli Enti che dispongono di un profilo adeguato.

Dalle tabelle sintetiche è possibile scendere fino al dettaglio dei singoli versamenti, evidenziando, nel caso dei versamenti rifiutati, opportuni codici d'errore, che consentono agli operatori di individuare le soluzioni necessarie alla risoluzione delle anomalie riscontrate. Le più comuni azioni di risoluzione delle anomalie prevedono:

- Utilizzo di parametri di forzatura dei **versamenti**: nel caso in cui i controlli sulle firme, sui *formati* o sui collegamenti presenti sul SIP non vadano a buon fine e il **versamento** del SIP fallisca, i SIP rifiutati possono essere versati nuovamente in conservazione forzando i controlli precedentemente falliti. Tali forzature, che sono operate dal *Produttore* valorizzando appositi parametri presenti nel SIP, consentono di portare in conservazione i SIP anche in presenza delle anomalie che inizialmente ne avevano pregiudicato l'acquisizione. In questi casi, il Sistema segnala al *Produttore* nell'**Esito versamento** che il SIP è stato acquisito a seguito di forzatura;
- Modifica di dati non corretti presenti nel SIP: nel caso in cui il SIP non superi i controlli a causa di alcuni dati non corretti nel SIP stesso, il *Produttore* provvede alla correzione dei dati indicati e a effettuare nuovamente il **versamento**;
- Modifica delle configurazioni del Sistema: nel caso in cui il **versamento** del SIP non vada a buon fine per la presenza nel SIP stesso di dati non corrispondenti con i valori configurati nel Sistema, ParER può procedere, d'accordo con il *Produttore*, a modificare di conseguenza le configurazioni. Di tale modifica viene data comunicazione al *Produttore* che provvede a inviare nuovamente in conservazione il SIP;
- Versamenti rifiutati e non risolubili: nel caso in cui un **versamento** sia stato rifiutato per la presenza di anomalie che il *Produttore* giudica non risolubili, il **versamento** può essere marcato come non risolubile ed escluso, di conseguenza, da futuri controlli;
- Annullamento di versamenti effettuati: nel caso in cui un **versamento** andato a buon fine sia stato effettuato per errore o contenga degli errori non correggibili altrimenti, il *Produttore* provvede ad annullarlo utilizzando apposite funzionalità del Sistema. Il SIP, e il relativo AIP eventualmente generato, non sono cancellati dal Sistema, ma marcati come Annullati. I SIP e gli AIP annullati sono esclusi dai risultati delle ricerche effettuate sul Sistema, e sono richiamabili solo da utenti appositamente abilitati a farlo.

Il modulo di Monitoraggio, inoltre, fornisce accesso alle statistiche dei sistemi, del Data Base, dei versamenti, ecc., mettendo a disposizione degli operatori report sia sintetici che analitici.

[\[Torna al Sommario\]](#)

7.4.2 Gestione delle anomalie

Le anomalie che possono riscontrarsi nell'operatività del servizio in fase di **versamento** sono gestite in generale secondo lo schema indicato nella tabella seguente.

Tipo anomalia	Descrizione	Modalità di gestione
Mancata risposta al versamento	È il caso in cui l' Unità documentaria viene correttamente versata ma, per vari motivi, la risposta di avvenuta ricezione non perviene al <i>Produttore</i> , che pertanto, può ritenerla erroneamente non versata, oltre a non ricevere il rapporto di versamento.	Il <i>Produttore</i> trasmette nuovamente l'Unità documentaria e il <i>Sistema di conservazione</i> restituisce una risposta di esito negativo che contiene l'indicazione che l' Unità documentaria risulta già versata e il relativo <i>Rapporto di versamento</i> . Tale risposta deve essere usata dal <i>Produttore</i> come attestazione di avvenuto versamento e l' Unità documentaria deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento , ma si presume non si ripresentino a un successivo tentativo di versamento . Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il <i>Sistema di conservazione</i> restituisce un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il versamento viene quindi rifiutato.	Il <i>Produttore</i> deve provvedere a rinviare l' Unità documentaria in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.
Versamenti non conformi alle regole concordate	È il caso in cui il versamento non viene accettato perché non conforme alle regole concordate (formato file non previsto, mancanza di <i>metadati</i> obbligatori, ecc.).	Produttore e ParER concordano una soluzione al problema.
Errori interni o dovuti a casistiche non previste o non gestite	In alcuni casi è possibile che il <i>Sistema di conservazione</i> risponda con un messaggio di errore generico che non indica le cause dell'anomalia	Il <i>Produttore</i> segnala il problema a ParER, che si attiverà per la sua risoluzione.

Tipo anomalia	Descrizione	Modalità di gestione
	riscontrata in quanto dovuta a un errore interno o perché legata a una casistica non prevista, non gestita o non gestibile dal <i>Sistema di conservazione</i> .	
Errori nel contenuto dei dati conservati	È il caso eccezionale in cui per ragioni tecniche il <i>Sistema di conservazione</i> abbia effettuato un errore, che non può essere corretto con le procedure standard, oppure siano stati versati dati errati da parte del <i>Produttore</i> , che, in accordo con il <i>Produttore</i> stesso, si ritiene più semplice correggere per via tecnica, piuttosto che annullare e versare nuovamente	Il <i>Produttore</i> richiede formalmente al personale archivistico di ParER di effettuare una correzione tecnica dei dati; il gruppo di sviluppo e manutenzione viene quindi incaricato ad intervenire manualmente sul database per effettuare la correzione: l'intervento effettuato viene annotato nell'AIP e l'azione manuale effettuata sul database viene tracciata nel log del database; la richiesta di intervento tecnico e la relativa soluzione rimangono tracciate all'interno del sistema di gestione delle attività di sviluppo e manutenzione.

[\[Torna al Sommario\]](#)

7.5 Preparazione e gestione del Pacchetto di archiviazione

Come elemento ulteriore di controllo dei versamenti effettuati, i SIP accettati e presi in carico sono inseriti in appositi **Elenchi di versamento**¹⁷ generati secondo criteri, definiti "criteri di raggruppamento", predefiniti per **tipologia documentaria** e anno di produzione. Normalmente il criterio standard prevede che l'elenco si chiuda al raggiungimento di un numero massimo di componenti (5000) o dopo 30 giorni dall'apertura, ma possono essere variati in base a specifiche esigenze conservative.

L'**Elenco di versamento** è un documento in formato XML, generato alla chiusura dell'elenco e fornito di un *Riferimento temporale* opponibile ai terzi. Riporta per ogni documento o aggregazione versata l'Identificativo univoco, un set di *metadati* descrittivi, le *impronte* degli **Oggetti-dati** che lo compongono e una serie di informazioni sintetiche relative alle verifiche a cui è il SIP è stato sottoposto durante il processo di acquisizione.

L'Elenco è recuperabile dal *Produttore* utilizzando apposite funzionalità dell'interfaccia web del Sistema.

Gli elementi inseriti nell'Elenco possono essere sottoposti a ulteriori controlli, anche a campione, finalizzati a verificare la corrispondenza degli oggetti versati con quanto concordato con il *Produttore* e a evidenziare eventuali anomalie non rilevabili dalle verifiche automatiche al **versamento**.

¹⁷Tali elementi vengono a sostituire le precedenti azioni di creazione volumi effettuate nel rispetto della Delibera CNIPA 11/2004. Gli **Elenchi di versamento** sono prodotti a partire dal 2015 a seguito dell'abbandono definitivo della creazione di volumi precedentemente prevista. Il sistema continua a gestire anche le informazioni relative ai volumi costituiti fino al 2014.

Una volta chiuso l'Elenco di versamento e completati i controlli, l'Elenco viene validato, automaticamente o manualmente dal Responsabile della funzione archivistica di conservazione, eventualmente anche con propria firma digitale.

Tale validazione avvia il processo di creazione dei Pacchetti di Archiviazione (AIP) e dei relativi indici in formato conforme allo standard UNI SinCRO.

I SIP accettati e presi in carico dal Sistema, dopo la validazione dell'**Elenco di versamento** in cui sono stati inseriti, sono soggetti a una fase di elaborazione finalizzata alla creazione dell'AIP (o all'aggiornamento di un AIP esistente).

A seguito di queste elaborazioni, nel caso di **Versamento anticipato**, viene generato (o aggiornato) l'AIP dell'**Unità documentaria**.

L'AIP dell'**Unità documentaria** è composto da:

- l'**Indice dell'AIP**: è un documento in formato XML prodotto in conformità alle specifiche contenute nella struttura dati dell'Allegato 4 delle **Regole tecniche** e descritto in dettaglio del documento "Modelli dei pacchetti di archiviazione" che contiene tutti i *metadati* dell'**Unità documentaria** presenti sul Sistema e i riferimenti agli altri file presenti nel pacchetto. Tra i dati contenuti nell'Indice vi sono:
 - la data di generazione dell'AIP (espressa con un *Riferimento temporale* opponibile ai terzi con le caratteristiche descritte al paragrafo 7.3) che costituisce il *Riferimento temporale* opponibile a terzi di tutti i file elencati nell'Indice stesso;
 - i *metadati* descrittivi dell'**Unità documentaria**;
 - i *metadati* generati dal Sistema nel corso delle verifiche e delle elaborazioni operate sul SIP;
 - le *impronte* dei singoli file (**Oggetti-dati**) dell'AIP stesso;
 - le *impronte* delle eventuali precedenti versioni dell'**Indice dell'AIP** (in caso di aggiornamento);
 - le *impronte* degli altri documenti generati dal Sistema nel *processo di conservazione*;
 - il riferimento agli **Elenchi di versamento** relativi ai SIP da cui è stato generato o aggiornato l'AIP;
- I file (**Oggetti-dati**) dell'**Unità documentaria** ricevuti nel SIP e le eventuali, relative copie informatiche generate dal Sistema;
- I file con le eventuali precedenti versioni dell'**Indice dell'AIP**;
- I file degli **Indici dei SIP** da cui è stato generato o aggiornato l'AIP;
- I file degli **Esiti versamento** relativi ai SIP da cui è stato generato o aggiornato l'AIP;
- I file dei **Rapporti di versamento** relativi ai SIP da cui è stato generato o aggiornato l'AIP.

L'AIP dell'**Unità documentaria** prodotto viene firmato dal Responsabile della funzione di archivistica di conservazione.

La firma degli AIP delle **Unità documentarie** può avvenire in due modi, a seconda che il processo di conservazione si svolga in regime di **versamento anticipato** o in regime di **versamento in archivio**.

Nel primo caso, la firma viene apposta su un'evidenza informatica, denominata Elenco Indici AIP, prodotta a partire dagli **elenchi di versamento** e contenente gli identificativi e l'impronta degli Indici degli AIP di ogni **Unità documentarie** contenuta negli elenchi stessi. Tale evidenza informatica, una volta firmata, è inserita negli AIP delle singole **Unità documentarie**.

Nel caso di **Versamento in archivio**, invece, la firma degli AIP delle **Unità documentarie** avviene attraverso la firma degli AIP delle aggregazioni (**Unità archivistiche** e **Serie**) in cui le **Unità documentarie** sono comprese. Gli Indici di tali AIP contengono, infatti, oltre ai *metadati* descrittivi dell'*Aggregazione documentale informatica*, le *impronte* degli Indici degli AIP delle **Unità documentarie** e/o delle **Unità archivistiche** che li compongono.

Gli **Indici dell'AIP** delle **Unità archivistiche** e delle **Serie** sono firmati dal Responsabile della funzione archivistica di conservazione ad attestare il corretto svolgimento del processo di **Versamento in archivio** che completa il processo di trasferimento al Sistema dal punto di vista del *Produttore*.

Con la firma dell'AIP dell'*Aggregazione documentale informatica* si determina anche l'accettazione della custodia da parte di ParER dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* versate, cioè la dichiarazione che tutte le **Unità documentarie** relative all'*Aggregazione documentale informatica* sono correttamente acquisite e conservate dal Sistema nell'*archivio*.

Contestualmente alla generazione degli AIP, il Sistema memorizza le **Informazioni descrittive** sul *Pacchetto di archiviazione*, ovvero un set di *metadati* derivato da quello presente nell'**Indice dell'AIP** ed eventualmente da altri documenti contenuti nell'AIP stesso, finalizzato a ricercare gli AIP conservati nel Sistema.

Gli AIP sono conservati nel Sistema per il tempo di conservazione previsto dalle norme; allo scadere del tempo di conservazione possono essere scartati con le procedure descritte nel paragrafo 7.8.

Il *Produttore* può accedere agli AIP conservati utilizzando le apposite funzionalità dell'interfaccia web del Sistema o chiamando l'apposito servizio con le modalità descritte nel documento "Specifiche tecniche dei servizi di recupero".

L'aggiornamento degli AIP può essere originato da due eventi: versamento di un SIP da parte del *Produttore* e attivazione di procedure di conservazione da parte del Sistema.

Nel primo caso l'aggiornamento dell'AIP viene innescato dal *Produttore* che può inviare ulteriori SIP per integrare o aggiornare le informazioni e/o altri elementi presenti nell'AIP secondo le modalità descritte nel documento Specifiche tecniche dei servizi di versamento. Nel secondo caso, invece, gli aggiornamenti derivanti dalle procedure di conservazione sono innescati dal Sistema al verificarsi di determinati eventi e sono finalizzati a mantenere la *leggibilità* e la reperibilità nel tempo degli AIP.

Infine, gli AIP in casi eccezionali possono essere sottoposti a procedure di sequestro e di eventuale annullamento. Le procedure da applicare in questi casi sono descritte operativamente in specifici documenti tecnici.

Le politiche di conservazione dei pacchetti di archiviazione (AIP), per assicurare sia il contenuto dell'informazione all'ente produttore sia l'integrità nel tempo dei pacchetti conservati sono descritte al capitolo 9.2. Inoltre, con periodicità quadrimestrale, viene verificato che il totale dei

componenti versati con i SIP corrisponda alla somma dei componenti presenti negli AIP, di quelli in lavorazione e di quelli in attesa di lavorazione, al netto dei componenti contenuti in versamenti annullati.

[\[Torna al Sommario\]](#)

7.6 Preparazione e gestione del Pacchetto di distribuzione (DIP) ai fini dell'esibizione

I DIP sono prodotti di norma a partire dagli AIP presenti sul Sistema. Nel caso in cui non sia stato ancora generato l'AIP è comunque possibile produrre DIP, riferiti agli oggetti versati e ai documenti di conservazione già prodotti.

Esistono varie tipologie di DIP, ognuno corrispondente alle specifiche esigenze di utilizzo da parte degli *Utenti* (**Comunità di riferimento**).

In base alla tipologia di DIP e alle sue specifiche esigenze di utilizzo, il Sistema mette a disposizione funzionalità per la sua produzione e distribuzione, sia automatiche che manuali.

Il Sistema fornisce le seguenti tipologie di DIP:

- DIP coincidente con l'AIP: contiene tutti gli elementi presenti nell'AIP (vedi anche paragrafo 7.9) ed è scaricabile dall'interfaccia web del Sistema o tramite appositi servizi descritti nel documento Specifiche tecniche dei servizi di recupero;
- DIP coincidente con il SIP: contiene gli Oggetti-dati presenti, l'**Indice del SIP** e l'**Esito versamento** ed è scaricabile dall'interfaccia web del Sistema;
- DIP del *Rapporto di versamento*: contiene i *Rapporti di versamento* relativi all'**Unità documentaria** ed è scaricabile dall'interfaccia web del Sistema o tramite appositi servizi descritti nel documento "Specifiche tecniche dei servizi di recupero";
- DIP dei documenti di conservazione: contiene i documenti di conservazione prodotti nel corso del processo di conservazione (**Indice del SIP**, PI SIP, **Esito versamento**, *Rapporto di versamento*) ed è scaricabile dall'interfaccia del Sistema;
- DIP dell'**Unità documentaria**: contiene esclusivamente gli **Oggetti-dati** che la compongono ed è scaricabile dall'interfaccia web del Sistema;
- DIP del **Documento**: contiene esclusivamente gli **Oggetti-dati** del **Documento** ed è scaricabile dall'interfaccia web del Sistema;
- DIP del **Componente**: contiene il singolo file del **Componente** ed è scaricabile dall'interfaccia web del Sistema;
- DIP dell'**Elenco di versamento**: contiene l'**Elenco di versamento** in cui è contenuta l'**Unità documentaria** ed è scaricabile dall'interfaccia web del Sistema;
- DIP per l'esibizione: contiene i file dell'**Unità documentaria** e una dichiarazione, sotto forma di file in formato testo, che illustra il contenuto del DIP e fornisce informazioni utili ad agevolarne l'esibizione.

La distribuzione dei pacchetti a fine di *esibizione* avviene utilizzando apposite funzionalità dell'interfaccia web del Sistema, oppure chiamando l'apposito servizio descritto nel documento "Specifiche tecniche dei servizi di recupero".

Normalmente i DIP sono trasmessi o resi disponibili al *Produttore*, che poi provvede a consegnarli agli interessati. La consegna o la messa a disposizione dei DIP direttamente agli interessati è possibile solo con specifico accordo tra *Produttore* e ParER.

Il *Produttore* può consultare quanto versato in ParER tramite interfaccia web, collegandosi all'indirizzo comunicato da ParER e autenticandosi tramite username e password preventivamente forniti da ParER.

Gli operatori da abilitare per l'accesso tramite interfaccia web al *Sistema di conservazione* sono comunicati formalmente dal *Produttore* a ParER, che provvede fornire le credenziali di accesso ai diretti interessati.

L'accesso web consente al *Produttore* di ricercare i documenti e le aggregazioni versati, di effettuarne il download e di acquisire le evidenze delle attività di conservazione.

[\[Torna al Sommario\]](#)

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

La produzione di duplicati informatici o copie informatiche dei *Documenti informatici* conservati nel Sistema avviene mediante la messa a disposizione del *Produttore* di DIP comprensivi degli **Oggetti-dati** che li compongono.

Tali pacchetti sono acquisibili dagli *Utenti* utilizzando specifiche funzionalità dell'interfaccia web del Sistema o utilizzando gli appositi servizi descritti nel documento "Specifiche tecniche dei servizi di recupero".

Non è previsto da parte di ParER né il rilascio di copie cartacee conformi agli originali digitali conservati, né l'accesso diretto alla documentazione da parte di colui che, dovendo tutelare situazioni giuridicamente rilevanti, abbia presentato istanza di consultazione.

Pertanto, in merito all'esercizio del diritto d'accesso ai documenti conservati da ParER, questo si limita a fornire al *Produttore*, su precisa richiesta di quest'ultimo e senza che su di esso debba gravare alcun particolare onere, il documento informatico conservato, qualora per un qualsiasi motivo il *Produttore* stesso abbia deciso di non acquisirlo direttamente mediante le modalità descritte nel paragrafo 7.6.

Permane in carico al *Produttore* sia la responsabilità di valutare la fondatezza giuridica della domanda di accesso, sia l'onere di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente.

ParER provvederà a consegnare direttamente la documentazione richiesta solo nel caso di visite ispettive presso ParER o provvedimenti di esibizione o sequestro da parte dell'autorità giudiziaria o di altra autorità ispettiva espressamente indirizzati al soggetto conservatore.

Nei casi previsti dalla normativa, il ruolo di pubblico ufficiale è svolto dal Responsabile del servizio ParER in qualità di dirigente dell'ufficio responsabile della conservazione dei documenti, o da altri dallo stesso formalmente designati, quale il Responsabile della Funzione archivistica di conservazione per l'attestazione di conformità all'originale di copie di *Documenti informatici* conservati.

Il ruolo di pubblico ufficiale, per i casi in cui è previsto l'intervento di soggetto diverso della stessa amministrazione, sarà svolto da altro dirigente all'uopo individuato o da altro soggetto da quest'ultimo designato.

[\[Torna al Sommario\]](#)

7.8 Scarto dei pacchetti di archiviazione

Il Produttore, in base ai tempi di conservazione risultanti dai propri **Massimari di scarto** invia a ParER un Elenco di scarto, in cui sono indicate le **Unità archivistiche** o le **Unità documentarie** da sottoporre a procedura di *scarto*.

Tale Elenco di scarto, viene verificato da parte di ParER ed eventualmente adeguato in modo da poter essere utilizzato nel Sistema. L'elenco, se modificato, viene trasmesso al *Produttore* che può rifiutarlo indicandone i motivi (innescando in tal modo una nuova verifica da parte di ParER) o accettato. e trasmesso dal *Produttore* all'Autorità di vigilanza che, in base alle norme vigenti, deve fornire il nulla-osta per lo *scarto*.

Il *Produttore*, una volta ricevuto il nulla-osta (che può essere concesso anche solo su una parte dell'Elenco proposto), provvede ad adeguare, se necessario, l'*Elenco di scarto* presente sul Sistema alle decisioni dell'Autorità. Una volta che l'*Elenco di scarto* definitivo viene predisposto, il *Produttore* lo valida e trasmette a ParER la richiesta di procedere allo *scarto*.

ParER effettua un ulteriore controllo sulla congruenza dell'*Elenco di scarto* definitivo con quello autorizzato dall'autorità e, in caso riscontrasse anomalie, provvede alla correzione e sottopone nuovamente l'Elenco alla validazione del *Produttore*.

Nel caso in cui il controllo sull'*Elenco di scarto* dia esito positivo, ParER procede alla cancellazione degli AIP contenuti nell'Elenco. Al termine delle operazioni viene data comunicazione al Produttore dell'avvenuto scarto, fornendo nella stessa tutti gli elementi utili a ricostruire l'intero processo.

[\[Torna al Sommario\]](#)

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

La **Convenzione** prevede che, in caso di recesso o a scadenza di contratto, l'IBACN, tramite il ParER, è tenuto a riversare i *Documenti informatici* e le *Aggregazioni documentali informatiche* conservate, i *metadati* a essi associati e le *evidenze informatiche* generate nel corso del *processo di conservazione* nel sistema indicato dal *Produttore*, secondo modalità e tempi indicati nel **Disciplinare Tecnico**.

ParER garantisce comunque il mantenimento nel proprio *Sistema di conservazione* dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* conservati, con i *metadati* a essi

associati e le *evidenze informatiche* generate nel corso del *processo di conservazione* fino alla comunicazione da parte del *Produttore* dell'effettiva messa a disposizione del *Sistema di conservazione* in cui effettuare il riversamento.

ParER provvederà all'eliminazione dal proprio *Sistema di conservazione* di tutti gli oggetti riversati e di tutti gli elementi riferiti al *Produttore* solo al termine del riversamento e solo dopo le opportune verifiche - effettuate da entrambe le Parti e svolte di concerto tra le stesse - di corretto svolgimento del riversamento stesso.

In tal caso viene garantita la cancellazione e non leggibilità dei dati entro 90 giorni sia dal sistema primario (compresi i backup), sia dal sito di ***business continuity***, sia dal sito di ***Disaster recovery***.

L'intera operazione dovrà comunque avvenire con l'autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MIBACT.

In caso di chiusura del servizio da parte della Regione Emilia-Romagna, con interventi di modifica alla normativa regionale, si provvederà a trasferire quanto conservato ai *Sistemi di conservazione* individuati per proseguire le attività svolte da IBACN e a cancellarlo da tutti i sistemi comprendendo le copie di backup, fornendo evidenze del trasferimento all'Ente Produttore.

Per quanto riguarda gli aspetti operativi per il trasferimento di *archivi* ad altri *sistemi di conservazione*, ParER adotta lo standard Uni Sincro, e provvede a mettere a disposizione l'*archivio* del *Produttore* in un'area a lui dedicata, da cui potrà prelevare utilizzando un canale sicuro di trasferimento (***FTPS***). Analogamente il Sistema è predisposto per la ricezione di *archivi* in formato Uni Sincro; qualora il precedente Conservatore non sia in grado di produrre l'*archivio* in formato Uni Sincro, ParER, a seguito di specifici accordi, può mettere a disposizione del *Produttore* consulenza e strumenti per facilitarne il trasferimento.

[\[Torna al Sommario\]](#)

8 IL SISTEMA DI CONSERVAZIONE

8.1 Componenti logiche

Il diagramma in figura, realizzato sul modello della rappresentazione delle entità funzionali di **OAIS**, schematizza dal punto di vista logico le principali componenti del *Sistema di conservazione* di ParER e le principali relazioni con i soggetti interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

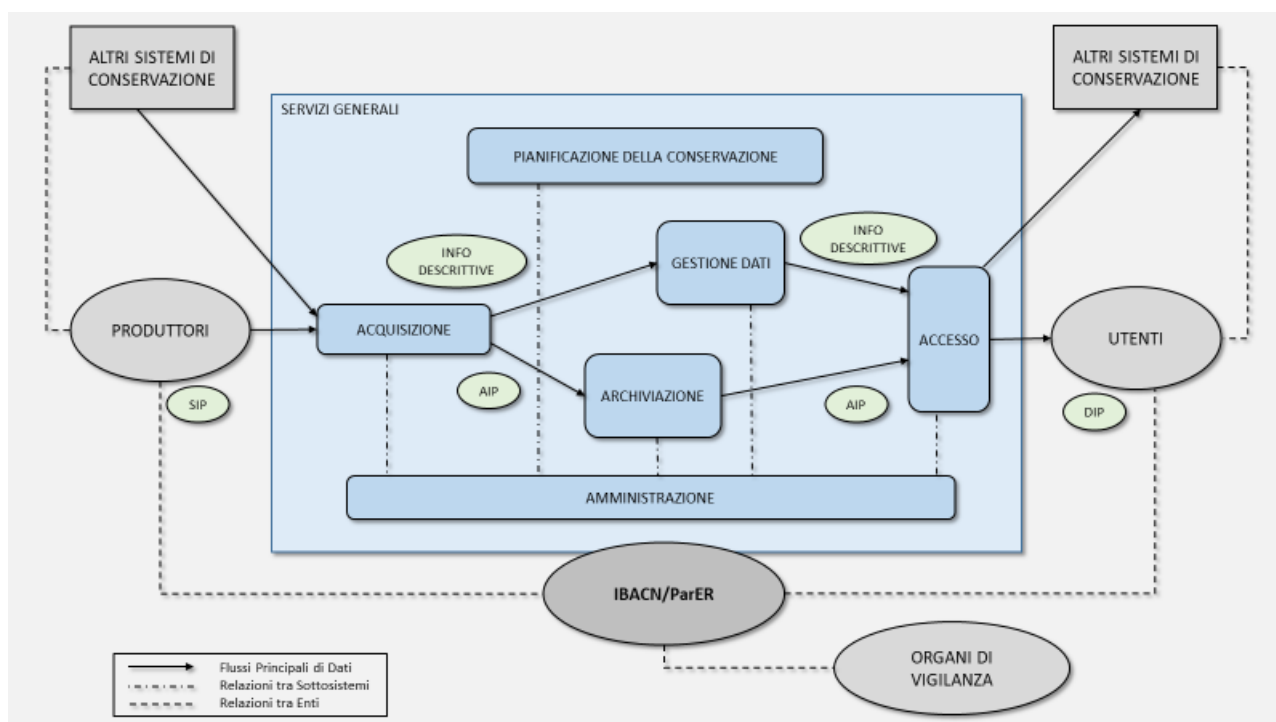


Figura 7 - Schema logico del Sistema di conservazione

Per la descrizione dei ruoli di *Produttori*, *Utenti*, IBACN/ParER, come soggetto Conservatore e Amministratore del Sistema, e Organi di vigilanza si rimanda al capitolo 4 del presente Manuale.

In ottica di *interoperabilità* ParER è in grado di ricevere da altri *sistemi di conservazione* documenti già sottoposti a conservazione, e di versarli ad altri Sistemi secondo gli accordi intercorsi con il *Produttore*.

Le funzionalità di Acquisizione gestiscono la fase di Acquisizione e *presa in carico* del *processo di conservazione* (vedi paragrafi 7.1 – 7.4), ovvero, attraverso i **Web Service** di versamento esposti dal Sistema, consentono la ricezione dei SIP dei *Produttori*, la loro verifica e la generazione, a partire dai SIP, dei relativi AIP e delle **Informazioni descrittive** per la loro ricerca.

Le funzionalità di Gestione Dati gestiscono le **Informazioni descrittive** generate al termine della fase di acquisizione e *presa in carico* del *processo di conservazione*. Tali funzionalità garantiscono: *memorizzazione*, manutenzione e aggiornamento all'interno del Sistema sia delle

Informazioni descrittive necessarie a ricercare gli AIP, ricevute dall'Acquisizione, che dei dati necessari per gestire i pacchetti.

Le funzionalità di Archiviazione gestiscono la fase di gestione degli AIP del *processo di conservazione* (vedi paragrafo 7.5): *memorizzazione*, **migrazione** dei supporti, backup, **Disaster recovery** ed eliminazione (*scarto*) degli AIP conservati nel Sistema.

Le funzionalità di Amministrazione gestiscono il governo dell'intero *processo di conservazione*, permettendo di definire e aggiornare nel Sistema politiche, standard e configurazioni che regolano tutte le altre funzionalità, incluse la gestione degli accordi con i *Produttori*, il monitoraggio del Sistema, la produzione di copie informatiche per la conservazione (**migrazione** dei *formati*) e la selezione degli AIP per lo *scarto*.

Le funzionalità di Pianificazione della conservazione gestiscono il monitoraggio dell'ambiente in cui il Sistema è inserito e forniscono le indicazioni necessarie per fare in modo che le informazioni conservate restino fruibili nel lungo periodo tenendo conto dell'evoluzione tecnologica dei sistemi e del cambiamento della **Comunità di riferimento** (*Utenti*). Intervengono nella progettazione dei *Pacchetti Informativi* e nella pianificazione dello sviluppo e dei test del software necessario per la **migrazione** degli AIP. Tale funzione non è svolta da uno specifico applicativo, né segue procedure meccaniche, configurandosi invece come una serie di attività svolte utilizzando un insieme di strumenti, non solo informatici, finalizzati a raccogliere informazioni, confrontarsi con la **Comunità di riferimento**, effettuare test e verifiche sugli oggetti conservati, il tutto finalizzato a fornire indicazioni utili a mantenere il *processo di conservazione* aggiornato in relazione sia all'evoluzione tecnologica, che alle esigenze della **Comunità di riferimento**.

I risultati di questa analisi si concretizzano, tipicamente ma non esclusivamente, in aggiornamenti nei modelli di *pacchetti informativi* gestiti dal Sistema, in implementazione di nuove librerie o altri strumenti software utilizzati dal Sistema, nella definizione e nell'aggiornamento delle politiche di conservazione, nei test su nuovi componenti hardware, e in altro ancora.

Normalmente questi elementi sono inseriti nel Sistema utilizzando principalmente le funzionalità di Amministrazione di SacER e, secondariamente, quelle analoghe presenti negli altri moduli del Sistema, garantendo che il *processo di conservazione* sia sempre in grado tanto di contrastare efficacemente l'obsolescenza tecnologica, quanto di rispondere adeguatamente alle esigenze della **Comunità di riferimento** di ParER.

Le funzionalità di *accesso* gestiscono la fase di gestione del DIP del *processo di conservazione* (vedi paragrafo 7.6): supporto agli operatori per la ricerca e la restituzione degli oggetti conservati. Le funzioni di *interoperabilità* consentono inoltre la restituzione da parte del Sistema di DIP coincidenti con gli AIP conformi a quanto previsto dagli allegati 3 e 4 delle **Regole tecniche**.

Il diagramma in figura schematizza i principali flussi di dati che intercorrono tra le componenti logiche del sistema descritte nei paragrafi precedenti; per completezza nello schema è stata inserita anche la componente '**Disaster recovery**', in quanto, pur non avendo un ruolo rilevante nella gestione ordinaria, riveste un ruolo significativo nello scambio di flussi informativi e svolge funzionalità elaborative autonome, seppur limitate, ai fini della produzione delle copie di salvataggio dei file su cassetta.

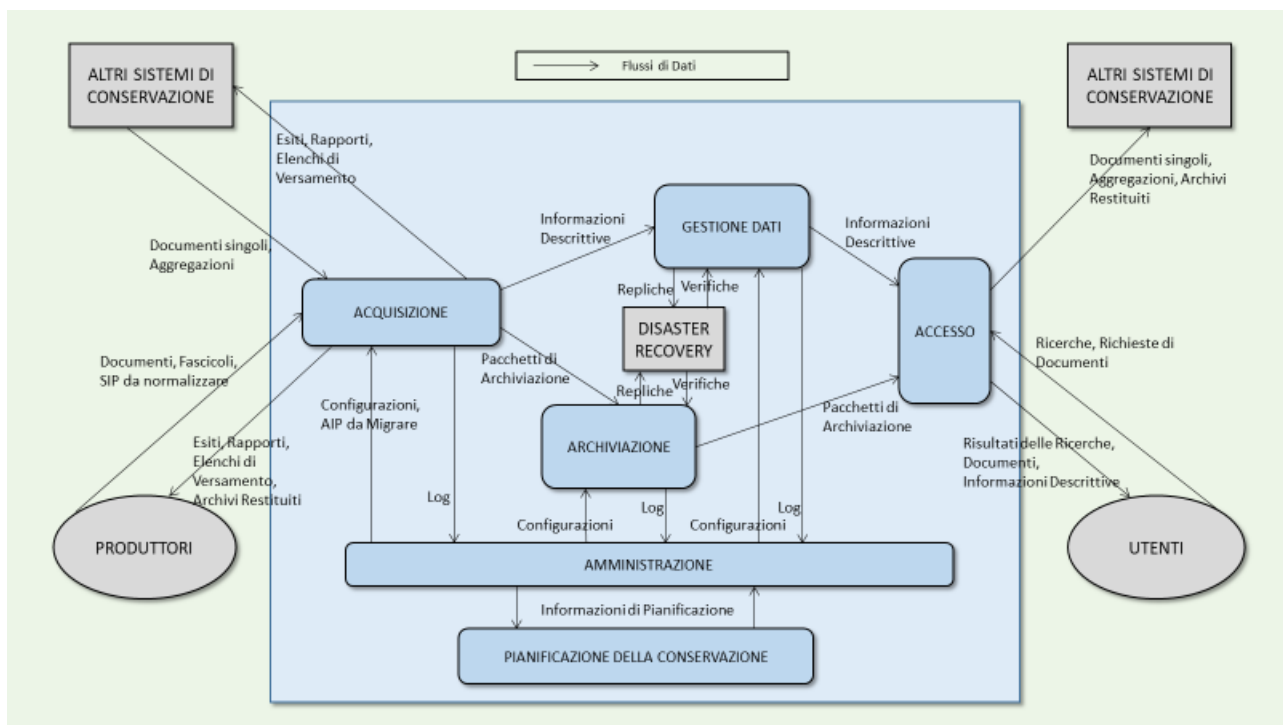


Figura 8 - Flussi di dati nel Sistema di conservazione

Il Servizio di conservazione è supportato da un unico Sistema integrato, suddiviso logicamente in sistemi dedicati agli specifici conservatori (ambienti). Nell'ambito del Sistema gli archivi di ogni Ente *Produttore* sono allocati in aree logicamente separate (strutture). Gli accessi degli utenti sono limitati alle strutture per i quali sono stati profilati in modo tale che gli archivi di ogni Ente risultano adeguatamente protetti.

In aggiunta alle componenti logiche delineate nei paragrafi precedenti, che ne costituiscono il nucleo centrale, il Sistema mette a disposizione diversi Servizi generali a supporto delle altre funzionalità. Oltre ai servizi di gestione e monitoraggio dei sistemi, della rete, e della sicurezza dei sistemi, mette a disposizione in particolare:

- il servizio di **Identity Management**, che, via *IDP*, garantisce i corretti accessi al Sistema da parte dei diversi utilizzatori;
- il servizio di Firma tramite dispositivo **HSM**, che consente di apporre le firme digitali necessarie nel processo di conservazione senza utilizzare **applet** di firma all'interno del browser
- il servizio di **Audit e Log**, che mantiene e manda in conservazione la storia degli accessi effettuati al Sistema e ai dati;
- il **Sito Web** di ParER, che fornisce informazioni e documentazioni relative al processo e al *Sistema di conservazione*;
- il Sistema di e-Learning della regione Emilia-Romagna, che nell'area dedicata a ParER mette a disposizione degli utenti corsi di vari livelli sul processo di Conservazione.

[\[Torna al Sommario\]](#)

8.2 Componenti tecnologiche

Il *Sistema di conservazione* è costituito da diversi moduli software che interagiscono tra loro per la gestione dell'intero *processo di conservazione*. Il Sistema, inoltre, si avvale di ulteriori componenti applicative esterne con funzioni di supporto al processo.

Il diagramma in figura schematizza dal punto di vista tecnologico le principali componenti del *Sistema di conservazione* di ParER e le principali relazioni con altri sistemi interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

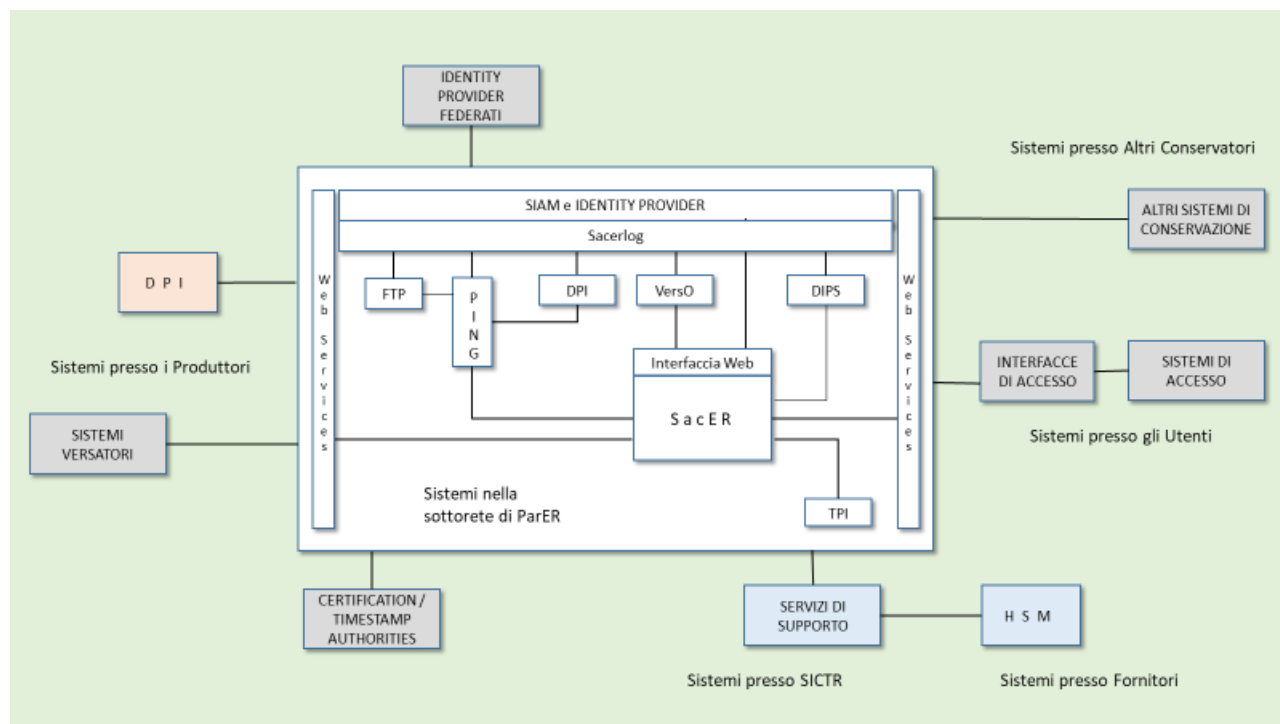


Figura 9 - Schema Tecnologico del Sistema di conservazione

Nella figura sono riportate:

- in bianco le componenti del *Sistema di conservazione* interne al perimetro di sicurezza del data center di ParER;
- in rosa le componenti del *Sistema di conservazione* sviluppate da ParER, ma esterne al perimetro di sicurezza del data center di ParER, in quanto installate nelle reti dei *Produttori*;
- in azzurro le componenti a supporto del Sistema gestite da ParER direttamente o tramite il **SICTR** della Regione Emilia-Romagna;
- in grigio le componenti che fanno riferimento ai soggetti esterni (*Produttori, Utenti e Authorities*).

Qui di seguito sono illustrati i singoli moduli software del Sistema e le componenti di supporto.

[\[Torna al Sommario\]](#)

8.2.1 SacER

Il modulo software SacER costituisce il nucleo centrale del Sistema e implementa le funzionalità principali del *processo di conservazione*, quali:

- Acquisizione SIP;
- Archiviazione;
- Gestione dati;
- Amministrazione;
- Accesso.

Le funzionalità di Acquisizione SIP di SacER consentono la gestione delle varie fasi del processo di Acquisizione e *presa in carico* (vedi paragrafi 7.1 – 7.4). Operativamente si compongono delle seguenti attività:

- acquisizione del SIP trasmesso attraverso i Servizi di versamento
- **memorizzazione** del SIP in un'area temporanea logicamente distinta dall'*archivio* vero e proprio per effettuare le verifiche previste;
- verifica del SIP in relazione alla struttura dati, ai *metadati* degli oggetti sottoposti a conservazione, alle eventuali firme apposte sui file (**Oggetti-dati**) associati ai **Componenti**, ai *formati* dei file stessi e generazione del *Rapporto di versamento* in caso di verifica positiva;
- restituzione dell'**Esito versamento**, comprensivo, in caso di esito positivo, del *Rapporto di versamento*;
- creazione degli **Elenchi di versamento**: un primo job provvede all'individuazione dei SIP da inserire negli Elenchi secondo i criteri di raggruppamento definiti da ParER; un secondo job genera gli Elenchi e vi appone un *Riferimento temporale* opponibile a terzi; un terzo job esegue i controlli finali e chiude l'Elenco per la sottoscrizione a cura del Responsabile della funzione archivistica di conservazione. Tutti i job sono eseguiti sugli Application server automaticamente ed in modo ricorrente secondo intervalli di tempo stabiliti nel modulo Amministrazione;
- eventuale migrazione di **formato** degli **Oggetti-dati** contenuti nei SIP sia per contrastarne l'obsolescenza tecnologica, sia per esigenze di miglioramento della fruibilità degli oggetti conservati;
- estrazione dei metadati dal SIP (ed eventuale loro normalizzazione) e dal Sistema da utilizzare per completare le informazioni necessarie a generare l'AIP (**Informazioni sulla rappresentazione, Informazioni sulla conservazione, Informazioni sull'impackettamento, Informazioni descrittive**);
- generazione dell'**Indice dell'AIP**, utilizzando i metadati estratti dal SIP e quelli generati dal Sistema nel corso del processo di conservazione. SacER produce report di eccezioni a fronte di situazioni anomale nella creazione dell'**Indice dell'AIP**. Tutte le azioni vengono registrate sul sistema in apposite tabelle di log;
- generazione dell'AIP, che avviene impacchettando in un oggetto auto-consistente l'Indice AIP, le evidenze informatiche prodotte nel corso del processo di conservazione e gli Oggetti-dati.

Le funzionalità di Archiviazione di SacER gestiscono la parte del processo di Gestione dell'AIP relativa alla *memorizzazione* e verifica degli **Oggetti-dati** su Data Base Oracle e **file system** (vedi paragrafo 7.5) e comprendono:

- la **memorizzazione** degli AIP e l'organizzazione gerarchica dei supporti di memorizzazione. In particolare, gli **Oggetti-dati** degli AIP, costituiti dagli Indici degli AIP e dei SIP, dagli **Esiti versamento**, dai *Rapporti di versamento* e dai file associati ai **Componenti**, sono memorizzati su supporti di diverso tipo in ragione della loro dimensione e della frequenza con cui vengono ricercati:

- gli **Oggetti-dati** di piccole dimensioni e ad accesso più frequente vengono salvati temporaneamente all'interno del Data Base in opportune tabelle di **BLOB** per poi essere memorizzati in modo permanente nell'**object storage**, utilizzando a questo scopo appositi job periodici, descritti più avanti
- gli **Oggetti-dati** di grande dimensione e di accesso meno frequente vengono salvati temporaneamente su **file system** in cartelle opportunamente strutturate per poi essere memorizzati in modo permanente su supporti a cassette, utilizzando a questo scopo un apposito componente software chiamato TPI, descritto più avanti;
- il controllo dell'integrità degli oggetti conservati, comprensivo della copia degli archivi, del controllo degli errori e delle procedure di refreshing dei supporti, come descritto nel paragrafo 9.2 e in conformità al Piano di Sicurezza;
- la restituzione dei pacchetti alle funzioni di Accesso, mediante opportune funzionalità dell'interfaccia web del Sistema o mediante l'utilizzo di Servizi di recupero;
- la cancellazione degli AIP sottoposti a scarto a seguito della procedura descritta nel paragrafo 7.8.

Le funzionalità di Gestione Dati di SacER sono finalizzate principalmente a gestire le **Informazioni descrittive** degli AIP generate durante il processo di acquisizione (vedi paragrafo 7.5) e includono:

- la **memorizzazione** dei *metadati* estratti dal SIP o generati dal Sistema nel corso del processo di Acquisizione SIP;
- la gestione degli aggiornamenti dei dati generati dalle funzionalità di Amministrazione e nel corso del *processo di conservazione*;
- l'esecuzione delle ricerche e la sua restituzione alle funzionalità di Accesso, che avvengono mediante l'utilizzo di funzionalità da interfaccia web del Sistema o mediante chiamata a Servizi specifici.

Le funzionalità di Amministrazione di SacER consentono di gestire configurazioni e parametrizzazioni in grado di determinare il funzionamento del Sistema in funzione degli specifici accordi intercorsi con i *Produttori*, definite nel **Disciplinare tecnico** e in funzione delle policy determinate nell'ambito della Pianificazione della conservazione (come descritto più avanti). Inoltre consentono di monitorare tutta l'attività svolta da SacER, così come descritto nel paragrafo 7.4.1. In particolare, in SacER è possibile configurare tutte le entità significative: Enti, **Strutture**, operatori e relativi profili, **tipologie documentarie**, **formati** accettati, logiche di controllo dei versamenti, logiche di creazione delle **Serie**, regole di *accesso* e di esibizione, politiche di monitoraggio del sistema. Anche l'interfaccia web di SacER è configurata automaticamente in ragione del profilo dei singoli operatori che vi accedono.

Le funzionalità di Amministrazione sono costituite da transazioni eseguibili tramite l'interfaccia web del sistema e riservate agli operatori di ParER, ma visibili negli esiti anche agli operatori dei *Produttori*.

Le funzionalità di Accesso di SacER consentono di restituire in forma di DIP gli oggetti conservati. A tal fine SacER mette a disposizione un'interfaccia web per le ricerche e per l'estrazione manuale dei documenti, e dei Servizi di recupero per l'estrazione automatica.

Gli AIP forniti sono trasformati in DIP sulla base delle caratteristiche dell'oggetto e degli utilizzi cui è destinato. In molti casi la trasformazione dell'AIP in DIP può richiedere specifici passi elaborativi e trasformazioni complesse che, necessitando di elaborazioni onerose, vengono normalmente eseguite da opportuni job batch e mantenute in modo permanente sul Data Base.

Secondo la natura dei DIP, l'*esibizione* può avvenire on-line, tramite download, oppure tramite il trasferimento in un'area di transito, da cui il successivo recupero viene effettuato dal sistema richiedente con chiamata FTP. In molti casi, per comodità di trasferimento e recupero i vari elementi che costituiscono il DIP vengono compressi in un archivio di tipo ZIP.

Il modulo di Accesso, oltre a verificare tramite i servizi di Autenticazione l'abilitazione dell'*Utente* al recupero del documento, traccia in apposite tabelle di log tutte le richieste prevenute, qualunque ne sia stato l'esito.

[\[Torna al Sommario\]](#)

8.2.2 VersO

Il client di versamento manuale VersO (Versamento Online) è un modulo che ParER mette a disposizione degli Enti produttori. Utilizza un'interfaccia web e quindi non richiede l'installazione di alcun software sulla stazione di lavoro del *Produttore*.

Il suo utilizzo tipico è per il **versamento** di **Unità documentarie** per le quali non esiste un sistema interfacciato con Sacer. VersO viene richiamato tramite interfaccia web, si autentica sull'**IdP** di ParER o su un **IdP** federato, utilizzando in ogni caso logiche di profilazione del Sistema, ed effettua il **versamento** dei SIP tramite interazione guidata con l'operatore del *Produttore*.

Tale modulo semplifica le operazioni di **versamento** manuale da parte del *Produttore*, automatizzando la generazione dell'**Indice del SIP** ed effettuando un test completo della correttezza del versamento prima di eseguire il versamento stesso. Inoltre, mantiene il log dei versamenti effettuati e consente di interrompere temporaneamente l'operazione (p.e per raccogliere informazioni necessarie per completarlo) riprendendola successivamente, indipendentemente dalla scadenza della sessione web.

[\[Torna al Sommario\]](#)

8.2.3 PING

Il modulo software PING (PreINGest) gestisce il processo di preacquisizione nel caso di **versamento** di Oggetti da trasformare in SIP (vedi paragrafo 7.1.1).

La trasmissione dei pacchetti, solitamente compressi, avviene tramite protocollo FTPS; l'**FTP server** provvede a memorizzare i file ricevuti sullo **storage** dedicato allo spazio FTP di input.

Una volta ricevuti gli Oggetti, un job schedulato provvede alla loro elaborazione per la produzione dei SIP da versare. Un ulteriore job schedulato si occupa di effettuare il **versamento** a SacER, che avviene utilizzando un apposito servizio di versamento. Tale servizio accetta in chiamata due file XML, uno con l'**Indice del SIP** e un altro con le **Informazioni sull'impacchettamento**, relative alla posizione dei file del SIP memorizzati sullo spazio FTP di input.

SacER utilizza le **Informazioni sull'impacchettamento** per recuperare i file dal **file system** di PING e depositarli nel proprio per le successive elaborazioni.

Le successive elaborazioni vengono eseguite da PING direttamente, nel caso in cui la normalizzazione richieda regole precodificate (come p.e. nel caso delle immagini diagnostiche in formato Dicom), oppure utilizzando un motore ETL di esecuzione delle trasformazioni nel caso in cui si debbano applicare regole di trasformazioni specifiche dell'oggetto in questione. In questo

caso le regole sono state definite durante nella fase di avvio del servizio, tramite uno strumento visuale ed eventuali integrazioni di codice sviluppato ad hoc.

PING traccia e memorizza nel proprio Data Base gli esiti dei versamenti a SacER e può essere interrogato per conoscere a quale punto del processo è giunto il SIP da un operatore tramite interfaccia web o dal sistema versante tramite opportuno **Web Service**.

PING mette inoltre a disposizione del *Produttore* un client di versamento di Oggetti da trasformare, sia on line, sia tramite l'utilizzo di un client **FTP** installato sulla postazione di lavoro dell'utente o su un server della rete del *Produttore*.

[\[Torna al Sommario\]](#)

8.2.4 DPI

Il modulo software DPI (Digital Preservation Interface), sviluppato e mantenuto da ParER, consiste in un sistema di interfaccia tra i sistemi dell'Ente produttore e PING, installato all'interno della rete dell'Ente stesso e gestito secondo le politiche di sicurezza dell'Ente, potendo tra l'altro autenticarsi sul suo **IdP**.

DPI implementa funzionalità di **versamento** per specifiche tipologie di SIP. In particolare, qualificandosi come nodo **DICOM**, DPI riceve dai **PACS** studi diagnostici, che poi trasmette a PING per la trasformazione e il **versamento** a SacER.

DPI può operare con logiche sia push che pull, ricevendo o estraendo dati e documenti dai sistemi del *Produttore* per poi versarli nel Sistema, richiamando gli opportuni servizi di PING.

Inoltre, DPI fornisce strumenti di monitoraggio dei versamenti effettuati a disposizione dell'Ente produttore.

[\[Torna al Sommario\]](#)

8.2.5 Interfacce di Acquisizione e di Recupero (Web Service)

I sistemi che debbono versare a SacER documenti o aggregazioni e ottenerne l'esibizione colloquiano con SacER tramite opportuni **Web Service**, che sono definiti nei documenti "Specifiche tecniche dei servizi di versamento" e "Specifiche tecniche dei servizi di recupero". Tali servizi sono invocati anche dai componenti di versamento sviluppati da ParER (DPI, VersO), oltre che dai sistemi di versamento dei *Produttori*.

Nel processo di preacquisizione il client versante (p.e. DPI) utilizza **Web Service** per coordinare il processo con il modulo PING, ma trasmette gli oggetti da conservare tramite protocollo FTPS, su un'opportuna area FTP, gestita dal server FTP di ParER. Fa eccezione il client interno a PING, che può versare anche on line, senza appoggiarsi su protocollo FTP.

[\[Torna al Sommario\]](#)

8.2.6 TPI

Il modulo software TPI (Tivoli Preservation Interface) gestisce la *memorizzazione* degli **Oggetti-dati** su supporti a cassette, operata utilizzando come sistema di gestione della **tape library** il software Tivoli.

In particolare, TPI opera nel seguente modo:

- un job schedulato sul file server invia al sistema di gestione della **tape library** il comando di archiviazione delle cartelle in cui SacER ha depositato gli oggetti da archiviare, selezionate tramite opportuni criteri definiti in sede di amministrazione di sistema;
- il sistema di gestione della **tape library** provvede a leggere i file dalle cartelle e ad archivarli tramite le sue funzionalità di archiving nella **tape library**, dove rimangono in situazione **near-line**, cioè disponibili e raggiungibili nella **tape library**, senza necessità di reperire cassette da un magazzino;
- una volta archiviati, TPI provvede a cancellare i file dal **file system** su disco;
- l'allineamento tra sito primario e sito di **Disaster recovery** viene garantito da un job periodico schedulato sul file server del sito primario che aggiorna automaticamente il **file system** del sito secondario. Il job invia al sito secondario i nuovi file pervenuti nel **file system**, senza replicare le cancellazioni effettuate in seguito all'archiviazione su cassetta;
- sul sito di **Disaster recovery**, in maniera indipendente da quanto avviene sul sito primario, ma con politiche analoghe, viene eseguito un job di archiviazione analogo a quello del sito primario, mantenendo così l'indipendenza tra i due siti per quanto riguarda l'archiviazione.

Le funzionalità di Archiviazione di SacER verificano lo stato degli Oggetti-dati nei due siti e lo registrano sul Data Base Oracle.

Presso il sito di **Disaster recovery** viene prodotta una seconda copia per ogni cassetta.

Le attività di gestione del sito secondario sono tracciate in uno specifico Data Base del sistema di gestione della **tape library**.

[\[Torna al Sommario\]](#)

8.2.7 DIPS

Il modulo software DIPS (DIPSpenser), previo controllo dei diritti di accesso alle informazioni, consente di attivare ricerche sul Sistema e di soddisfare richieste relative agli oggetti conservati, anche quando le funzionalità di ricerca messe a disposizione dall'interfaccia web di SacER non riescono a soddisfare le particolari esigenze dell'utente.

DIPS consente ricerche complesse sugli oggetti conservati sulla base delle **Informazioni descrittive** memorizzate dalle funzionalità di Gestione dati, e di ottenere l'*esibizione* dei documenti individuati dalla ricerca, sfruttando le funzionalità di Accesso di SacER. DIPS opera ricercando gli AIP da esibire, attraverso le **Informazioni descrittive** fornite dalle funzionalità di Gestione dati, e richiedendo gli AIP alle funzionalità di Archiviazione.

Il modulo DIPS consiste di un sistema generalizzato in grado di configurare tramite opportuna parametrizzazione i criteri da utilizzare nella ricerca e la presentazione dei risultati in ragione delle necessità e delle preferenze dei diversi utenti.

[\[Torna al Sommario\]](#)

8.2.8 SIAM

Il modulo software SIAM (SacER Identity and Access Management) consente di gestire l'autenticazione e la profilatura degli operatori. Tale profilatura viene utilizzata da SacER e dagli altri moduli software del Sistema per valutare a quali viste specifiche di dati e a quali attività ogni operatore abbia accesso, sulla base dei ruoli assegnati.

Per le funzionalità di autenticazione SIAM utilizza sistemi di **IdP** (Identity Provider); ParER mette a disposizione un proprio **IdP**, ma può accettare anche l'autenticazione effettuata su altri **IdP** opportunamente federati nel rispetto delle logiche di sicurezza richieste dalle Politiche della Sicurezza di ParER.

SIAM mantiene il Data Base degli operatori dell'**IdP** di ParER, nonché il Data Base dei profili di tutti gli operatori abilitati al Sistema, qualunque sia l'**IdP** su cui si sono autenticati, gestendo quindi in modo centralizzato la profilatura per tutti i moduli del Sistema.

La profilatura si spinge fino al livello delle singole attività previste dal Sistema (p.e. pressione di uno specifico bottone di una specifica videata) ed al livello elementare dei dati gestiti (**Struttura, Unità documentaria**, Registro, ecc.) tramite la definizione e la combinazione di opportuni ruoli. L'**IdP** implementato da ParER colloquia con gli altri moduli del Sistema tramite standard SAML (Security Assertion Markup Language); l'utilizzo di SAML consente al *Sistema di conservazione* di accettare operatori autenticati su altri sistemi federati.

[\[Torna al Sommario\]](#)

8.2.9 Sacerlog

Il modulo Sacerlog raccoglie e conserva nel sistema informazioni essenziali sul processo di conservazione in base al paradigma proposto da PREMIS, basato sui concetti di Agente (in generale l'utente collegato al sistema), Evento (p.e. "Inserimento" o "Cancellazione") e Oggetto (p.e. "Parametro di configurazione della **Struttura**").

In pratica, ogniquale volta un agente scatena un evento che modifica un oggetto (inclusa la creazione dell'oggetto stesso), il sistema di log registra la fotografia dell'oggetto modificato e le informazioni essenziali sulla modifica (agente, evento, timestamp, ecc.).

Sacerlog è utilizzato anche per registrare nel log eventi di sola consultazione (ad es. "Visualizzazione dettaglio **Unità documentaria**"), di cui è necessario tenere traccia per ragioni di sicurezza.

Il sistema di log è completamente parametrabile tramite funzioni di amministrazione, che consentono di stabilire quali combinazioni di agenti / eventi / oggetti / debbano essere registrati nel log.

Il log può essere consultato da un utente che possiede le dovute abilitazioni per determinare la storia di quanto accaduto su un oggetto. Il log può essere anche consultato per esporre il contenuto dell'oggetto ad un qualunque istante di riferimento, determinando la fotografia dell'oggetto più recente rispetto all'istante di riferimento.

[\[Torna al Sommario\]](#)

8.2.10 Componenti di supporto

Completano il Sistema i vari moduli di supporto, ovvero le componenti che non implementano specifiche logiche applicative, ma mettono a disposizione funzionalità trasversali agli altri moduli. Più nello specifico:

- il time server della rete regionale tramite protocollo NTP distribuisce il *Riferimento temporale* all'interno dei **Data Center** con fuso orario Europe/Rome (GMT+1) e configurazione della variazione automatica dell'ora solare, allineandolo costantemente con l'orario dell'Istituto Elettrotecnico Nazionale Galileo Ferraris di Torino (ntp.ien.it), che è a disposizione di qualsiasi altro sistema che voglia mantenere l'orario allineato con i sistemi di ParER.
- il modulo di Audit e Log di sistema è costituito da un insieme eterogeneo di componenti che si occupano di raccogliere tutte le informazioni rilevanti sugli eventi accaduti durante la vita del sistema. Si tratta di informazioni sistemistiche (*log di sistema* operativo, del data base e degli application server), di sicurezza (accessi andati a buon fine e rifiutati), che vengono raccolte dai diversi strati tecnologici del Sistema con il supporto di componenti specifici, ivi incluso Sacerlog. Il modulo di Log si basa su un sistema **SIEM** (HP ArcSight) opportunamente configurato e alimentato, che si occupa di raccogliere i *log* e memorizzarli in conformità con le politiche definite da ParER sulla base della normativa vigente, con i disciplinari regionali in materia di sicurezza informatica e con la necessità di mantenere nel Sistema tutte le informazioni necessarie a documentare le attività svolte, anche per funzionalità di audit. Le informazioni memorizzate in ArcSight vengono analizzate continuamente in remoto dal Centro Operativo per la Sicurezza (**SOC**), utilizzando opportuni strumenti atti a individuare tempestivamente eventuali minacce per la sicurezza del servizio. Componenti di audit e log sono presenti anche nel sito di **Disaster recovery**;
- il modulo di Monitoraggio Tecnico è costituito da un insieme eterogeneo di componenti che si occupano di raccogliere in tempo reale le segnalazioni di possibili malfunzionamenti dell'infrastruttura e di segnalarle alla struttura SICTR della Regione Emilia-Romagna preposta alla gestione; allo scopo vengono utilizzati diversi software open source tra cui Zabbix, che viene alimentato da opportuni agenti software, e Graylog, che raccoglie temporaneamente i log dei sistemi e li indicizza, per agevolare la diagnostica delle problematiche applicative. Le informazioni di monitoraggio sono raccolte per analisi di periodo nel cruscotto realizzato tramite un'applicazione di **business intelligence** costruita con lo strumento open source SpagoBI. Componenti di monitoraggio tecnico sono presenti anche nel sito di **Disaster recovery**;
- il modulo di Request Tracking viene utilizzato per automatizzare e mantenere traccia dei processi fondamentali del servizio di conservazione: tra questi la gestione dei malfunzionamenti, la gestione delle richieste di rilascio in produzione delle nuove versioni dell'applicativo e le richieste di manutenzione dell'infrastruttura; allo scopo viene utilizzato il software di **trouble ticket** open source RT (Request Tracker) messo a disposizione dal SICTR;
- i componenti di supporto allo sviluppo vengono utilizzati per garantire la corretta gestione degli sviluppi del software, per quanto riguarda sia l'evoluzione che la manutenzione correttiva del sistema; in generale si tratta di componenti open source normalmente utilizzati dai gruppi di sviluppo della Regione Emilia-Romagna sulla base di metodologie consolidate; tali componenti, oltre a facilitare lo sviluppo del software e a supportare la gestione dei progetti e delle risorse, consentono di tenere traccia di tutte le attività significative nell'ambito dello sviluppo, dal momento della definizione dei requisiti fino al momento della richiesta di rilascio, e delle relative evidenze documentali. La tracciatura del processo di sviluppo è supportata da un opportuno strumento open source (Redmine),

su cui sono definiti diversi workflow in ragione della problematica di sviluppo da affrontare;

- il sito web di ParER espone in modo strutturato informazioni e documentazione utile sia ai *Produttori* che agli *Utenti* (**Comunità di riferimento**). Tali informazioni riguardano, ad esempio, le procedure amministrative di attivazione dei servizi di conservazione e le specifiche per effettuare i **versamenti** dei SIP. Inoltre, rende disponibili informazioni aggiornate sulla quantità dei Documenti conservati e sulle tematiche legate agli *archivi*, alla gestione documentale e alla conservazione degli oggetti digitali. Dal sito è possibile, inoltre, iscriversi alla newsletter settimanale con cui ParER tiene aggiornata la **Comunità di riferimento** sulle novità in materia;
- il sito interno di ParER gestisce in modo strutturato informazioni e documentazione a supporto del Sistema di Gestione Integrato (SGI) della Qualità e della Sicurezza necessario per il conseguimento e il mantenimento delle certificazioni ISO sulla Sicurezza e sulla Qualità del servizio;
- SELF, sistema di e-Learning federato della Regione Emilia-Romagna, è il sistema che la Regione ha adottato per la diffusione dell'e-learning nelle proprie pratiche formative e in quelle di altri enti pubblici, cui SELF offre tecnologie, servizi, risorse didattiche e competenze gestione di corsi in e-learning. In particolare, per quanto riguarda ParER SELF mette a disposizione corsi introduttivi e intermedi sul processo di Conservazione e risorse formative sulla gestione della privacy.

[\[Torna al Sommario\]](#)

8.3 Componenti fisiche

8.3.1 Schema generale

Dal punto di vista tecnico il sistema è progettato e realizzato in maniera da fornire un'elevata continuità di servizio, garantire l'*integrità* degli oggetti conservati, gestire grandi volumi di dati, mantenere performance stabili indipendentemente dai volumi di attività ed assicurare la riservatezza degli accessi.

Il Sistema è sviluppato con tecnologie di larga diffusione open source o comunque di libero utilizzo, a parte i sistemi di memorizzazione di dati, per i quali si utilizzano prodotti proprietari, che dispongono però di interfacce standard de facto o de jure; in particolare il Data Base per ragioni di sicurezza e di performance è proprietario (Oracle), ma standard SQL, l'**Object Storage** (NetApp) è proprietario, ma adotta le specifiche **S3**, mentre il sistema di gestione dello **storage** su cassetta (TMS) è fornito da IBM, fornitore della **tape library**.

Il diagramma in figura schematizza le principali componenti infrastrutturali del *Sistema di conservazione* di ParER e le principali relazioni con altri sistemi interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

Il Sistema è realizzato su due siti che distano circa 100 chilometri l'uno dall'altro: un sito primario con caratteristiche di continuità operativa, installato presso il **Data Center** della Regione Emilia-Romagna a Bologna, che svolge funzioni di normale operatività, ed un sito secondario, installato

presso il **Data Center** di Lepida a Parma, ma gestito per i sistemi di ParER dal SICTR, che ha lo scopo di subentrare come sito di **Disaster recovery** nel caso di caduta irreparabile del sito primario.

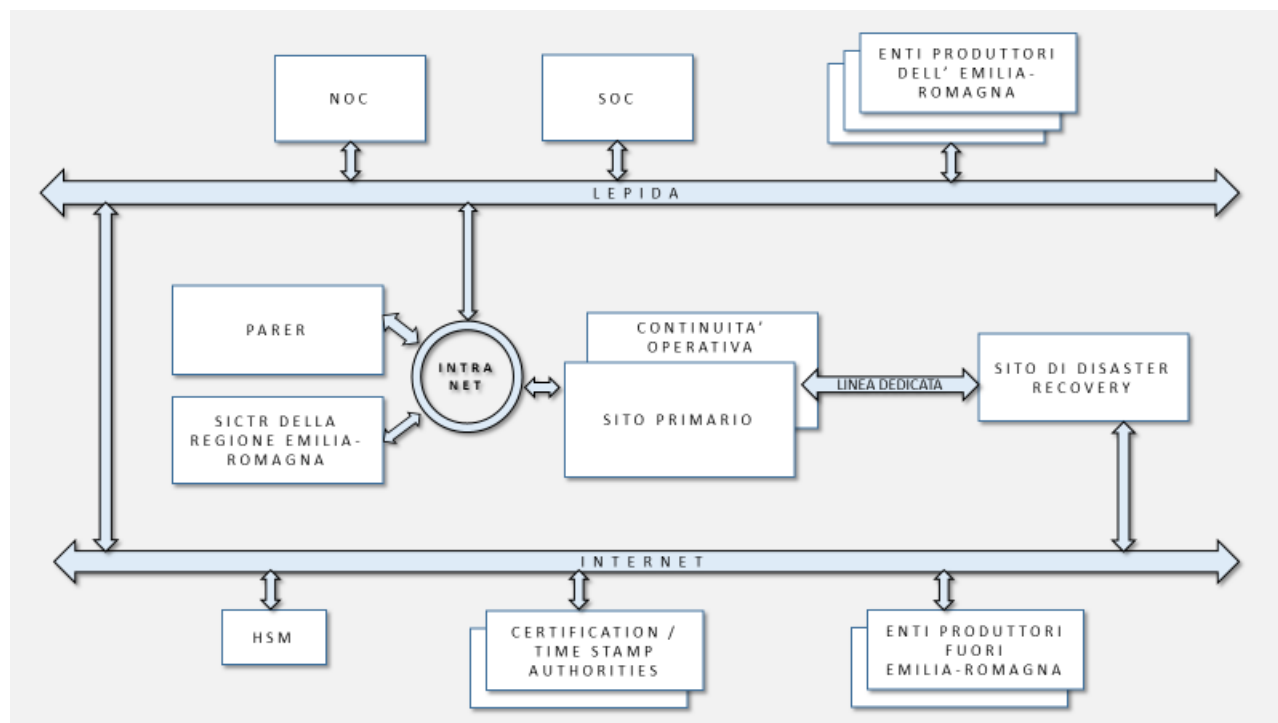


Figura 10 - Schema Infrastrutturale del Sistema di conservazione

Il sito primario e il sito di Parma sono gestiti dal SICTR della Regione Emilia-Romagna all'interno di una sottorete dell'Intranet regionale dedicata al *Sistema di conservazione*. Il collegamento tra i due siti è garantito da una linea dedicata in banda larga fornita da Lepida S.p.A. Il sito di **Disaster recovery** viene reso accessibile via Internet solo nel momento in cui, a seguito di disastro, dovesse essere promosso a sito primario.

Il Sistema di conservazione, benché sia ospitato in data center di terzi, dispone di sotto reti proprie isolate dalle altre sotto reti.

Alcuni sistemi di supporto sono installati in una sotto rete del **data center** del SICTR; nello specifico si tratta dei log server, dei time server, dei server di monitoraggio, dei server che ospitano il sito web di ParER e dei **proxy** che gestiscono gli scambi con gli **HSM**. La comunicazione tra la sotto rete del *Sistema di conservazione* e la sotto rete del SICTR è limitata a protocolli e porte ben specifiche, in modo tale da garantire l'isolamento della porzione di rete del *Sistema di conservazione* dai rimanenti sistemi regionali.

Gli **HSM** sono installati presso un fornitore esterno, aggiudicatario di gara per la gestione del servizio per la Regione Emilia-Romagna.

Presso un fornitore esterno aggiudicatario di apposita gara è allocato il Centro di Monitoraggio dell'Infrastruttura (**NOC**), che effettua il controllo continuo delle apparecchiature informatiche e dei server per tutti i sistemi della regione Emilia-Romagna, e quindi anche di ParER (escluso il sito di DR).

Presso un altro fornitore esterno aggiudicatario di apposita gara è allocato il Centro Operativo per la Sicurezza (**SOC**), che fornisce i servizi di sicurezza per tutti i sistemi della regione Emilia-Romagna, e quindi anche di ParER (escluso il sito di DR).

Il sito primario è costituito da due sotto-siti collegati in rete locale in due diversi edifici della Regione, che operano per garantire la **continuità operativa** del servizio.

Tutti i componenti del sito primario e del sito di continuità operativa, inclusi quelli installati nella sottorete del SICTR, e i componenti esterni sviluppati da ParER, nonché gli **HSM**, sono ridondati, mentre non lo sono i componenti del sito di **Disaster recovery**.

Il sistema interagisce con i *Produttori* dell'Emilia-Romagna tramite la rete regionale in banda larga **Lepida**, che è completamente ridondata; **Lepida** è a sua volta attestata su Internet con collegamenti in banda larga. In questo modo viene garantita tramite Internet una connessione ad alta velocità con i sistemi delle Certification / Time Stamp Authorities, con gli **HSM** e con i *Produttori* che non appartengono all'Emilia-Romagna e che quindi non sono connessi a **Lepida**.

In situazione di normale funzionamento il Sistema è attivo solo sul sito primario con garanzia di **continuità operativa** anche nel caso di caduta di uno dei due sotto-siti; il sito di **Disaster recovery** si limita a replicare le informazioni del sito primario in maniera asincrona man mano che vengono generate e a compiere funzioni di **backup** gestite autonomamente e di **archiving** sotto il controllo del sito primario.

Nel sito primario in situazione di normale funzionamento il carico della maggior parte delle applicazioni è distribuito tra i due sotto-siti; nel caso di caduta di uno dei due sotto-siti, l'altro ancora attivo provvede a garantire la continuità del servizio, sia pure con performance ridotte, fino al ripristino della situazione normale. Nel caso di caduta irreparabile di ambedue i sotto-siti del sito primario (disastro) il sito di **Disaster recovery** viene posto in stato di attività e attivato come destinatario del traffico di rete, con funzionalità ridotte fino al ripristino del sito primario.

Sia nel sito primario che nel sito di **Disaster recovery** sono presenti diverse istanze del Sistema:

- un'**istanza** di Produzione, cui è riservata la maggior parte delle risorse;
- un'**istanza** di Test, riservata al personale di ParER per il test delle nuove versioni rilasciate dai laboratori di sviluppo;
- un'**istanza** di Preproduzione, allineata all'**istanza** di produzione, per i test dei *Produttori*.

I sistemi di sviluppo risiedono presso il **Data Center** del SICTR.

La separazione delle istanze viene assicurata attraverso l'utilizzo di domini di rete distinti, che non sono visibili l'uno all'altro.

Nell'ambito di ciascuna istanza, il sistema utilizza una logica multi-Ente, assimilabile ad un sistema **multi-tenant**, intendendo con ciò un insieme di "aree" che - pur condividendo una medesima istanza applicativa - sono logicamente separate tra loro. Tale separazione è realizzata sia per quanto concerne gli accessi, sia per quanto concerne la conservazione dei dati.

[\[Torna al Sommario\]](#)

8.3.2 Caratteristiche tecniche dei Sistemi

Il diagramma in figura schematizza le principali componenti tecniche dei sistemi di ParER. I due sotto-siti del sito primario sono tra loro identici, tranne che per la presenza di una **tape library** di dimensioni ridotte in uno dei due siti, che svolge solamente funzioni di **Backup**; i sistemi del sito di **Disaster recovery** sono analoghi a quelli di un sotto-sito del sito primario, a parte la mancata ridondanza dei componenti e l'assenza del **proxy** per **HSM**.

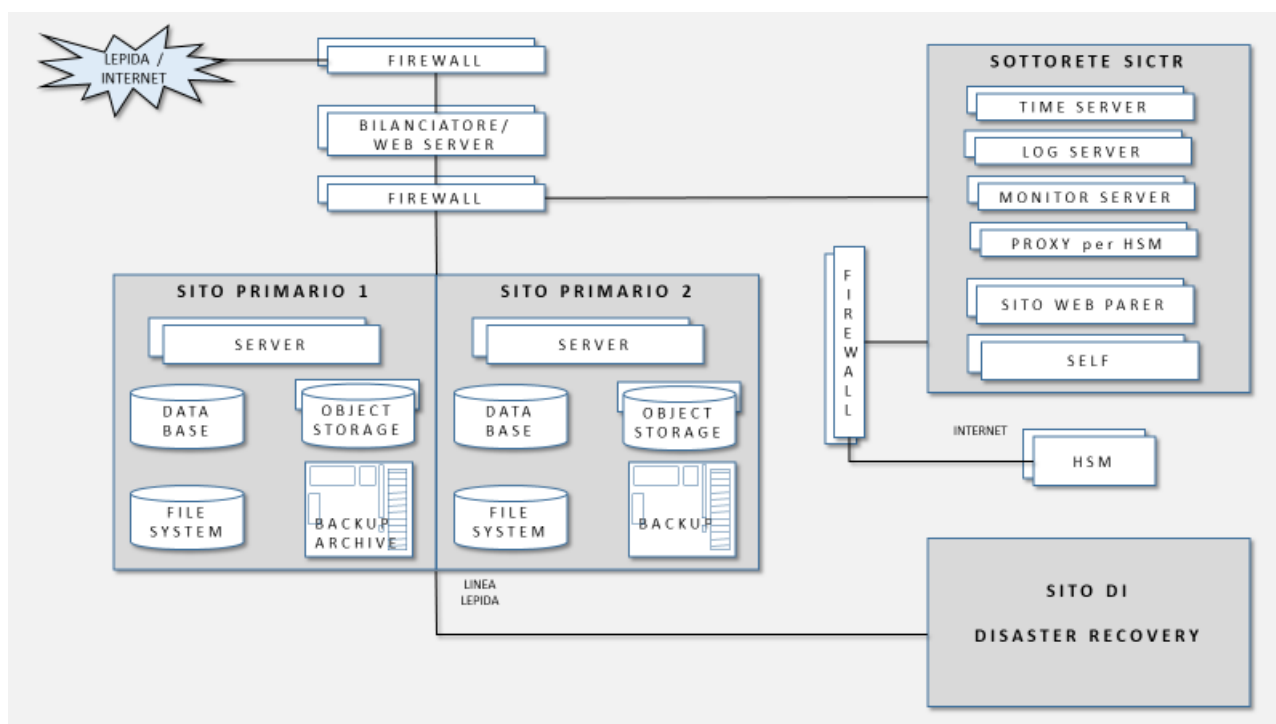


Figura 11 - Schema dei Sistemi di ParER

I servizi ausiliari, in quanto di interesse di tutta l'infrastruttura regionale, sono ospitati su server della sottorete del SICTR; tra questi fondamentale per il processo di conservazione è il time server della rete regionale tramite protocollo NTP distribuisce il *Riferimento temporale* all'interno dei **Data Center** con fuso orario Europe/Rome (GMT+1) e configurazione della variazione automatica dell'ora solare, allineandolo costantemente con l'orario dell'Istituto Elettrotecnico Nazionale Galileo Ferraris di Torino (ntp.iien.it).

Nell'ambito del sito primario i sistemi sono aggregati in **cluster**, mentre nel sito di **Disaster recovery**, in quanto non ridondato, non sono presenti cluster fisici di sistemi; sono però presenti cluster logici di Application server, in numero ridotto rispetto al sito primario, con lo scopo di distribuire il carico applicativo tra diversi sistemi.

Gli accessi al sistema avvengono esclusivamente passando da **firewall** tramite protocolli sicuri (**HTTPS** e **FTPS**).

Lo **storage** utilizza come supporti di memorizzazione sia dischi che nastri magnetici su cassetta.

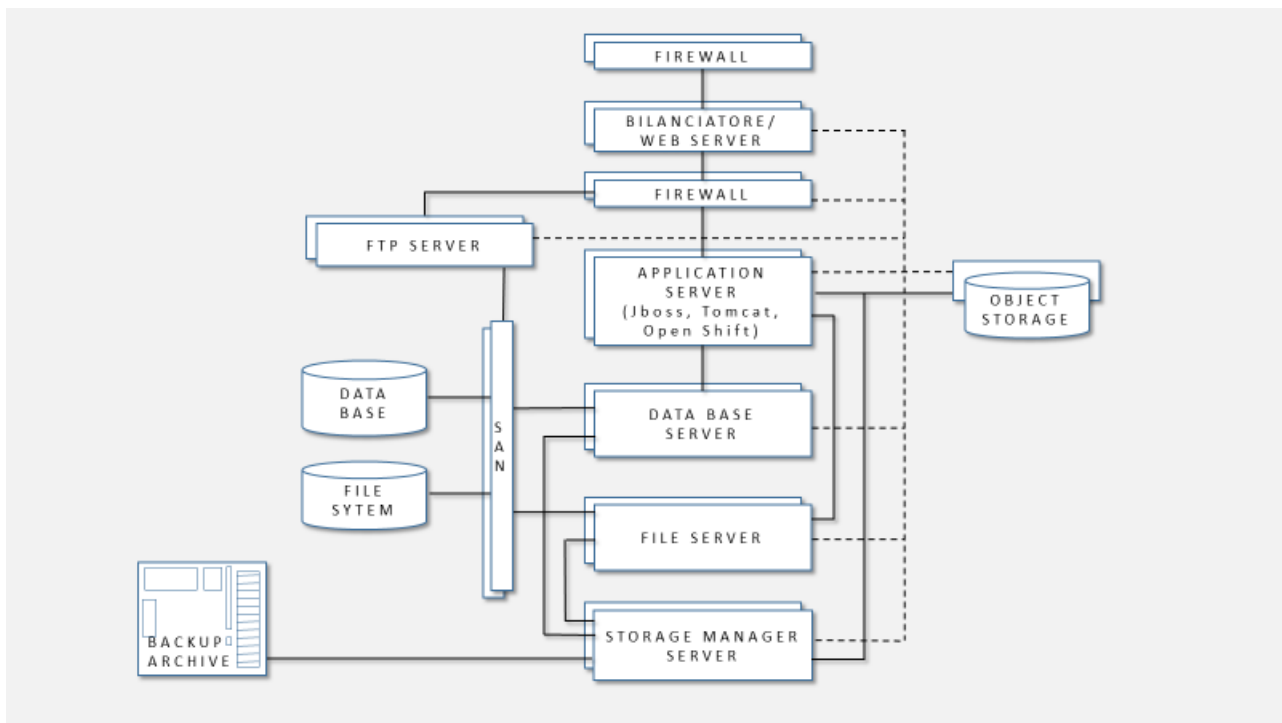


Figura 12 - Schema del Sito Primario

Lo **storage** su disco è suddiviso tra:

- **Data Base Oracle** per la *memorizzazione* dei metadati delle informazioni tipiche del processo di conservazione; viene utilizzato anche per memorizzare temporaneamente in forma di **BLOB** una parte degli **Oggetti-dati** dal momento del loro ingresso nel sistema fino al momento della loro conservazione definitiva nell'**Object storage**;
- **File system** per la *memorizzazione* temporanea degli **Oggetti-dati** che, in base alle politiche configurate nel sistema, verranno archiviati su cassette; il **file system** contiene inoltre tutti i file di servizio (log, configurazioni, ecc.) e un'Area **FTP** per il trasferimento ed il recupero asincrono degli **Oggetti-dati** da parte dei *Produttori*. Le aree temporanee vengono cancellate normalmente entro una settimana dopo l'utilizzo da opportune procedure applicative. Le aree utilizzate vengono sovrascritte continuamente e quindi i dati temporanei dopo un breve tempo non sono più accessibili.

Lo **storage** su disco è ospitato su uno storage array ed è costituito da un'area di storage primario con dischi ad alta velocità e da un'area di storage secondario con dischi a media velocità; in questo modo è possibile ottimizzare la distribuzione dei dati sui dischi in ragione delle necessità applicative.

La maggior parte degli **Oggetti-dati** conservati nel sistema risiede permanentemente all'interno di **appliance** dedicate alla gestione dell'**Object storage**, su cui vengono trasferite da un processo di elaborazione che li sposta dall'originaria posizione temporanea nel data base.

Lo **storage** su nastri magnetici si basa su un sistema a cassette (**tape library**), completamente governato da Tivoli Management System (TMS), che gestisce cassette in standard **LTO6** su cui vengono mantenuti:

- in modalità **archiving**, in situazione **near-line** gli **Oggetti-dati** che non vengono mantenuti nell'**Object storage** (tipicamente quelli molto voluminosi e di accesso non frequente);

- in modalità di **backup**, i backup full ed incrementali e gli archive log del Data Base, immediatamente disponibili per qualsiasi attività di restore che si rendesse necessaria;
- in modalità di **backup** i file presenti nel **File system**.

Il Sistema è sviluppato in **Java** su sistemi operativi Linux (Red Hat) utilizzando i seguenti componenti principali:

- **Bilanciatore di carico LBL** (Oplon), che svolge anche il ruolo di Web server;
- **File Server** GlusterFS per la gestione del file system condiviso tra diversi server e delle aree **FTP**;
- **FTP server** in cluster;
- **Application server** JBoss Enterprise (Red Hat) in cluster logico gestito dai componenti di clustering di JBoss;
- **Servlet container** Tomcat (Apache) per i componenti che non richiedono l'utilizzo di un application server (p.e. TPI, DPI, Kettle server);
- Open Shift (Red Hat) come orchestratore dei container in cui vengono eseguiti i **Microservizi**;
- Data Base Oracle con utilizzo delle funzionalità di **RAC, di Data Guard** e di **partitioning**;
- **Object Storage** NetApp distribuito in replica su tre siti;
- Storage Manager Tivoli (IBM) con funzionalità di **Backup** e **Archiving** su **tape library**.

I moduli applicativi del Sistema, essendo sviluppati in **Java** secondo le specifiche **Java Platform Enterprise Edition (J2EE)**, sono raggruppati in diversi contesti applicativi caricati su JBoss. I moduli principali sono ognuno connesso ad un proprio schema di Data Base, in modo da garantire una buona modularità dell'applicativo. I componenti che non dispongono di proprio schema di Data Base utilizzano gli altri schemi, accedendo tramite **Web Service** appositamente ottimizzati per l'accesso ai dati, oppure tramite opportuni **grant**. I componenti applicativi che richiedono un'esecuzione fortemente dinamica sono invece sviluppati tramite **Microservizi** caricati in opportuni contenitori la cui gestione viene orchestrata da Open Shift.

Il colloquio tra il Sistema e gli applicativi esterni è effettuato tramite **Web Service**.

Il trasferimento dei dati sincrono è realizzato in **HTTPS** tramite tecnologie **ReST**, mentre il trasferimento asincrono utilizza tecnologie **FTPS**.

Il Sistema è Web-based e testato per diversi browser (Firefox, Explorer, Chrome). Non richiede l'installazione di alcun componente sul client.

Il **framework di sviluppo** utilizzato è stato derivato dal framework open source Spring, migliorandone gli aspetti di accessibilità; la **persistenza** è gestita tramite **EJB**, generati con il framework JPA e solo in pochissimi casi particolari ben identificati e documentati tramite chiamate dirette JDBC, in modo da garantire portabilità verso altri Data Base relazionali e quindi facilitare il riuso dell'applicativo. Il sistema ingloba diverse librerie applicative open source, molte delle quali sviluppate nell'ambito di progetti internazionali, in particolare per la verifica delle firme e dei **formati**.

La replica dei dati sul sito secondario è garantita da diverse tecnologie:

- il Data Base viene sincronizzato da Oracle tramite Data Guard con modalità di physical standby e maximum availability (il sito primario non attende la fine della scrittura del sito di **Disaster recovery** per considerare chiusa la transazione);

- l'**Object storage** viene replicato nei diversi siti dalle tecnologie intrinseche di NetApp;
- il file system su disco viene allineato tramite **SCP**;
- l'archivio su cassette viene mantenuto aggiornato da TMS in maniera indipendente tra i due siti tramite opportune politiche di schedulazione; l'applicativo controlla periodicamente la corretta sincronizzazione dei file system e degli archivi su cassette tra i due siti.

Nel caso di dismissione di dispositivi elettronici di memorizzazione dei dati ParER si occupa di garantire la cancellazione sicura delle informazioni presenti nel sistema; a tal fine negli accordi con i gestori dell'infrastruttura ParER richiede esplicitamente l'impegno ad adottare idonei accorgimenti e misure per la distruzione dei supporti di memorizzazione dei dati, una volta dismessi.

[\[Torna al Sommario\]](#)

8.4 Procedure di gestione e di evoluzione

La gestione del *Sistema di conservazione* è affidata a diversi gruppi di operatori di ParER, secondo la natura delle attività da svolgere; tali attività includono la gestione operativa del sistema in esercizio, l'avviamento di nuovi enti e di nuovi servizi di conservazione e le eventuali successive modifiche, e infine la gestione dei malfunzionamenti e degli incidenti di sicurezza.

[\[Torna al Sommario\]](#)

8.4.1 Gestione dell'Esercizio

Per quanto attiene alla gestione operativa del sistema in esercizio, l'Area Esercizio dei Servizi di Conservazione di ParER presidia le attività descritte nello specifico punto del paragrafo 5.2.

L'Area di Gestione dei Servizi e delle Infrastrutture di ParER presidia parallelamente l'operatività quotidiana dell'infrastruttura hardware e software sottostante il *Sistema di conservazione*, nonché la pianificazione ed il controllo delle attività straordinarie che possono avere impatto sull'esercizio, come descritto allo specifico punto del paragrafo 5.2, oltre a quelle dettagliate nel paragrafo 9.2; è suo compito indirizzare le attività di gestione che sono svolte dal SICTR della regione Emilia-Romagna ai fini della gestione del sito primario incluso il sito di **Continuità Operativa** e verificarne il buon funzionamento; infine si occupa di verificare il buon funzionamento dell'infrastruttura di **Disaster Recovery**.

[\[Torna al Sommario\]](#)

8.4.2 Gestione delle utenze

La procedura riportata nel documento "Gestione utenze" e schematizzata in figura descrive le modalità con cui viene garantita la corretta gestione dei soggetti che hanno accesso al sistema

di conservazione, con particolare riguardo alla sicurezza dei dati e delle informazioni conservate, nel rispetto della politica generale di controllo degli accessi di ParER.

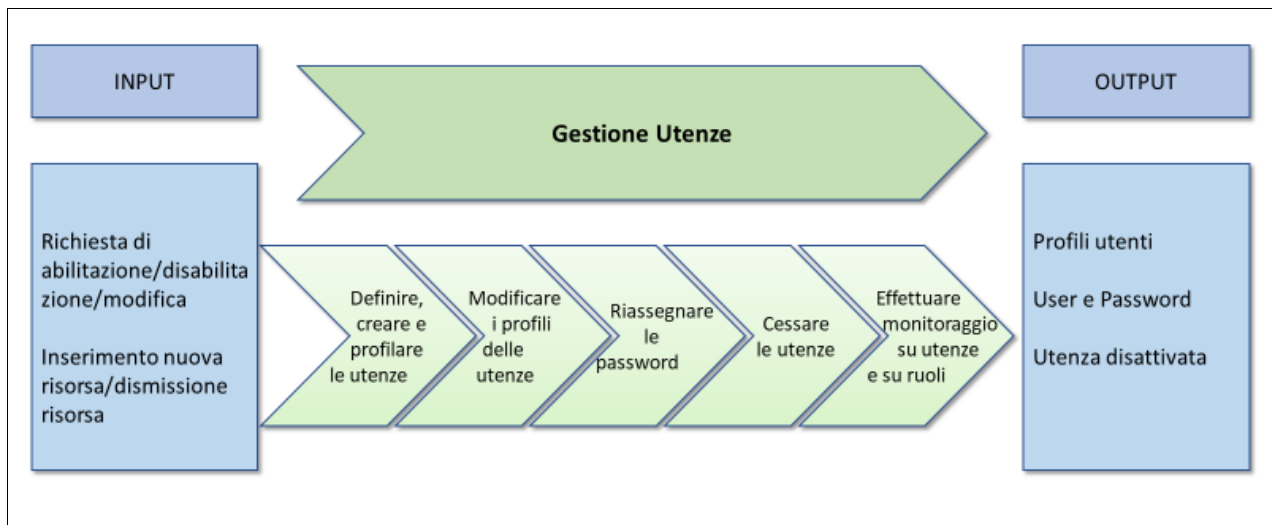


Figura 13 - Procedura di Gestione utenze

La procedura descrive inoltre il metodo seguito per la gestione delle password in coerenza con quanto descritto nella *Politica sulla sicurezza delle informazioni del servizio di Conservazione*.

In particolare, in caso di Creazione di nuovo utente, Riattivazione e Reset di password il sistema genera casualmente le password, le memorizza in forma criptata e le presenta temporaneamente a video in modo che l'operatore possa comunicarle all'utente.

L'operatore di Help Desk di ParER provvede a creare l'utenza nel sistema inviando tramite due e-mail separate lo user-id e la password, che l'utente deve necessariamente cambiare al primo accesso. Nell'*Appendice – regole di Autenticazione e Linee guida per una password "sicura"* del Documento "Gestione Utenze" sono esplicitate:

- le regole di validazione a cui sono sottoposte le password;
- le regole "di buon senso" da applicare nella creazione di una password, suggerite all'utente, ma non validabili dal sistema.

Nel caso in cui l'utente abbia dimenticato la password il suo Referente può chiederne la riassegnazione (reset) inviando l'opportuna richiesta tramite una comunicazione formale. L'operatore di Help Desk di ParER (o del gestore esterno) provvede a caricare la richiesta in riferimento alla comunicazione, desumendo le informazioni dal testo della comunicazione o dal file allegato.

Il sistema di gestione delle autenticazioni viene costantemente aggiornato in base alle direttive regionali in termini di sicurezza informatica e alle risultanze dei processi di certificazione per la sicurezza e di accreditamento.

[\[Torna al Sommario\]](#)

8.4.3 Gestione dei Malfunzionamenti

La procedura riportata nel documento “Gestione Richieste e Malfunzionamenti” e schematizzata in figura descrive la maniera in cui ParER tratta le richieste di informazioni, i malfunzionamenti e gli eventuali reclami da parte degli utenti del sistema.

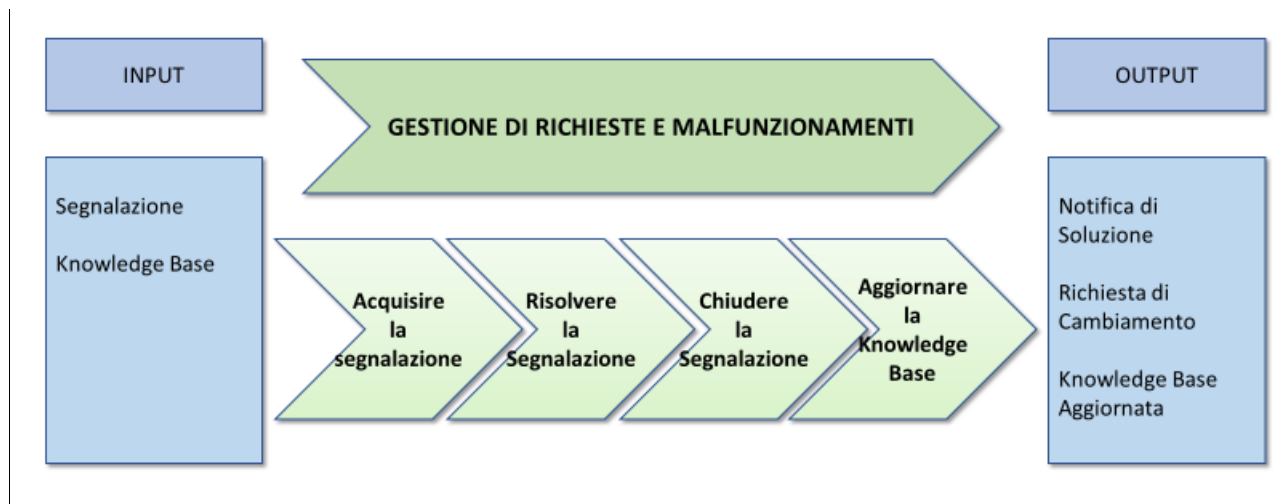


Figura 14 - Procedura di Gestione richieste e malfunzionamenti

La gestione dei malfunzionamenti può coinvolgere diverse strutture di ParER, secondo la natura del malfunzionamento stesso, che può essere rilevato da diverse fonti: malfunzionamenti di natura applicativa possono essere segnalati dagli Enti *Produttori*, dagli *Enti Conservatori* e dagli *Enti Gestori*, dall'Area Esercizio dei Servizi di Conservazione, dall'Area Funzione Archivistica di Conservazione di ParER o dall'Area Tecnologia e Sviluppo Sistemi di Conservazione, mentre malfunzionamenti di natura tecnica possono essere segnalati dall'Area di Gestione dei Servizi e delle Infrastrutture del ParER dal SICTR della Regione Emilia-Romagna.

Allo stesso modo diverse possono essere le strutture che intervengono nella soluzione del malfunzionamento: l'Area Esercizio dei Servizi di Conservazione è normalmente in grado di risolvere i malfunzionamenti che non sono dovuti a problemi tecnici, eventualmente coinvolgendo il l'Ente che ha rilevato il malfunzionamento e per suo tramite i suoi fornitori di servizi; i malfunzionamenti di natura infrastrutturale vengono risolti dall'Area di Gestione dei Servizi e delle Infrastrutture, che coordina gli interventi del; l'Area Tecnologie e sviluppo sistemi di conservazione viene coinvolta nel caso in cui si sia verificato un malfunzionamento del software applicativo; in questo caso si attivano le procedure di manutenzione, che sono descritte nei successivi paragrafi.

[\[Torna al Sommario\]](#)

8.4.4 Gestione degli Incidenti di Sicurezza

Tutte le aree organizzative di ParER e il SICTR con il supporto del **SOC** sono sistematicamente coinvolte nelle attività di prevenzione e di risoluzione degli incidenti di sicurezza, secondo le politiche definite nella *Politica sulla sicurezza delle informazioni del sistema di conservazione* di ParER.

La procedura riportata nel documento “Gestione incidenti di sicurezza” e schematizzata in figura descrive le modalità con cui vengono gestiti gli eventi che possono avere un impatto sui requisiti di *integrità, disponibilità e riservatezza* dei dati conservati o del Servizio di conservazione.

L’obiettivo della procedura viene raggiunto attraverso le seguenti attività:

- gestire gli eventi;
- gestire gli incidenti di sicurezza;
- gestire le attività post-incidente.

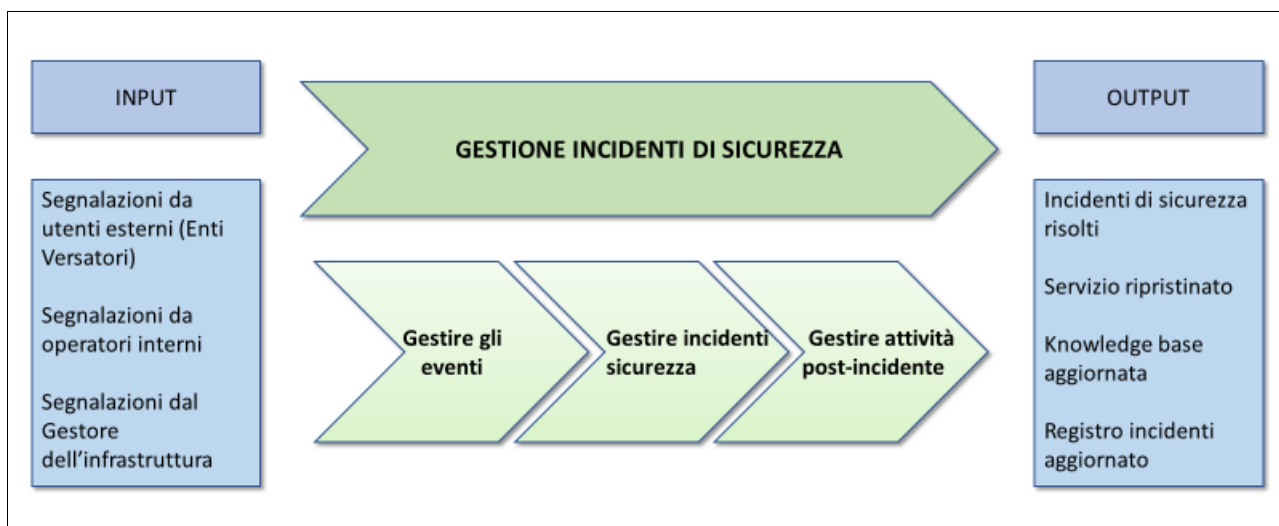


Figura 15 - Procedura di Gestione incidenti di sicurezza

All'interno della Procedura, ParER ha definito le responsabilità nell'ambito della gestione degli incidenti di sicurezza.

In particolare,

- gli Enti convenzionati hanno l'obbligo di notificare tempestivamente a ParER (alla casella helpdeskParER@Regione.Emilia-Romagna.it) gli **Incidenti di sicurezza (compresi i Data Breach)** di qualsiasi natura, che coinvolgono il Sistema di conservazione, al fine di garantire l'applicazione delle contromisure adeguate. Le notifiche devono essere effettuate sulla base delle regole definite di seguito.
- ParER ha l'obbligo di
 - gestire gli incidenti di sicurezza, garantendone la tracciatura e l'applicazione di soluzioni adeguate alla riduzione degli impatti;
 - notificare tempestivamente agli Enti convenzionati un'incidente di sicurezza di qualsiasi natura, che coinvolga l'ambito di titolarità dell'Ente. Le notifiche devono essere effettuate sulla base delle regole definite di seguito.

Le notifiche devono essere effettuate via e-mail e contenere almeno le seguenti informazioni:

- data/ora e modalità attraverso le quali si è venuti a conoscenza dell'evento.
- causa, sistemi coinvolti, eventuali disservizi causati, utenti coinvolti, dettagli tecnici rilevanti.
- data/ora e azioni intraprese per contenere i danni causati dall'incidente e per ripristinare i sistemi
- considerazioni sull'incidente, suggerimenti, adeguamenti da effettuare.

Nel caso in cui tutte le informazioni sopraindicate non siano immediatamente disponibili, queste saranno comunicate nel corso della gestione dell'incidente.

A fronte della richiesta da parte dell'Ente impattato da un eventuale incidente, ParER può condividere eventuali evidenze digitali o altre informazioni dopo la chiusura dell'incidente stesso attraverso opportuni canali di comunicazione.

[\[Torna al Sommario\]](#)

8.4.5 Evoluzione pianificata

L'evoluzione pianificata del Servizio di Conservazione segue le linee guida formulate dal Responsabile del Servizio, che ne stabilisce politiche, priorità e tempistiche; l'evoluzione è inquadrata nell'ambito di un piano annuale, rivisto semestralmente e articolato in progetti, ed è monitorata tramite Stati di Avanzamento Lavori (SAL) periodici, cui partecipano diversi soggetti in ragione dei diversi argomenti trattati. In particolare, si tengono SAL per l'evoluzione degli aspetti operativi del servizio, cui partecipano gli addetti all'Area Esercizio dei Servizi di Conservazione, SAL per l'evoluzione degli applicativi, cui partecipano i responsabili delle diverse aree di ParER e i responsabili dei fornitori dello sviluppo e, quando necessario, SAL per l'evoluzione dell'infrastruttura, cui partecipano anche i responsabili del SICTR. I progetti sono gestiti tramite una pianificazione di dettaglio, che fissa tempi di realizzazione ed impiego delle risorse, con il supporto, ove applicabile, di un opportuno strumento di gestione (Redmine).

[\[Torna al Sommario\]](#)

8.4.6 Richieste di Cambiamento

All'evoluzione pianificata si affiancano evoluzioni derivanti dalle necessità di migliorare l'operatività dell'esercizio, e, soprattutto per quanto riguarda il software applicativo, dalla necessità di correggere eventuali errori o imperfezioni del sistema; tali necessità vengono formalizzate come Richieste di Cambiamento, la cui gestione è descritta in dettaglio nel documento "Gestione richieste di cambiamento" e la cui procedura è schematizzata in figura.

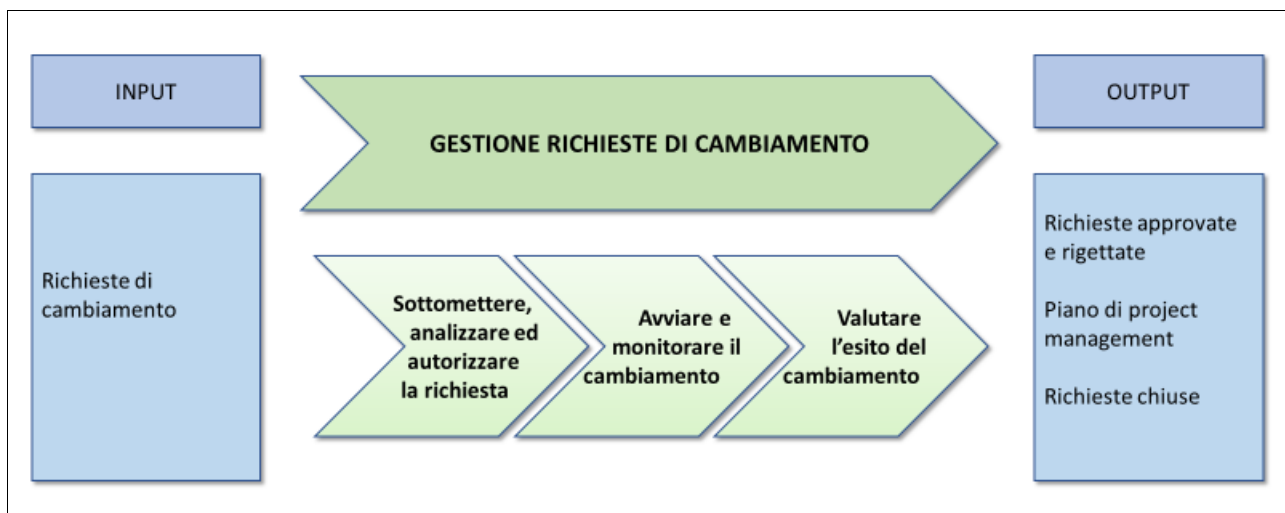


Figura 16 - Procedura di Gestione richieste di cambiamento

Le richieste di cambiamento riguardano sia cambiamenti di tipo applicativo, che infrastrutturale e di configurazione. Per ogni ambito esiste un responsabile di riferimento che costituisce il punto di raccolta delle richieste / esigenze che emergono nell'area di competenza. Le richieste di cambiamento vengono valutate prima di essere autorizzate; se autorizzate, ottengono una priorità di realizzazione e vengono pianificate nell'ambito della pianificazione generale dei lavori, qualora non abbiano alta criticità; se invece rivestono carattere d'urgenza, ottengono priorità massima e risorse dedicate, fino alla soluzione; la pianificazione generale riserva normalmente una quota delle risorse per le attività correttive urgenti.

Il monitoraggio della realizzazione dei cambiamenti di una certa entità e la valutazione degli esiti è normalmente discusso nei SAL; i cambiamenti realizzati sono comunicati dai Responsabili delle diverse Aree al personale del ParER ed eventualmente agli altri soggetti coinvolti nel servizio di conservazione.

Se la richiesta di cambiamento riguarda le componenti applicative del sistema, viene attivato il processo di sviluppo del software, dalla definizione dei requisiti fino al rilascio in produzione, come descritto nei prossimi paragrafi.

La procedura di evoluzione è più snella nel caso di interventi evolutivi di minore rilevanza, quali correzioni di errori e piccole migliorie, che non richiedono la definizione di requisiti e la verifica di compatibilità tecnica; anche il test di accettazione in generale in questi casi risulta notevolmente semplificato.

ParER comunica tempestivamente agli Enti i cambiamenti che hanno impatto sul Servizio.

In particolare:

- modifiche all'infrastruttura di erogazione,
- modifiche dei referenti del Servizio,
- modifiche al processo di conservazione,

sono comunicate tramite pubblicazione sul sito web di ParER e sulla pagina dei conservatori accreditati di AgID, mentre il rilascio di nuove funzionalità viene comunicato tramite la pubblicazione delle informazioni sulle nuove **release** sul sistema di conservazione.

[\[Torna al Sommario\]](#)

8.4.7 Progettazione e Realizzazione di Software Applicativo

La procedura riportata nel documento “Progettazione e realizzazione di software applicativo” e schematizzata in figura descrive le modalità con cui vengono garantiti lo sviluppo del software e l’esecuzione dei test preliminari al rilascio in produzione, in accordo con tempi, risorse e modalità attuative concordate nel piano delle attività, assicurando l’allineamento con le esigenze espresse e coordinandosi con i fornitori coinvolti.

La procedura inizia con la definizione dei requisiti in accordo con l’Area Tecnologie e Sviluppo dei Sistemi di Conservazione, e procede poi con il test di integrazione effettuato dagli analisti funzionali e dagli analisti informatici della soluzione realizzata. Il superamento del test di integrazione produce una nuova **release**, che viene deployata in ambiente di Test.

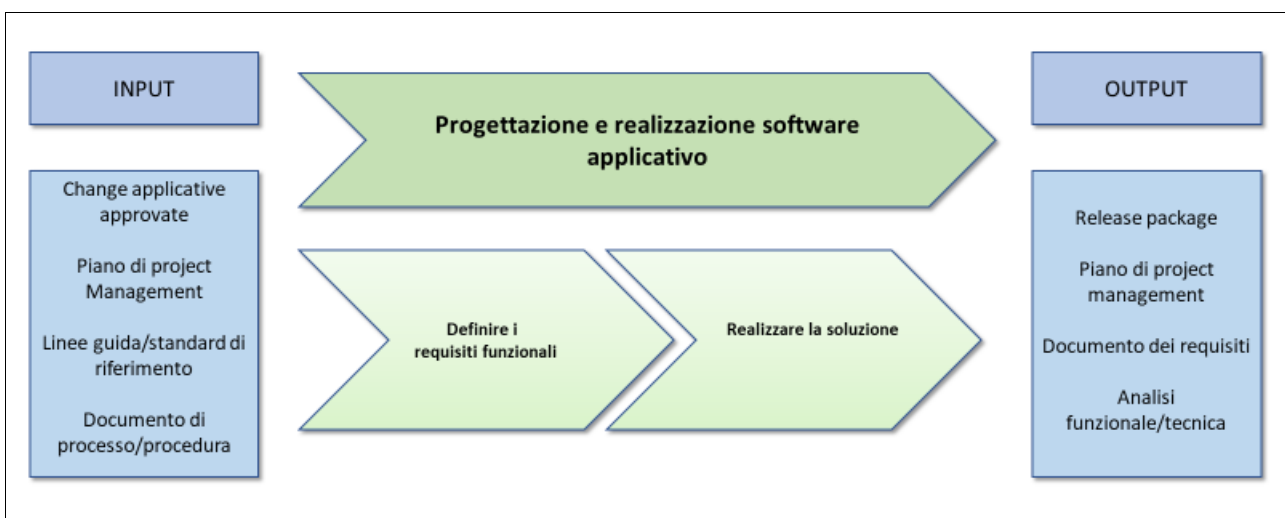


Figura 17 - Procedura di Progettazione e realizzazione di software applicativo

I test della nuova **release** vengono condotti nell’ambiente di Test sulla base del piano di test sotto responsabilità dell’Area Tecnologie e Sviluppo con il supporto dell’Area Esercizio dei Servizi Archivistici. Questi test analizzano i comportamenti globali del sistema che non è possibile osservare in riferimento al singolo modulo o componente e coprono l’intera gamma delle caratteristiche da testare (test funzionali, test di performance, test di interfaccia, test di affidabilità, test di stress, test di sicurezza).

Le diverse attività prevedono un continuo scambio di informazioni tra il personale dell’Area Tecnologie e Sviluppo dei Sistemi di Conservazione e il personale dell’Area Esercizio Servizi di Conservazione, al fine di garantire la coerenza tra i requisiti (funzionali, di sicurezza e di esercibilità) e quanto sviluppato.

Lo sviluppo del software applicativo segue le linee guida fissate dalla Regione Emilia-Romagna per lo sviluppo sicuro e le raccomandazioni degli standard di riferimento internazionali; i dettagli in merito sono riportati nel *Piano della Sicurezza* di ParER.

Lo sviluppo è supportato da strumenti di gestione dello sviluppo e di versioning del codice secondo gli standard definiti dai Sistemi Informativi della Regione Emilia-Romagna.

La tracciatura del processo di sviluppo è supportata da un opportuno strumento (Redmine), su cui sono definiti diversi workflow in ragione della problematica di sviluppo da affrontare.

Al termine del processo di sviluppo il software applicativo viene rilasciato come nuova **release** eventualmente deployabile in pre-produzione e produzione.

[\[Torna al Sommario\]](#)

8.4.8 Gestione dei Rilasci

Prima di effettuare il rilascio in preproduzione e produzione, L'Area Tecnologie e Sviluppo verifica tramite sistemi automatici e controlli manuali l'eventuale obsolescenza delle librerie di componenti utilizzate nella produzione della nuova **release**; qualora si rilevino criticità nell'ambito della sicurezza o rischi di malfunzionamenti, la nuova release non viene rilasciata, ma rimandata agli sviluppatori per l'aggiornamento dei componenti obsoleti e un nuovo system test. Se non si rilevano problemi bloccanti, l'Area Tecnologie e Sviluppo concorda con l'Area di Gestione dei Servizi e delle Infrastrutture e con l'Area Esercizio dei Servizi di Conservazione il piano di rilascio della nuova **release** nell'ambiente di preproduzione e successivamente nell'ambiente di produzione, e richiede al SICTR di effettuare il rilascio.

La procedura di rilascio di una nuova **release** è illustrata in figura e descritta in dettaglio nel documento "Gestione dei Rilasci".

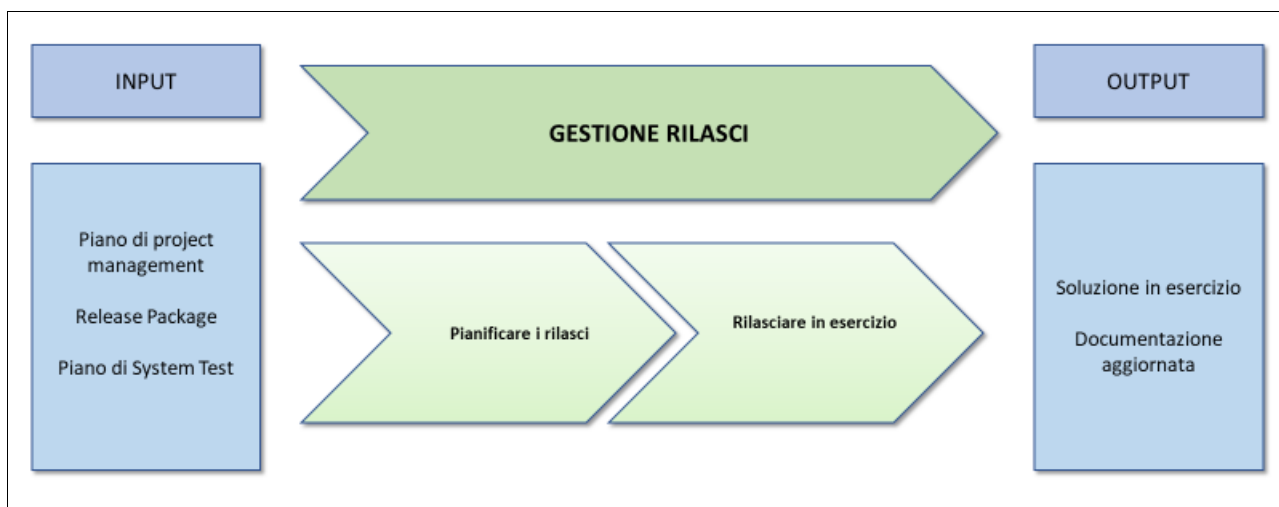


Figura 18 - Procedura di Gestione dei rilasci

L'obiettivo del processo di Gestione dei rilasci viene raggiunto attraverso le seguenti attività:

- pianificare i rilasci relativi a nuove soluzioni nei diversi ambienti precedenti al passaggio in esercizio, in accordo con tempi, finestre temporali predefinite, risorse e modalità attuative concordate;
- definire e pianificare le eventuali attività formative (per utenti, personale interno, Gestore dell'infrastruttura e Outsourcer) che devono accompagnare il rilascio in esercizio;
- verificare che il rilascio non abbia avuto impatti negativi sull'esercizio, e nel caso risolverli;
- coordinare i rilasci in esercizio delle nuove funzionalità mantenendo il coordinamento e la verifica delle attività in carico al Gestore dell'infrastruttura e all'Outsourcer e garantendo il rispetto dei tempi pianificati.

Il SICTR tramite una procedura automatica provvede inoltre a installare nel sito di **Disaster recovery** la nuova **release**, da attivare nel caso di dichiarazione di disastro.

[\[Torna al Sommario\]](#)

8.4.9 Gestione e conservazione dei Log

Tutti i log di sistema, qualunque sia lo strumento che li genera, vengono raccolti nel sistema di log (ArcSight) della regione Emilia-Romagna, dove possono essere analizzati da personale dotato delle opportune autorizzazioni, secondo quanto definito nei disciplinari regionali in materia; inoltre sono continuamente verificati dal Centro Operativo per la Sicurezza (**SOC**) nell'ambito delle attività di prevenzione e controllo delle minacce informatiche.

In base alle politiche regionali periodicamente i log più vecchi di un anno vengono cancellati automaticamente dal sistema, sotto controllo del personale del SICTR, in quanto si ritiene dopo tale periodo di tempo abbiano esaurito la loro utilità.

Fanno eccezione i log degli accessi ai documenti e degli errori di accesso ai sistemi raccolti da Sacerlog, che vengono cancellati da ArcSight al massimo dopo un anno, ma vengono mantenuti nel data base di SacER per un massimo di 10 anni, in quanto possono essere utili all'identificazione delle ragioni di un malfunzionamento anche parecchio tempo dopo il suo verificarsi. Tali log sono accessibili secondo necessità solo a personale tecnico esplicitamente incaricato a tale scopo dal Responsabile del Servizio.

Su richiesta motivata dell'Ente, i Log sono resi disponibili per la consultazione, limitatamente alle informazioni di pertinenza dell'Ente.

[\[Torna al Sommario\]](#)

9 MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

Oltre alle funzionalità di monitoraggio applicativo gestite dal personale di ParER, che sono state illustrate al paragrafo 7.4.1, sono attive procedure di monitoraggio tecnico gestite dal personale del **SICTR**, che provvede a produrre e rendere disponibili periodicamente all'Area Gestione dei servizi e delle infrastrutture di ParER report di controllo di tutte le aree infrastrutturali (rete, server, **storage**, database, **backup**). Si tratta di report tra loro eterogenei, ottenuti per rielaborazione e integrazione delle informazioni prodotte per via automatica dal software di base dei sistemi e dal software di monitoraggio tecnico installato sui medesimi e dai log delle attività svolte dal personale tecnico. Analoghi report vengono prodotti dalla gestione del **Disaster recovery**.

Periodicamente i report di monitoraggio tecnico vengono esaminati congiuntamente dall'Area Gestione dei servizi e delle infrastrutture di ParER e dall'Area Tecnologie e sviluppo sistemi di conservazione, con lo scopo di individuare eventuali aree di miglioramento negli aspetti tecnici dell'applicativo.

[\[Torna al Sommario\]](#)

9.2 Funzionalità per la verifica e il mantenimento dell'integrità degli archivi

Le procedure di monitoraggio illustrate nel paragrafo precedente, le politiche di conservazione dei **backup** e le caratteristiche delle tecnologie utilizzate garantiscono la completa *integrità* di quanto archiviato in SacER, ovvero di quanto depositato nel Data Base e negli archivi su cassetta, una volta che sia stato duplicato nel sito di **Disaster recovery** e salvato tramite opportuno **backup** sia nel sito primario che nel sito secondario

Le funzionalità messe a disposizione per realizzare le componenti logiche di Archiviazione e di Gestione dei dati consentono:

- la manutenzione e l'amministrazione del Data Base, che si occupa di gestire tutti i metadati trattati nel Sistema. La gestione sistemistica del Data Base è effettuata tramite prodotti certificati da Oracle, ed è tracciata nel *log di sistema*. Il Data Base fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificare attività di manutenzione del Data Base stesso e degli applicativi che lo utilizzano;
- il controllo dell'*integrità* del Data Base, che avviene utilizzando funzionalità native del Data Base stesso. Le funzionalità di **Data Guard** del Data Base assicurano la replica del Data Base nel sito di **Continuità operativa** (in maximum security) e di **Disaster recovery** (in maximum availability), mentre le funzionalità di Recovery Management consentono **backup** del Data Base completi e incrementali, a caldo e a freddo, secondo le politiche di sicurezza descritte nel Piano della Sicurezza

- la manutenzione e l'amministrazione dell'**object storage**, che si occupa di gestire tutti i **Componenti** (files) che transitano nel Sistema, a parte i file memorizzati temporaneamente nel **file system** e definitivamente nello storage a cassette, è effettuata tramite prodotti certificati da NetApp, ed è tracciata nel *log di sistema*. L'**object storage** fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificarne le attività di manutenzione del Data Base stesso e degli applicativi che lo utilizzano;
- la congruenza delle copie dei file nei diversi siti in cui è installato l'**object storage** è garantita dalle caratteristiche intrinseche dell'**object storage**, che vengono opportunamente utilizzate dagli applicativi. Allo stesso modo è garantita dalle specifiche dell'**object storage** la possibilità di aggiungere ulteriori nodi anche in altri siti, per aumentare il numero delle copie dei documenti;
- la manutenzione e l'amministrazione ai **Componenti** memorizzati su storage a cassette è effettuata tramite prodotti certificati da IBM, ed è tracciata nel *log di sistema*;
- per quanto attiene invece ai **Componenti** memorizzati su storage a cassette, l'integrità nel singolo sito è garantita da funzionalità intrinseche del modulo di archiving di TMS per tutti i dati archiviati su cassetta; queste ultime includono tra l'altro il controllo ed il riversamento periodico dei dati archiviati su nuove cassette; la congruenza tra il sito primario e il sito di **Disaster recovery** è invece garantita dalle logiche applicative implementate nel modulo TPI.

Per quanto riguarda l'integrità del contenuto informativo delle **Unità Documentarie** e in particolare dei **Componenti**, essa è garantita dal mantenimento delle impronte dei file per tutta la vita dei pacchetti informativi.

Esistono nel sistema diversi momenti in cui le impronte vengono verificate dopo il versamento, come ad esempio la creazione dell'AIP e la copia del file dal **Blob** del Data Base all'**object storage**.

Qualora, nonostante le garanzie fornite dalle tecnologie impiegate, si verificassero anomalie nell'*integrità* degli archivi, sono previste le opportune procedure applicative di ripristino illustrate nel paragrafo seguente; tali procedure sono rese possibili dalle politiche di gestione dei **backup**, che garantiscono la manutenzione di copie integre degli archivi fino a superamento delle verifiche di *integrità* e ad adozione di procedure di ripristino.

Non sono considerati facenti parte del Sistema, e quindi non fruiscono della stessa garanzia di *integrità*, i dati in ingresso presenti su aree temporanee (spazi FTP, **file system** del DPI, ecc.), per i quali le procedure di soluzione di cui al paragrafo seguente prevedono la ritrasmissione nel caso di anomalie.

Il *Piano della Sicurezza* di ParER descrive le modalità con cui ParER assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i back up degli archivi e il **Disaster recovery**.

[\[Torna al Sommario\]](#)

9.3 Soluzioni adottate in caso di anomalie

Le anomalie vengono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che le ha generate nel *processo di conservazione*; quindi oltre alle procedure atte a garantire l'*integrità* degli archivi, nel senso indicato al paragrafo precedente, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema che registrano dati in SacER. Qui di seguito si trattano esclusivamente le anomalie di origine tecnica, in quanto il trattamento delle anomalie verificatesi nel processo di versamento è già stato descritto precedentemente nel paragrafo 7.4.2

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici; in particolare:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area FTP o nel **File System** operano in modalità transazionale;
- il **backup** del Data Base assicura il restore all'ultima transazione completata correttamente;
- la distribuzione delle copie dell'**object storage** sui diversi nodi ove necessario è verificata per via applicativa;
- del **File System** del DPI non viene effettuato backup;
- dell'Area **FTP** non viene effettuato backup;
- il **File System** di SacER è sottoposto a **backup** full a caldo con frequenza settimanale.

Non è quindi possibile far fronte a tutte le possibili anomalie con le stesse procedure, ma sono necessarie procedure specifiche secondo la natura dell'anomalia stessa.

La tabella seguente illustra le misure adottate per risolvere eventuali anomalie, classificate in ragione della collocazione delle informazioni nell'ambito del sistema nel momento in cui si è verificata l'anomalia:

Ambito del sistema	Misure adottate
File System del DPI	Si richiede la ritrasmissione dei SIP, sulla base dell'elenco fornito dalla funzione 'Recupero Studi' del DPI
Area FTP	Si eseguono opportune procedure di quadratura sia in DPI che in PING, guidati da informazioni ottenute tramite un'opportuna interrogazione del Data Base di PING; in caso si evidenzino perdite i file perduti debbono essere ritrasmessi dal <i>Produttore</i>
Data Base	Si effettua la restore tramite le funzioni standard di Oracle dal sito primario o dal sito secondario (nel caso di indisponibilità del DB primario)
Object Storage	Si effettua un controllo di congruenza tra Data Base e Object Storage per via applicativa, e si procede poi al recupero dei Componenti ancora presenti nei Blob temporanei del Data Base
File System di SacER	Si effettua la restore tramite le funzioni standard del file server per tutti i file inseriti nel file system fino all'ultimo back up; per i file inseriti successivamente all'ultimo back up si eseguono opportune procedure di quadratura tra Data Base e file system , che provvedono a riportare il sistema in stato di congruenza.

Ambito del sistema	Misure adottate
	Le procedure di recupero debbono essere eseguite sia sul sito primario che sul secondario.
Data Base del TSM	Si effettua la restore tramite le funzioni standard di DB2 (Data Base di TMS)

[\[Torna al Sommario\]](#)

9.4 Verifica periodica di conformità a normativa e standard di riferimento

Il Responsabile della Funzione Archivistica di Conservazione partecipa attivamente e regolarmente alle iniziative locali e nazionali sulla conservazione digitale e in particolare ai tavoli promossi in materia da AgID e dal MiBACT.

Qualora siano emerse problematiche significative, provvede a diffonderle all'interno di ParER e, se lo ritiene necessario, con il supporto dell'Area Esercizio del Sistema di Conservazione, anche tra gli altri attori della procedura di conservazione.

Le notizie di maggior interesse vengono anche pubblicate sul sito web di ParER.

[\[Torna al Sommario\]](#)

9.5 Audit e gestione delle Non Conformità

ParER effettua periodicamente audit interni sul suo Sistema di Gestione Integrato (SGI), per verificare l'efficacia di policy, procedure e documenti nel rispetto dei requisiti di:

- ISO9001
- ISO27001 con le estensioni ISO27017 e ISO27018
- Accreditamento dei Conservatori secondo le modalità definite da AgID con la circolare n.65/2014
- Qualificazione nel Cloud Marketplace di AgID.

Gli audit interni costituiscono momento fondamentale per il conseguimento e il mantenimento delle certificazioni ISO, dell'accreditamento e della qualificazione.

ParER si impegna a fornire su richiesta dei propri Enti convenzionati (Produttori, Conservatori, Gestori) copia aggiornata delle certificazioni conseguite e della relativa documentazione.

Inoltre, ParER garantisce la disponibilità agli audit sia da parte di Organi di vigilanza sia da parte degli Enti convenzionati.

Dall'altra parte, ParER in tutte le convenzioni con i fornitori di infrastruttura, si riserva la possibilità di effettuare a sua volta Audit mirati allo scopo di verificare il mantenimento delle condizioni contrattuali stabilite.

La procedura riportata nel documento "Audit del SGI" e schematizzata in figura descrive l'insieme di attività e responsabilità legate alla pianificazione, conduzione e documentazione degli Audit di ParER.

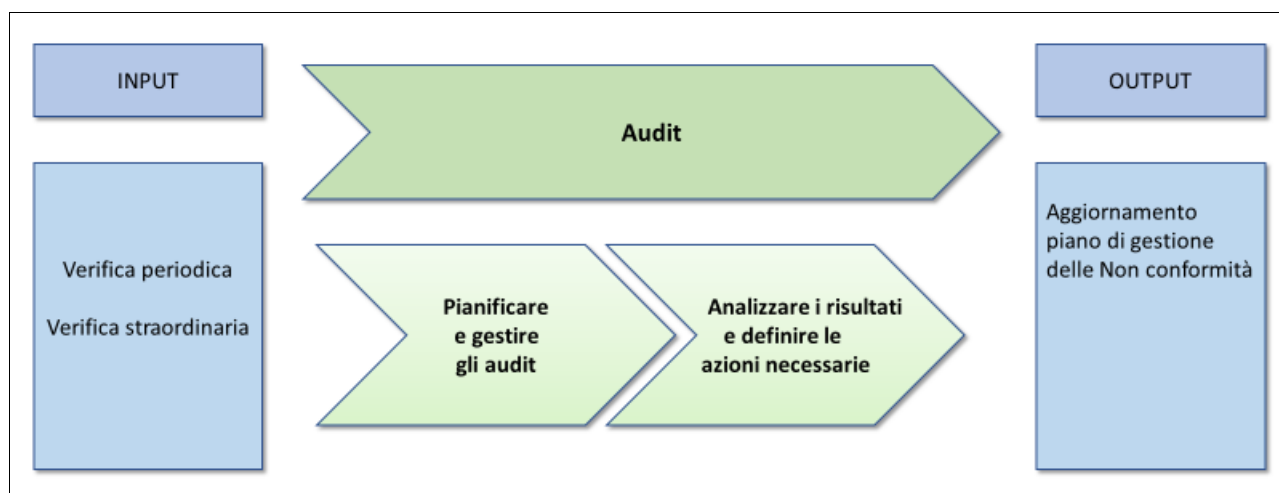


Figura 19 - Procedura di Audit del SGI

Gli Audit vengono eseguiti su base periodica, o in modo straordinario, se i Responsabili lo richiedono, per valutare il grado di applicazione e di efficacia di quanto indicato nella "Politica di sicurezza del sistema di conservazione", nella "Politica per la qualità" e nei documenti ad esso collegati e per orientare la successiva gestione delle Non Conformità riscontrate.

Gli ambiti di verifica sono sia i processi interni che i processi esterni (outsourcing).

Le eventuali non conformità rilevate nei processi di audit vengono gestite seguendo la procedura descritto nel documento "Gestione delle Non Conformità" e schematizzata in figura.

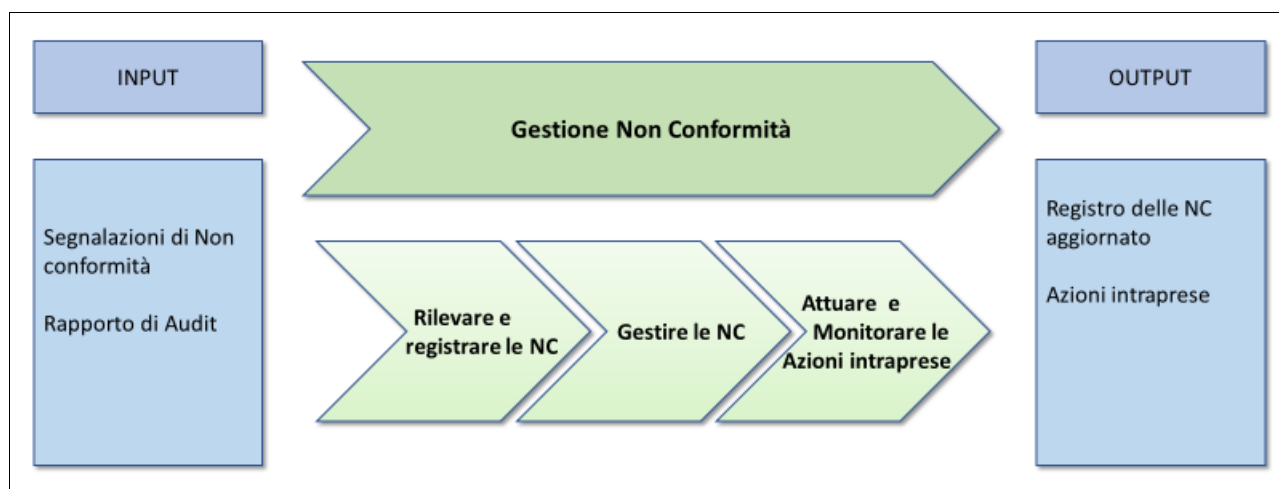


Figura 20 - Gestione delle Non Conformità

Lo scopo della procedura è fornire indicazioni operative per la gestione delle non conformità effettive o potenziali che, verificandosi, inficiano il buon andamento operativo del Servizio di conservazione e per l'attuazione di azioni volte a eliminare le cause delle non conformità stesse.

[\[Torna al Sommario\]](#)

9.6 Controlli di sicurezza

ParER dedica particolare attenzione alla sicurezza del sistema informativo utilizzato nell'ambito del *servizio di conservazione*. Le politiche e gli strumenti adottati a protezione del sistema in esercizio sono descritte nei documenti "Politica sulla sicurezza delle informazioni del servizio di Conservazione" e "Piano della Sicurezza".

La Politica sulla sicurezza è pubblicata e costantemente aggiornata da ParER sul sito web a disposizione di tutti i soggetti interessati e in particolare degli utilizzatori del Sistema di conservazione.

Il rispetto delle regole di sicurezza stabilite da ParER viene periodicamente controllato tramite opportuni test, che vengono svolti da personale esterno specializzato con cadenza periodica prestabilita o anche in maniera estemporanea, qualora il Responsabile della Sicurezza lo richieda.

Di seguito in figura viene rappresentato un quadro di sintesi della procedura relativa alle Verifiche Tecniche e VA/PT (Vulnerability Assessment / Penetration Test), che si implementa nell'ambito dei sistemi e degli applicativi in esercizio.

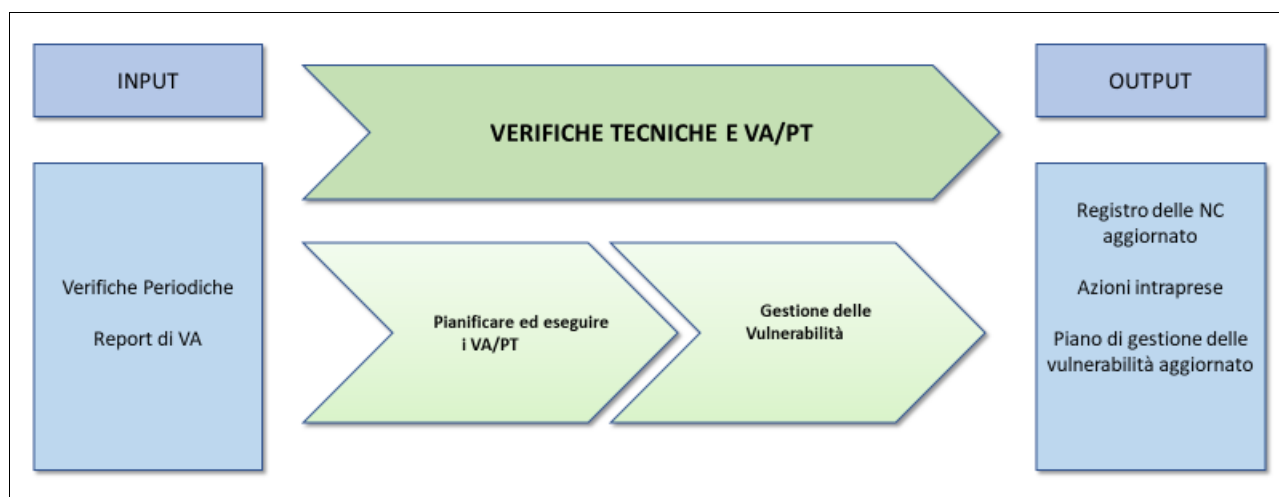


Figura 21 - Procedura di Verifiche Tecniche e VA/PT

I principali obiettivi della procedura sono:

- verificare l'efficacia dei controlli e delle misure di sicurezza implementate dal ParER;
- valutare l'efficacia delle metodologie e delle soluzioni tecniche/tecnologiche adottate;
- fornire indicazioni operative per la correzione delle vulnerabilità;
- innescare le azioni correttive a chiusura delle vulnerabilità;
- verificarne la corretta attuazione.

[\[Torna al Sommario\]](#)

10 TRATTAMENTO DEI DATI PERSONALI

Il nuovo Regolamento europeo sulla protezione dei dati personali (Regolamento (UE) 2016/679 – cd. "GDPR"), ha definito le seguenti figure:

- Titolare del Trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, par. 1, n. 7 GDPR);
- Responsabile del trattamento: la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).

Al Titolare del Trattamento, ai sensi dell'art. 24 del GDPR spetta l'adozione di misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento effettuato è conforme al Regolamento ed in particolare:

- gli interventi normativi necessari per l'adeguamento al GDPR;
- l'attribuzione di funzioni e compiti ai "soggetti attuatori" per gli adempimenti previsti dal GDPR.

Il Responsabile del Trattamento, ai sensi dell'art. 28 del GDPR, è soggetto esterno, con esperienza, capacità e conoscenza necessarie per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento comunitario, anche relativamente al profilo della sicurezza, il quale effettua trattamenti di dati personali per conto del Titolare sulla base di un contratto o da altro atto giuridico che determini la materia del trattamento, la durata, la finalità, le categorie di dati personali trattati, le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

Con deliberazione di Giunta regionale n. 2169 del 20 dicembre 2017, ai sensi dell'art. 37 del GDPR, è stato designato il Responsabile della protezione dei dati (DPO - Data Protection Officer), nella persona del dirigente regionale Dott. Ing. Alessandro Zucchini, specificandone le caratteristiche organizzative e i compiti assegnati. I compiti e le responsabilità del DPO sono stati poi ulteriormente dettagliati nell'allegato A della deliberazione di Giunta regionale n. 1123 del 16 luglio 2018. Tali compiti sono svolti anche per tutte le strutture della Giunta regionale e delle Agenzie e Istituti regionali ai sensi della lettera b), comma 3 bis, art. 1, L.R. 43/2001, compreso quindi IBACN e ParER.

Con successiva deliberazione della Giunta regionale n. 2329 del 22/11/2019 a seguito del collocamento a riposo del Dott. Ing. Alessandro Zucchini dal 1/1/2020 il Responsabile della protezione dei dati (DPO) per le strutture della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna e delle Agenzie e Istituti regionali ai sensi della lettera b), comma 3 bis, art. 1, L.R. 43/2001, compreso quindi IBACN e ParER è stato designato tramite contratto di servizio con la Società LEPIDA S.C.P.A., che lo ha individuato nella persona di Sergio Duretti. Tale designazione esterna del DPO ha durata triennale, salvo mutate condizioni organizzative interne all'Amministrazione che permettano di procedere alla nomina interna del DPO.

Il DPO funge da punto di contatto per l'autorità di controllo per questioni connesse al trattamento dei dati personali.

Con deliberazione del Consiglio Direttivo dell'IBACN n. 54 del 7 dicembre 2018 sono state ridefinite le competenze e le responsabilità in materia di protezione dei dati personali a seguito dell'entrata in vigore del Regolamento (UE) 2016/679 e dell'approvazione da parte della Giunta regionale della deliberazione n. 1123 il 16 luglio 2018.

Nel succitato atto deliberativo l'IBACN è stato individuato quale "Titolare dei trattamenti di dati personali" e il Direttore dell'IBACN quale "Soggetto attuatore" con attribuzione di funzioni e compiti per gli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dall'Ente in esecuzione del regolamento; con riferimento ai "Responsabili del trattamento" detta deliberazione dispone che, attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale, anche in aderenza ai facsimili messi a disposizione dalla struttura della Giunta regionale competente in materia di privacy.

Il Direttore dell'IBACN con propria determinazione dirigenziale n. 355 del 21 dicembre 2018 ha successivamente delegato ai Responsabili di Servizio funzioni e compiti meglio specificati al punto 3 della soprarichiamata deliberazione n. 54/2018.

Con deliberazione del Consiglio Direttivo dell'IBACN n. 38 del 17 dicembre 2019 è stato, tra l'altro, approvato lo schema di atto giuridico con il quale le parti regolano i trattamenti di dati personali necessari e conseguenti alla sottoscrizione dei medesimi (art. 28 GDPR), ed è stato autorizzato il Responsabile del Servizio Polo Archivistico regionale alla sottoscrizione dell'atto giuridico conseguente alla stipula di ciascun accordo/convenzione, quale parte integrante e sostanziale, con cui le parti disciplineranno il trattamento dei dati personali ai sensi del Regolamento (UE) 2016/679, necessari e conseguenti alla sottoscrizione dei medesimi, con possibilità di apportare modifiche che si rendessero eventualmente necessarie nell'ambito dei rapporti negoziali con il Titolare del trattamento, nonché sottoscrivere accordi di diversa formulazione contenenti disposizioni coerenti con lo schema adottato.

Dal quadro organizzativo sopra esposto risulta che il Responsabile del Servizio Polo Archivistico dott. Ing. Marco Calzolari svolge le funzioni ed i compiti di responsabile del trattamento dati personali previsti in materia di privacy correlati alla conservazione digitale.

Con riferimento alla tematica del trattamento dei dati personali, occorre distinguere preliminarmente la categoria più ampia dei dati personali contenuti nei documenti oggetto di conservazione e la categoria dei dati personali degli *Utenti* del servizio di conservazione, trattati per consentire l'accesso al *Sistema di conservazione*.

L'impostazione adottata negli schemi di convenzione con i *Produttori* consiste pertanto nel riconoscimento della titolarità del trattamento di dati personali contenuti nei documenti oggetto di conservazione in capo allo stesso *Produttore* e nella contestuale nomina dell'IBACN quale "Responsabile del trattamento" dei dati personali necessari all'esecuzione della **Convenzione/Accordo** e al compimento degli atti conseguenti.

Di conseguenza, l'IBACN si impegna, nel trattamento dei suddetti dati, ad attenersi alle istruzioni e a svolgere i compiti indicati dall'Ente Produttore, così come meglio definiti nell'Allegato ex art. 28 del GDPR "Accordo Trattamento dati personali", da considerarsi parte sostanziale e integrante di ogni **Convenzione/Accordo** sottoscritta con i *Produttori*.

Coerentemente a quanto espresso, il Responsabile del Servizio Polo Archivistico regionale individuato dagli Enti Produttori, Titolari del trattamento, sulla base di Accordi ex art. 28 del GDPR quale *Responsabile del trattamento*, assume la responsabilità sulla garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e sulla garanzia che il trattamento dei dati affidati dai *Produttori* avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Con precipuo riferimento invece al trattamento dei dati personali degli operatori del servizio di conservazione con livello di abilitazione consultatore, il trattamento dei dati in oggetto ha luogo conformemente a quanto previsto dal GDPR sempre sotto la responsabilità del Responsabile del Servizio Polo Archivistico regionale.

L'archivio logico comprendente i dati degli operatori abilitati alla consultazione di una o più strutture contiene i soli dati obbligatori indispensabili per il rilascio delle credenziali di accesso al sistema e per la corretta gestione del sistema di autorizzazione, nel rispetto di quanto previsto dal sopraindicato GDPR.

L'articolo 35, paragrafo 1, del GDPR prevede che il processo della Valutazione di Impatto sulla Protezione dei Dati (DPIA) sia obbligatorio quando un trattamento di dati personali "*presenti un rischio elevato per i diritti e le libertà delle persone fisiche*"; il soggetto obbligato ad effettuare una DPIA è il titolare del trattamento (nel processo di conservazione quindi il *Produttore*), con il supporto del Responsabile della protezione dei dati (DPO - *Data Protection Officer*), se nominato, e del Responsabile del trattamento eventualmente coinvolto. Considerando la dimensione e la criticità dei documenti conservati, ParER, benché non Titolare, ma Responsabile del trattamento, ha comunque ritenuto opportuno effettuare la DPIA sul trattamento "*Gestione dei dati e dei documenti trasmessi dagli Enti produttori al sistema di conservazione del ParER, ai fini del corretto svolgimento del processo di conservazione (trattamento effettuato nel pubblico interesse)*", identificando le misure opportune per la mitigazione del rischio di violazione dei dati personali, sensibili e giudiziari, con il supporto del DPO dell'IBACN.

[\[Torna al Sommario\]](#)

11 DOCUMENTI DI RIFERIMENTO E ALLEGATI

Si riporta l'elenco dei documenti citati nel presente Manuale con indicazione della collocazione in cui sono rintracciabili.

Documento	Collocazione
Politica della Qualità del servizio di Conservazione	pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it , in "Documentazione"
Modelli dei SIP (Linee guida per la realizzazione dei SIP)	pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it , in "Documentazione"
Modelli dei pacchetti di archiviazione (AIP)	pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it , in "Documentazione"
Specifiche tecniche dei servizi di versamento	pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it , in "Documentazione"
Specifiche tecniche dei servizi di recupero	pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it , in "Documentazione"
Politica sulla sicurezza delle informazioni del servizio di Conservazione	pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it , in "Documentazione"
Piano della Sicurezza	share ParER Doc / Area riservata
Piano di Continuità Operativa	share ParER Doc / Policy
DPIA	Share regionale / Area riservata
Gestione incidenti di sicurezza	share ParER Doc / Procedure / Supporto
Gestione richieste di cambiamento	share ParER Doc / Procedure / Supporto
Progettazione e realizzazione di software applicativo	share ParER Doc / Procedure / Supporto
Gestione dei rilasci	share ParER Doc / Procedure / Supporto
Audit del SGI	share ParER Doc / Procedure / Supporto
Gestione delle Non Conformità	share ParER Doc / Procedure / Supporto
Verifiche tecniche e VA/PT	share ParER Doc / Procedure / Supporto
Registro dei formati	SacER
Gestione utenze	share ParER Doc / Procedure / Realizzazione del Servizio
Procedura di restituzione dell'archivio	share ParER Doc / Procedure / Realizzazione del Servizio
Gestione di richieste e malfunzionamenti	share ParER Doc / Procedure / Supporto

Si riporta l'elenco dei documenti allegati al presente Manuale:

- **Allegato 1 "Normativa e standard di riferimento"**
- **Allegato 2 "Registro dei responsabili"**

[\[Torna al Sommario\]](#)

Comune di Casalgrande

Provincia di Reggio Emilia

SCHEMA DI CONVENZIONE PER LO SVOLGIMENTO DELLA FUNZIONE DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI

tra

1 – Il Comune di Casalgrande P.I. 00284720356 (di seguito denominato Ente produttore), in persona del Vice Segretario Dott.ssa Roberta Barchi nata a Reggio Emilia il 06.02.1968 la quale interviene nel presente atto in forza della delibera n. di G.C. n. 140 del 30.12.2013, esecutiva ai sensi di legge, con la quale si è altresì approvata la presente Convenzione;

e

2 – L'Istituto per i Beni Artistici, Culturali e Naturali della Regione Emilia-Romagna (di seguito anche denominato più brevemente "IBACN"), in persona del Direttore Alessandro Zucchini , domiciliato per la sua carica in Bologna, via Galliera 21, il quale interviene nel presente atto in forza della Deliberazione del Consiglio Direttivo n. 33 del 23/09/2013, esecutiva ai sensi di legge;

PREMESSO CHE

- alla luce della progressiva digitalizzazione dell'attività amministrativa vi è interesse ad assicurare alle pubbliche amministrazioni del territorio sistemi sicuri e giuridicamente validi per conservare documenti digitali, nonché supporto tecnico archivistico di varia natura per la gestione dei documenti informatici;
- la Giunta della Regione Emilia-Romagna ha approvato, con delibe-

ra n. 601 del 28 aprile 2008, il “Programma operativo 2008” al Piano telematico dell’Emilia-Romagna 2007-2009, in attuazione delle “Linee guida per la predisposizione del Piano Telematico dell’Emilia-Romagna - PITER (2007-2009), ai sensi dell’art. 6 della legge regionale n. 11 del 24 maggio 2004”, approvate con delibera dell’Assemblea legislativa regionale n. 111 del 2 maggio 2007, in cui si prevede tra le linee di intervento una specifica iniziativa dedicata alla gestione documentale, nell’ambito della quale è compresa la realizzazione del Polo Archivistico della Regione Emilia-Romagna (PARER), che si propone di conservare in un sistema sicuro ed evoluto il patrimonio documentale degli enti dell’intero territorio regionale, nel pieno rispetto della normativa vigente e degli standard proposti a livello internazionale;

- la Giunta della Regione Emilia-Romagna ha approvato, con delibera n. 529 del 6 maggio 2013, il “Programma operativo 2013” al Piano telematico dell’Emilia-Romagna 2011-2013, in attuazione delle “Linee guida per il Piano telematico dell’Emilia-Romagna 2011-2013: un nuovo paradigma di innovazione ai sensi dell’articolo 6 della legge regionale n. 11 del 2004” approvate con delibera dell’Assemblea legislativa regionale n. 52 del 27 luglio 2011, in cui si prevede tra le linee di intervento, in continuità con i risultati dei precedenti Piani Telematici, l’archiviazione e la conservazione digitale
- la legge regionale dell’Emilia-Romagna 24 maggio 2004, n. 11 e s.m.i. (recante “Sviluppo regionale della società dell’informazione”) ha stabilito all’art. 2, comma 4bis, che: “La Regione, anche in collaborazione con le altre pubbliche amministrazioni interessate, favorisce altresì lo svi-

luppo integrato della conservazione digitale dei documenti informatici e, nel rispetto dei principi di efficacia, efficienza ed economicità, svolge le funzioni di archiviazione e conservazione digitale dei documenti informatici secondo quanto disposto dall'articolo 2, comma 1, lettera f bis) della legge regionale 10 aprile 1995, n. 29 (Riordinamento dell'Istituto dei beni artistici, culturali e naturali della Regione Emilia-Romagna”;

- ai sensi della legge regionale dell'Emilia-Romagna n. 29/1995, così come modificata per ultima dalla legge regionale n. 17/2013, l'Istituto per i Beni Artistici, Culturali e Naturali della Regione Emilia-Romagna svolge la funzione di “archiviazione e conservazione digitale dei documenti informatici anche a rilevanza fiscale, con le modalità previste dalle disposizioni vigenti, prodotti o ricevuti dalla Regione e dagli altri soggetti di cui all'articolo 19, comma 5, lettera a) della legge regionale 24 maggio 2004, n. 11 nonché, mediante apposita convenzione, dei documenti informatici prodotti o ricevuti dai soggetti di cui all'articolo 19, comma 5, lettera b) della medesima legge e da altri soggetti pubblici”;

- la Regione Emilia-Romagna, con delibera di Giunta n. 877 del 22 giugno 2009 ha attivato il Servizio Polo Archivistico Regionale dell'Emilia-Romagna (di seguito denominato più brevemente “ParER”) presso l'IBACN e ha autorizzato l'IBACN a costituire il Servizio Polo Archivistico Regionale della Regione Emilia-Romagna con la responsabilità dello svolgimento dei processi di conservazione sostitutiva e di riversamento sostitutivo dei documenti informatici della Regione e degli altri Enti convenzionati e il compito di promuovere l'adesione degli Enti del sistema regionale al Polo archivistico regionale e di supportare l'azione dei respon-

sabili del protocollo informatico presso gli Enti produttori per la messa a punto degli strumenti archivistici, organizzativi e software per le esigenze di produzione e conservazione dei documenti digitali, anche per l'adeguamento al sistema di conservazione digitale;

- ai sensi del successivo art. 43 del Codice dell'Amministrazione Digitale: “I documenti informatici, di cui è prescritta la conservazione per legge o regolamento,(...) sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell' articolo 71”;
- la deliberazione di Consiglio Direttivo dell'IBACN n. 29 adottata in data 8 luglio 2013, esecutiva ai sensi di legge, ha approvato la Convenzione Operativa tra l'IBACN, l'Agenzia per l'Italia Digitale e l'Archivio Centrale dello Stato per la definizione di un modello nazionale di riferimento per la realizzazione di Poli conservativi;
- in virtù di quanto stabilito nella sopraindicata Convenzione Operativa, finalizzata alla definizione di un modello tecnologico e organizzativo per la conservazione, l'archiviazione e l'accesso ai documenti amministrativi informatici, e ogni altro oggetto digitale, prodotti dalle Pubbliche Amministrazioni, in grado di garantire nel tempo l'integrità, la provenienza e la reperibilità dei documenti stessi e l'economicità dell'azione amministrativa, l'Archivio Centrale dello Stato e l'Agenzia per l'Italia Digitale hanno manifestato la volontà di avvalersi dell'esperienza dell'IBACN, maturata nel Polo Archivistico Regionale, per sperimentare le procedure e le modalità operative da quest'ultimo adottate, ai fini della definizione del suddetto modello;

- l'IBACN ha provveduto a inviare all'Agenzia per l'Italia Digitale – con comunicazione prot. IB/2012/5149 del 21 dicembre 2012, successivamente integrata con comunicazione prot. IB/2012/5161 di pari data - istanza di accreditamento, ai sensi della circolare 29 dicembre 2011 n. 59, come soggetto pubblico che svolge attività di conservazione dei documenti informatici, conformemente a quanto previsto dall'art. 44-bis del Codice dell'Amministrazione Digitale;
- L'Ente produttore è da tempo impegnato nella progressiva digitalizzazione dei documenti e intende organizzare in modo efficace e a lungo termine la loro conservazione, ma ritiene non economico dotarsi autonomamente delle complesse strutture per una conservazione a lungo termine dei documenti informatici;
- ai sensi dell'art. 15 della legge 7 agosto 1990, n. 241 e s.m.i. “le pubbliche Amministrazioni possono sempre concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune”;
- è pertanto interesse dell'Ente produttore avvalersi, per la conservazione digitale dei documenti informatici e di altri oggetti digitali, di ParER, quale soggetto in grado di fornire idonee garanzie di sicurezza ed efficacia e che dispone della strumentazione tecnica necessaria e di personale adeguato allo scopo, stipulando apposita convenzione ai sensi dell'art. 2, comma 1, lettera f-bis, della legge regionale n. 29/1995 e s.m.i.;

Visto il Codice dell'Amministrazione Digitale, approvato con Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni e le relative regole tecniche;

Visto l'Accordo per il coordinamento delle attività in tema di conservazione dei documenti informatici sottoscritto fra la Soprintendenza Archivistica per l'Emilia-Romagna (MIBACT) e l'IBACN in data 11 maggio 2010 e successivamente prorogato e aggiornato con atto scritto delle parti, che approva il presente schema di Convenzione;
si conviene e si stipula quanto segue:

CAPO I

DISPOSIZIONI GENERALI

Art. 1

(Oggetto della convenzione)

1. L'Ente produttore affida all'IBACN la conservazione dei propri documenti informatici e delle loro aggregazioni documentali informatiche con i metadati a essi associati.
2. L'attività di conservazione svolta dall'IBACN si ispira ai principi indicati dall'art. 29 del Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i., recante il "Codice dei beni culturali e del paesaggio", di coerente, coordinata e programmata attività di studio, prevenzione, e manutenzione, e si ritiene in grado di soddisfare gli obblighi in capo all'Ente produttore di conservazione sostitutiva di documenti informatici e in prospettiva di conservazione e ordinamento dell'archivio nella sua organicità.
3. L'IBACN, nel rispetto delle norme di legge, è individuato come responsabile della conservazione degli oggetti informatici trasferiti in base alla presente Convenzione.
4. L'Ente produttore può inoltre affidare all'IBACN altri oggetti informatici, frutto di attività di digitalizzazione.

Art. 2 (Finalità)

1. La presente Convenzione ha le seguenti finalità:

- creare le condizioni giuridico-organizzative per la conservazione dei documenti informatici con le loro aggregazioni e metadati, nel rispetto delle finalità istituzionali degli Enti;
- garantire economicità, efficienza ed efficacia alla funzione di conservazione dei documenti informatici con le loro aggregazioni e metadati;
- garantire una elevata qualità nella fornitura del servizio anche a favore di eventuali utenti esterni per l'esercizio del diritto di accesso ai sensi della disciplina sull'accesso ai documenti amministrativi e del Decreto Legislativo 30 giugno 2003 n. 196 e s.m.i., recante il "Codice in materia di protezione dei dati personali" o, in futuro, per ricerche storiche.

CAPO II

FUNZIONAMENTO E RESPONSABILITÀ

Art. 3 (Obblighi delle Parti)

1. L'IBACN, tramite il ParER, si impegna alla conservazione dei documenti trasferiti e ne assume la funzione di responsabile della conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione.

2. L'Ente produttore si impegna a depositare i documenti informatici e le loro aggregazioni nei modi e nelle forme definite dall'IBACN, tramite il ParER, garantendone l'autenticità e l'integrità nelle fasi di produzione e di archiviazione corrente, effettuata nel rispetto delle norme sulla produzione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utiliz-

zando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente.

3. L'Ente produttore si impegna a depositare e mantenere aggiornati, nei modi e nelle forme definite dall'IBACN, tramite il ParER, gli strumenti di ricerca e gestione archivistica elaborati a supporto della formazione dei documenti e della tenuta degli archivi.

4. L'Ente produttore mantiene la titolarità e la proprietà dei documenti depositati.

5. Entrambi gli Enti dichiarano che le attività previste dalla presente Convenzione saranno effettuate nel rispetto dei principi di tutela da parte dello Stato dei beni archivistici come beni culturali e nel rispetto di quanto stabilito dal MIBACT.

6. Il responsabile della conservazione è individuato nella figura del responsabile della conservazione del ParER.

Art. 4 (Servizi offerti)

1. I servizi offerti dall'IBACN tramite il ParER riguardano la conservazione digitale, la restituzione per la consultazione o l'esibizione dei documenti a fini di accesso o per scopi storici, la consulenza e il supporto tecnico-archivistico.

2. I servizi di conservazione digitale e di restituzione dei documenti a fini di accesso e ricerca, saranno erogati in base al Manuale di conservazione - redatto dal ParER e verificato dalla Soprintendenza Archivistica per l'Emilia-Romagna per quanto concerne il rispetto della normativa sulla tutela degli archivi e dei singoli documenti come beni culturali - e sulla base delle specifiche tecniche contenute nel Disciplinare Tecnico concorda-

to tra le Parti sulla base di uno schema generale definito in collaborazione con la Soprintendenza Archivistica per l'Emilia-Romagna.

3. Il Disciplinare Tecnico definisce le specifiche operative e le modalità di descrizione e di versamento nel sistema di conservazione digitale delle tipologie di documenti oggetto di conservazione. E' redatto a cura dei referenti e responsabili di riferimento delle Parti per l'erogazione dei servizi per le diverse tipologie di documenti, indicati in esso. E' formato da specifiche parti relative alle diverse tipologie di documenti oggetto di conservazione. Potrà essere aggiornato in caso di modifiche nelle modalità di erogazione dei servizi, anche a seguito di eventuali modifiche normative.

4. Viene garantita la restituzione in ogni momento dei documenti trasferiti e conservati presso il ParER e delle relative evidenze informatiche che comprovano la corretta conservazione degli stessi, fornendo gli elementi necessari per valutare l'autenticità e la validità giuridica degli stessi.

5. L'IBACN, tramite il ParER, si impegna ad adeguare il servizio di conservazione alle future modifiche normative.

6. Il servizio di conservazione è finalizzato alla conservazione dei documenti informatici e delle loro aggregazioni documentali con i metadati a essi associati, garantendo il mantenimento nel tempo delle caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, accessibilità, riproducibilità e intelligibilità all'interno del contesto proprio di produzione e archiviazione e preservando il vincolo originario per mantenere l'archivio nella sua organicità.

7. L'IBACN, tramite il ParER, garantisce la gestione e l'accesso agli oggetti conservati secondo le norme vigenti in tema di tutela dei beni cultu-

rali e dei dati personali, garantendo l'effettiva attuazione di eventuali procedure di selezione e scarto predisposte dall'Ente produttore e approvate dalla Soprintendenza Archivistica per l'Emilia-Romagna.

8. Nella prospettiva della costituzione e accrescimento, nei tempi e nei modi previsti dalla normativa, dell'archivio storico dell'Ente produttore, l'IBACN, tramite il ParER, provvederà – sulla base di specifico progetto da concordare con l'Ente produttore e con la Soprintendenza Archivistica per l'Emilia-Romagna – all'inventariazione del patrimonio documentario digitale conservato, prevedendo gli opportuni collegamenti logici e descrittivi tra documentazione informatica e documentazione cartacea.

9. L'IBACN, tramite il ParER, in accordo con la Soprintendenza Archivistica per l'Emilia-Romagna, su richiesta dell'Ente produttore, provvederà a erogare servizi di supporto tecnico-archivistico strettamente correlati ai servizi di conservazione quali:

- a) supporto nella redazione e nell'applicazione degli strumenti di gestione archivistica (titolario, massimario di scarto, manuale di gestione, piano di conservazione);
- b) consulenza per la re-ingegnerizzazione dei sistemi di gestione degli archivi correnti (flussi documentali, modalità di comunicazione, diritti di accesso e di visibilità, ecc.);
- c) supporto nell'ordinamento e descrizione degli archivi;
- d) formazione/addestramento archivistico dei responsabili del Protocollo informatico, dei flussi documentali e degli archivi, nonché degli operatori tecnici in relazione alle attività connesse ai servizi forniti dal ParER;
- e) supporto tecnico informatico sui formati digitali e l'utilizzo della

firma digitale.

Art. 5 (Accesso ai documenti conservati presso il ParER)

1. L'accesso ai documenti conservati presso il ParER avviene con i medesimi tempi e modalità previsti per i documenti conservati presso l'Ente produttore, che mantiene la responsabilità del procedimento ai sensi del regolamento adottato per l'accesso ai documenti amministrativi e delle norme sull'accesso vigenti nel tempo.
2. Qualora la domanda di accesso venga presentata al ParER, quest'ultimo provvederà a trasmetterla immediatamente all'Ente produttore. Il ParER è tenuto a fornire la propria collaborazione, se necessario, per il pieno rispetto dei tempi e delle modalità di accesso previste dalle norme.
3. Il ParER, qualora venga richiesto dall'Ente produttore, può consentire direttamente l'accesso a documenti soggetti a obblighi di pubblicazione, nel rispetto della normativa vigente.
4. Possono essere stipulati appositi accordi operativi fra i responsabili delle Parti della presente Convenzione per definire con maggior dettaglio modalità e obblighi reciproci, in particolare per quanto riguarda l'eventuale produzione di copie conformi cartacee, nel rispetto del principio per cui la copia conforme cartacea viene effettuata, se richiesta, dal soggetto che stampa il documento cartaceo traendolo dall'originale informatico.

CAPO III

RAPPORTI TRA SOGGETTI CONVENZIONATI

Art. 6 (Strumenti di consultazione e controllo)

1. Il ParER consente all'Ente produttore l'accesso ai propri sistemi per verificare il corretto svolgimento dell'attività di conservazione e per con-

sultare ed eventualmente estrarre i documenti depositati e le prove di conservazione, secondo le modalità indicate nel Manuale di conservazione.

2. L'Ente produttore concorda con il ParER i nominativi e le funzioni del personale abilitato allo svolgimento della funzione di cui al comma 1.

3. Il ParER consente alla Soprintendenza Archivistica per l'Emilia-Romagna l'accesso ai propri sistemi per rendere possibile e operativo lo svolgimento della funzione di vigilanza e tutela prevista dalla legge ed effettuare le opportune verifiche sul corretto svolgimento dell'attività di conservazione.

Art. 7 (Oneri a carico delle Parti)

1. I servizi oggetto della presente Convenzione sono erogati dall'IBACN, tramite il ParER, gratuitamente all'Ente produttore.

2. Non sono previsti altri oneri a carico delle Parti per il periodo di durata della presente Convenzione.

Art. 8 (Trattamento dei dati personali)

1. Conformemente a quanto stabilito dall'art. 44, comma 1-bis, del Codice dell'Amministrazione digitale, il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del Decreto Legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza.

2. L'Ente produttore è titolare del trattamento dei dati personali conte-

nuti nei documenti dallo stesso prodotti. Al fine di consentire l'erogazione dei servizi di cui al precedente art. 4, l'Ente produttore nomina l'IBACN quale responsabile esterno del trattamento dei dati personali necessari all'esecuzione della presente Convenzione e al compimento degli atti conseguenti.

3. L'IBACN accetta e si impegna, nel trattamento dei suddetti dati, ad attenersi alle istruzioni e a svolgere i compiti indicati dall'Ente produttore nell'Allegato A alla presente Convenzione, di cui costituisce parte integrante e sostanziale.

4. Alla scadenza della presente Convenzione, nell'ipotesi di recesso di una delle Parti ovvero al termine, per qualsivoglia causa, di validità della stessa Convenzione, la designazione a responsabile esterno del trattamento dei dati personali decade automaticamente.

Art. 9 (Decorrenza e durata della convenzione)

1. La scadenza della presente Convenzione è fissata al 31 dicembre 2033, fermo restando quanto previsto per le date di effettiva attivazione dei servizi al successivo comma.

2. Le date di effettiva attivazione dei servizi di conservazione delle diverse tipologie di documenti informatici sono definite dai referenti e responsabili di riferimento delle Parti di cui all'art. 4, comma 3 e sono indicate nelle specifiche parti del Disciplinare Tecnico.

Art. 10 (Recesso)

1. E' sempre possibile il recesso dalla presente Convenzione su richiesta di una della Parti, informata la Soprintendenza Archivistica per l'Emilia-Romagna.

2. Il recesso avrà effetto decorsi 90 giorni dalla comunicazione. In tal caso, l'IBACN, tramite il ParER, è tenuto a riversare i documenti conservati, con i metadati a essi associati e le eventuali aggregazioni documentali informatiche con tutte le prove dei processi di conservazione nel sistema indicato dall'Ente produttore, secondo modalità e tempi indicati nel Disciplinare Tecnico.

3. Nel caso di recesso da parte dell'IBACN, il ParER è tenuto al mantenimento nel proprio sistema di conservazione dei documenti conservati, con i metadati a essi associati e le eventuali aggregazioni documentali informatiche con tutte le prove dei processi di conservazione fino alla comunicazione da parte dell'Ente produttore dell'effettiva messa a disposizione del sistema di conservazione in cui effettuare il riversamento di cui al precedente comma.

4. In caso di recesso, l'IBACN tramite il ParER provvederà solo al termine del riversamento e solo dopo le opportune verifiche - effettuate da entrambe le Parti e svolte di concerto tra le stesse - di corretto svolgimento del riversamento stesso, all'eliminazione dal proprio sistema di conservazione di tutti gli oggetti riversati e di tutti gli elementi riferiti all'Ente produttore.

Art. 11 (Interpretazione ed esecuzione della Convenzione)

1. Per le eventuali controversie concernenti l'interpretazione o l'esecuzione della presente Convenzione, l'esclusiva competenza è quella del Foro di Bologna. E' espressamente escluso il ricorso all'arbitrato.

CAPO IV

DISPOSIZIONI FINALI

Art. 12 (Disposizioni di rinvio)

1. Per quanto non previsto nella presente Convenzione, potrà rinviarsi alle norme del codice civile applicabili e alle specifiche normative vigenti nelle materie oggetto della Convenzione.
2. Eventuali modifiche o deroghe alla Convenzione potranno essere apportate dall'Ente produttore e dall'IBACN soltanto con atti aventi le medesime formalità della medesima Convenzione.

Art. 13 (Esenzioni per bollo e registrazione)

1. Per tali adempimenti, si osserveranno le norme di cui al D.P.R. 26 ottobre 1972, n. 642, allegato B, articolo 16, e al D.P.R. 26 aprile 1986, n. 131.

p. Il Comune di Casalgrande

Dott.ssa Roberta Barchi

.....

(firmato digitalmente)

p. L'Istituto per i Beni Artistici, Culturali e Naturali della Regione Emilia-Romagna

Il Direttore

Alessandro Zucchini

.....

(firmato digitalmente)

Allegato A

Oggetto: istruzioni e individuazione dei compiti ai quali deve attenersi il responsabile esterno al trattamento di dati personali.

L'IBACN, in qualità di responsabile esterno del trattamento di dati personali per conto dell'Ente produttore, ai sensi dell'art. 8 della presente Convenzione, si impegna ad attenersi alle istruzioni impartite dal titolare e svolgere i compiti previsti dal Decreto Legislativo 30 giugno 2003 n. 196 e s.m.i., recante il "Codice in materia di protezione dei dati personali". In particolare, l'IBACN si impegna a:

- a) adempiere l'incarico attribuito adottando idonee e preventive misure di sicurezza, con particolare riferimento a quanto stabilito dal D. Lgs. n. 196/2003 e dall'Allegato B del D. Lgs. n. 196/2003;
- b) dare riscontro oralmente, anche tramite propri incaricati, alle richieste dell'interessato di cui ai commi 1 e 2 dell'art. 7 del D. Lgs. n. 196/2003, con le modalità indicate nell'art. 9 del suddetto decreto;
- c) trasmettere, con la massima tempestività, le istanze dell'interessato per l'esercizio dei diritti di cui agli artt. 7 e ss. del D. Lgs. n. 196/2003, che necessitino di riscontro scritto, all'Ente produttore per consentire allo stesso di dare riscontro all'interessato nei termini stabiliti dal suddetto decreto; di fornire inoltre all'Ente produttore la massima assistenza, necessaria per soddisfare tali richieste, nell'ambito dell'incarico affidatogli;

d) individuare gli incaricati del trattamento dei dati personali, comunicare i relativi nominativi all'Ente produttore nel caso in cui quest'ultimo ne faccia richiesta, nonché fornire agli stessi incaricati istruzioni per il corretto trattamento dei dati;

e) sovrintendere e vigilare sull'attività degli incaricati e sull'attuazione delle istruzioni impartite, nonché, in generale, sul rispetto della normativa in materia di tutela dei dati personali, provvedendo personalmente alla formazione degli incaricati medesimi in materia di protezione dei dati personali;

f) consentire al Titolare, dandogli piena collaborazione, verifiche periodiche tramite il responsabile dell'Ente produttore delle operazioni di trattamento dei dati personali e, limitatamente ai casi in cui il trattamento dei dati avvenga con l'utilizzo di strumenti informatici, tramite l'Amministratore di sistema dell'Ente produttore;

g) attestare, qualora l'incarico affidato ricomprenda l'adozione di misure minime di sicurezza e su specifica richiesta dell'Ente produttore, la conformità degli interventi alle disposizioni di cui alla misura 25 dell'Allegato B del D. Lgs. n. 196/2003 e trasmettere tale attestazione all'Ente produttore richiedente;

h) garantire altresì tutte le misure e gli accorgimenti prescritti al Titolare dei trattamenti effettuati con strumenti elettronici relativamente alle attri-

buzioni delle funzioni di amministratore di sistema (conformemente a quanto previsto dal provvedimento del Garante sulla Privacy del 27 novembre 2008) e rendere disponibile all'Ente Produttore, in qualsiasi momento, su espressa richiesta del medesimo, l'elenco degli Amministratori di sistema che accedono a informazioni di titolarità dell'Ente Produttore, gestiti dall'IBACN tramite il Servizio Polo Archivistico Regionale.



GRUPPO FINMATICA

Registro di Emergenza

Manuale utente

versione 1.0.0.0

www.gruppofinmatica.it

INDICE

1 Registro di emergenza	3
1.1 Prerequisiti	3
1.2 Configurazione applicazione “Gestione Protocollo di Emergenza”	4
1.2.1 Conessione al DB	4
1.2.2 Importazione Dizionari	5
1.3 Modalità operativa	6
1.3.1 Avvio client di emergenza	6
1.3.2 Allineamento Dati con l’Applicativo Prisma	6
1.3.3 Inizio Emergenza	6
1.3.4 Inserimento Protocolli in emergenza	7
1.3.5 Chiusura emergenza	10
1.3.6 Invio Dati	10
1.3.7 Prisma: gestione protocollo di emergenza	12

1 Registro di emergenza

L'applicativo integra una specifica procedura per gestire i protocolli di emergenza. Attraverso un'apposita applicazione vengono raccolte le informazioni da inviare al sistema al termine del periodo di emergenza. L'applicazione dedicata viene fornita in fase di start-up del sistema; è possibile richiederne una copia tramite il servizio di Assistenza Tecnica.

1.1 Prerequisiti

Ad ogni unità che può protocollare in emergenza è associato UN solo registro di emergenza aperto nell'anno in corso.

È importante che sia stato codificato un registro di emergenza collegato all'unità indicata in fase di caricamento dei dati (vedi paragrafi successivi) perché in questo modo il sistema "incrocia" il registro di emergenza attivo per l'unità di appartenenza indicata in fase di richiesta dei parametri.

Per l'inserimento del registro di emergenza associato all'unità è necessario accedere all'area di lavoro Amministrazione, all'interno della voce Tipi_Registro, e cliccare il pulsante "Crea Doc". Verrà proposta la maschera seguente:

DocumentView - Internet Explorer

Registra Salva Apri nuovo anno Chiudi Registro

Tipo Registro

Dati

Codice	EMER		
Descrizione	REGISTRO DI EMERGENZA EDI		
Automatico	NO	Q.ta max	
Anno	2020	Aperto	SI
Ultima Data	01/01/2020	Ultimo numero	70
Da protocollare	☐ NO ☒ SI		
Registro di Emergenza	☐ NO ☒ SI		
Unità di Emergenza	A.F.(AFFARI GENERALI)		

È quindi necessario compilare i campi, specificando tramite l'ultima voce che si sta creando un Registro di Emergenza, e per quale unità, selezionandola dal menu a tendina contestuale.

1.2 Configurazione applicazione “Gestione Protocollo di Emergenza”

Ogni utente abilitato ha quindi a disposizione sul proprio PC il file “emergenza.bat”, lanciando il quale verrà aperta l’applicazione, la quale si presenta come segue:

[illegible]

1.2.1 Conessione al DB

Dalla voce di menu Impostazioni -> Connessione è possibile configurare la stringa di connessione al database applicativo, necessario per allineare le informazioni:

Connessione al database remoto

Impostazioni di connessione

Database: jdbc:oracle:thin:@10.97.11.28:1521:ORCL

User AD4: AD4 Password AD4: ●●●

User AGSPR: AGSPR Password AGSPR: ●●●●●

Server Web: http://test-agspr-as02

Ottica: IST

Test Conn. Salva Chiudi

La stringa di connessione al server che l'utente deve specificare per poter scaricare i dizionari, è specifica di ogni installazione, e riferisce al database applicativo. Si invita a far riferimento ai Sistemi Informativi dell'Ente o all'Assistenza Tecnica per maggiori informazioni.

1.2.2 Importazione Dizionari

Per poter utilizzare l'applicazione è necessario procedere al caricamento dei dati memorizzati nei Dizionari dell'applicativo Prisma – Gestione Protocollo e Flussi Documentali, selezionando dal menu Impostazioni la voce Importa Dizionari e compilando la maschera con i dati "Nominativo", "Codice Unità":

Importa dati

Importa Dati

Server: jdbc:oracle:thin:@10.97.11.28:1521:ORCL

Ottica: IST

Nominativo: CECILIOT

Codice Unità: A04.01

Importa Chiudi

In particolare:

NOMINATIVO: user di accesso dell'utente al sistema di protocollo

CODICE UNITÀ: codice dell'unità che protocolla in emergenza (il codice si ricava dall'applicativo di struttura organizzativa), codificata nel registro di emergenza.

Questa funzione allinea i dati relativi a Tipo Documento, Classificazione e Struttura Organizzativa (unità di smistamento), Tipi di Spedizione (Mod. Rich. /Sped.)

1.3 Modalità operativa

Al termine dell'emergenza, ovvero dell'impossibilità all'utilizzo dell'applicativo di protocollo Prisma, l'utente protocollatore dovrà eseguire i passi illustrati in questa sezione.

1.3.1 Avvio client di emergenza

L'utente che può protocollare, avvia l'applicazione tramite il file "emergenza.bat", presente sul proprio pc.

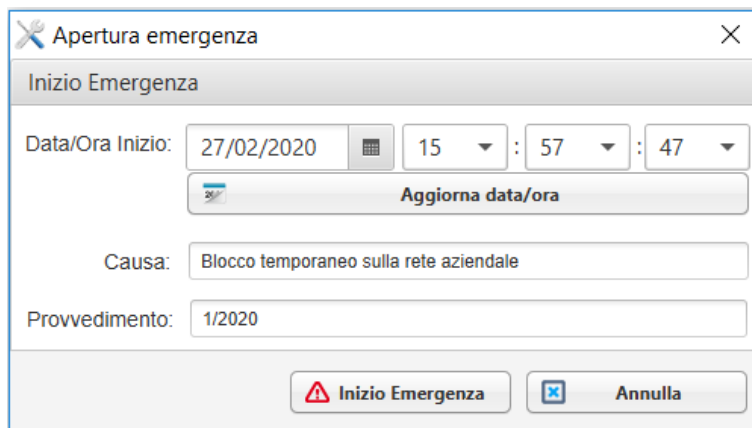
1.3.2 Allineamento Dati con l'Applicativo Prisma

Al primo utilizzo del registro di emergenza l'utente deve procedere al caricamento dei dati memorizzati nei Dizionari dell'applicativo Prisma – Gestione Protocollo e Flussi Documentali come riportato al paragrafo 1.2.2.

1.3.3 Inizio Emergenza

L'utente inizia una nuova emergenza cliccando il pulsante "Inizia Emergenza"  sulla maschera principale.

Nella finestra "Apertura Emergenza", compila i dati richiesti:

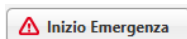


In particolare:

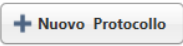
DATA/ORA INIZIO: Data e ora inizio emergenza; tramite il pulsante  è possibile valorizzare data/attuale, in alternativa editare i campi manualmente.

CAUSA: Motivo apertura registro di emergenza.

PROVVEDIMENTO: Numero/Descrizione del Provvedimento.

Il protocollatore deve cliccare il pulsante "Inizio Emergenza"  e confermare l'inizio emergenza al messaggio che appare a video: sulla maschera principale viene riportata in verde la dicitura "EMERGENZA APERTA" con i dettagli data/ora inizio emergenza, Registro e Prossimo Numero del registro di emergenza:

1.3.4 Inserimento Protocolli in emergenza

Tramite il pulsante “Nuovo Protocollo”  l’utente crea un protocollo; è possibile crearne quanti necessari alla gestione della situazione di emergenza.

Protocollo di emergenza	
Dati Protocollo Anno: 2020 Numero: Data: 27/02/2020 Registro: REGISTRO DI EMERGENZA EDI Ufficio di Protocollo: A04.01 Utente di Protocollo: TSUPERUSER	Dati Documento Movimento *: <i>filtro tipi documento ↵</i> Tipo Documento: Oggetto *: <i>filtro classificazioni ↵</i> Classificazione: Fascicolo Anno: Fascicolo Numero:
Dati Movimento Mod. Ric. / Sped.: Data Arrivo / Sped.: : : Tipo Anagrafica: ☒ Persona ☐ Amministrazione / Impresa Cognome *: Nome: Numero Doc Esterno: Data Doc Esterno:	Dati Smistamento Tipo Smistamento: <i>filtro unità ↵</i> Smistamento:
Salva Chiudi	

I dati minimi sono: “Movimento”, “Oggetto”.

Se non vengono compilati questi campi viene restituito un messaggio, al momento del salvataggio, che indica l’obbligo dell’inserimento del valore per la registrazione.

I campi con l’icona sulla destra, sono tipologie di dato con elenchi di valori possibili tra cui è possibile selezionare il desiderato; è sufficiente cliccare sul campo per visualizzare l’elenco.

Sono disponibili dei campi “Filtro” nei quali è possibile digitare stringa di testo al fine di delimitare la ricerca dei valori disponibili per la tipologia di dato: verranno estrapolati solo quelli che contengono la stringa digitata; ad esempio “filtro unità”, digitando “AREA”, l’elenco dei valori proporrà solo le unità che contengono tale parola:

Protocollo di emergenza			
Dati Protocollo		Dati Documento	
Anno: 2020	Numero:	Data: 27/02/2020	
Registro:	REGISTRO DI EMERGENZA EDI		
Ufficio di Protocollo:	A04.01		
Utente di Protocollo:	TSUPERUSER		
		Movimento *:	
		filtro tipi documento ↵	
		Tipo Documento:	
		Oggetto *:	
		filtro classificazioni ↵	
		Classificazione:	
		Fascicolo Anno:	
		Fascicolo Numero:	
Dati Movimento		Dati Smistamento	
Mod. Ric. / Sped.:			
Data Arrivo / Sped.:			
Tipo Anagrafica:	☒ Persona ☐ Amministrazione / Impresa		
Cognome *:			
Nome:			
Numero Doc Esterno:			
Data Doc Esterno:			
		Tipo Smistamento:	
		filtro unità ↵	area
		Smistamento:	
		AREA ADULTI AREA ANZIANI AREA DISABILI AREA MINORI	
		Salva Chiudi	

I campi obbligatori cambiano a seconda del tipo di movimento selezionato

- INTERNO: **Oggetto, Tipo Smistamento** (Competenza o Conoscenza), **Smistamento** (Unità di smistamento selezionabile dall'elenco delle unità presenti in Struttura Organizzativa).
- PARTENZA: **Oggetto, Cognome / Denominazione** (anagrafica destinatario).
- ARRIVO: **Oggetto, Cognome** (anagrafica destinatario), **Tipo Smistamento** (Competenza o Conoscenza), **Smistamento** (Unità di smistamento selezionabile dall'elenco delle unità presenti in Struttura Organizzativa).

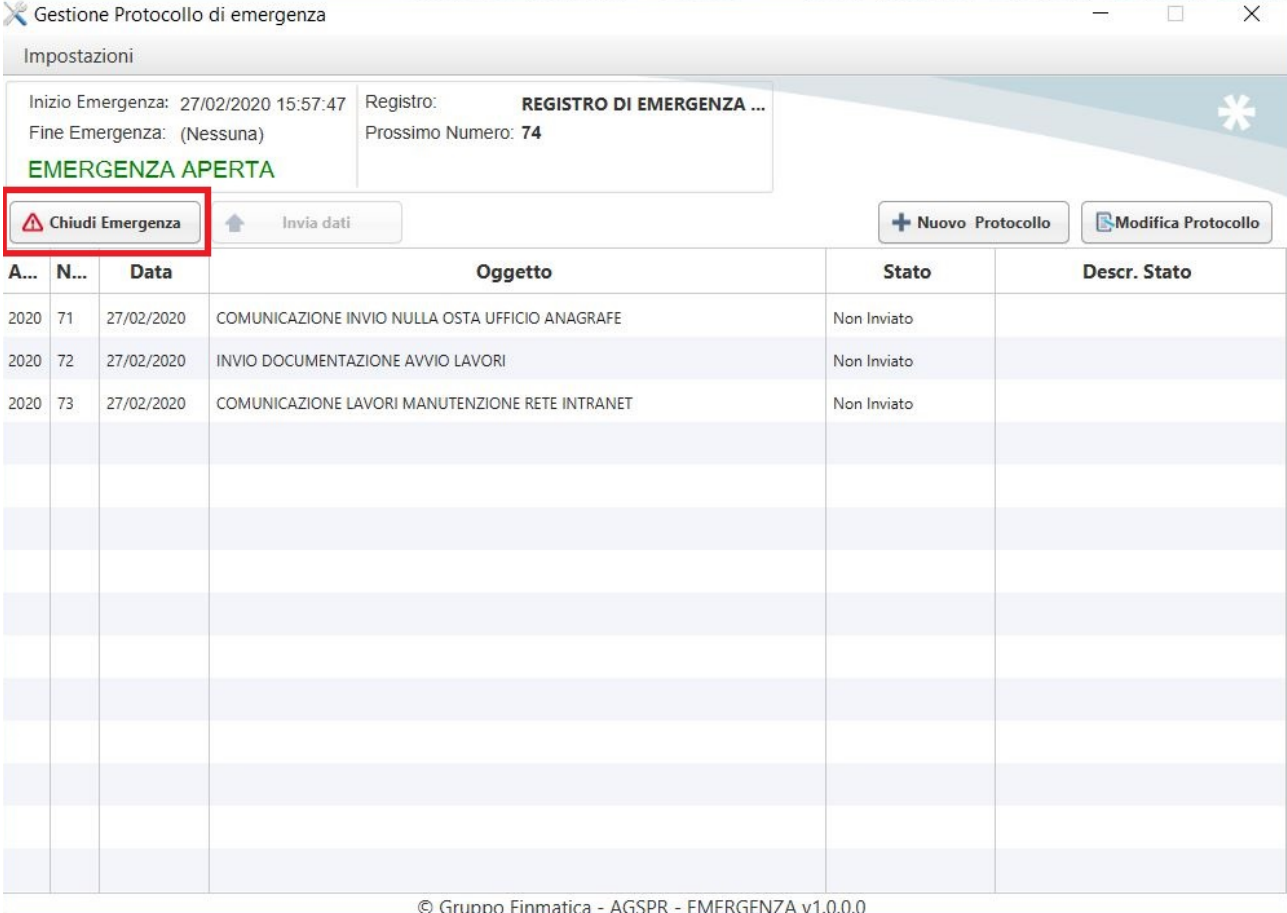
Tra i campi non obbligatori è possibile specificare il

- **Tipo Documento**, selezionando il valore dall'elenco di quelli disponibili nei Dizionari di Prisma.
- **Classificazione**, se tale campo non è valorizzato ma è obbligatorio nelle configurazioni di Prisma, all'invio dei dati non verrà registrato un protocollo automaticamente, ma il documento sarà disponibile nella vista "Da protocollare" da parte dell'utente che ha inviato i dati di emergenza. I valori disponibili sono quelli importati da Prisma al momento dell'allineamento Dizionari (vedi paragrafo 1.2.2).
- **Fascicolo**, se tale campo non è valorizzato ma è obbligatorio nelle configurazioni di Prisma, all'invio dei dati al documentale non verrà registrato un protocollo automaticamente ma il documento sarà disponibile nella query "Da protocollare" da parte dell'utente che ha inviato i dati di emergenza.

- **Mod. Ric. / Sped.:** selezionando il valore dall'elenco di quelli disponibili nei Dizionari di Prisma (voce Dizionari : Tipi di Spedizione; campo Tramite in maschera Protocollo).
- **Data Arrivo / Sped.:** valorizzando Data tramite apposito "calendario"  ; Ora, Minuti e Secondi tramite apposito menu a tendina .
- **Tipo Anagrafica:** selezionando il radio button "Persona" i campi sottostanti saranno "Cognome:" e "Nome"; selezionando il radio button "Amministrazione / Impresa" avremo un solo campo "Denominazione:"
- **Numero Doc. Esterno:** editando stringa relativa a Estremi Documento.
- **Data Doc. Esterno:** valorizzando Data tramite apposito "calendario" .

1.3.5 Chiusura emergenza

Una volta ultimata l'emergenza, l'utente deve concludere cliccando il pulsante "Chiudi Emergenza":



A...	N...	Data	Oggetto	Stato	Descr. Stato
2020	71	27/02/2020	COMUNICAZIONE INVIO NULLA OSTA UFFICIO ANAGRAFE	Non Inviato	
2020	72	27/02/2020	INVIO DOCUMENTAZIONE AVVIO LAVORI	Non Inviato	
2020	73	27/02/2020	COMUNICAZIONE LAVORI MANUTENZIONE RETE INTRANET	Non Inviato	

© Gruppo Finmatica - AGSPR - EMERGENZA v1.0.0.0

Confermando su "Fine emergenza" nella finestra "Chiusura Emergenza", e nel successivo messaggio di "Conferma Fine Emergenza".

1.3.6 Invio Dati

Successivamente è necessario inviare i dati così caricati al sistema Prisma, tramite l'apposito pulsante "Invio Dati", attivo dopo la chiusura dell'emergenza:

[illegible]

Il sistema richiede l'inserimento dei dati necessari alla creazione del protocollo d'emergenza:

 Invio dati emergenza al sistema centrale

Invio Dati Emergenza **NON ANCORA PROTOCOLLATO**

filtra tipi documento ↵

Tipo Documento:

Oggetto:

Protocollo emergenza 27/02/2020

filtra classificazioni ↵

Classificazione:

01/06 - ARCHIVIO GENERALE

Anno Fascicolo:

2020

Numero Fascicolo:

1

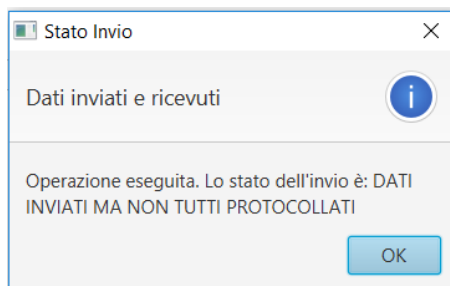
 **Invia**

 **Salva**

 **Chiudi**

NOTA BENE: Oggetto e Classificazione sono obbligatori; se il campo non è valorizzato ma è obbligatorio nelle configurazioni di Prisma, all’invio dei dati al documentale non verrà registrato un protocollo automaticamente ma il documento sarà disponibile nella vista “Da protocollare” da parte dell’utente che ha inviato i dati di emergenza.

Cliccando sul pulsante “Invia” il sistema procede all’invio dei dati a Prisma; al termine dell’operazione appare il messaggio di Conferma:

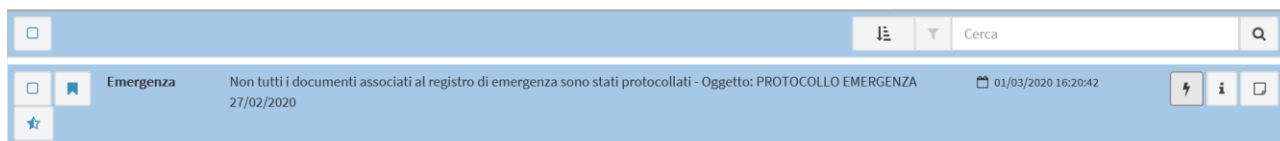


Il dettaglio è riportato nella maschera principale dell’applicazione di Gestione Emergenza:

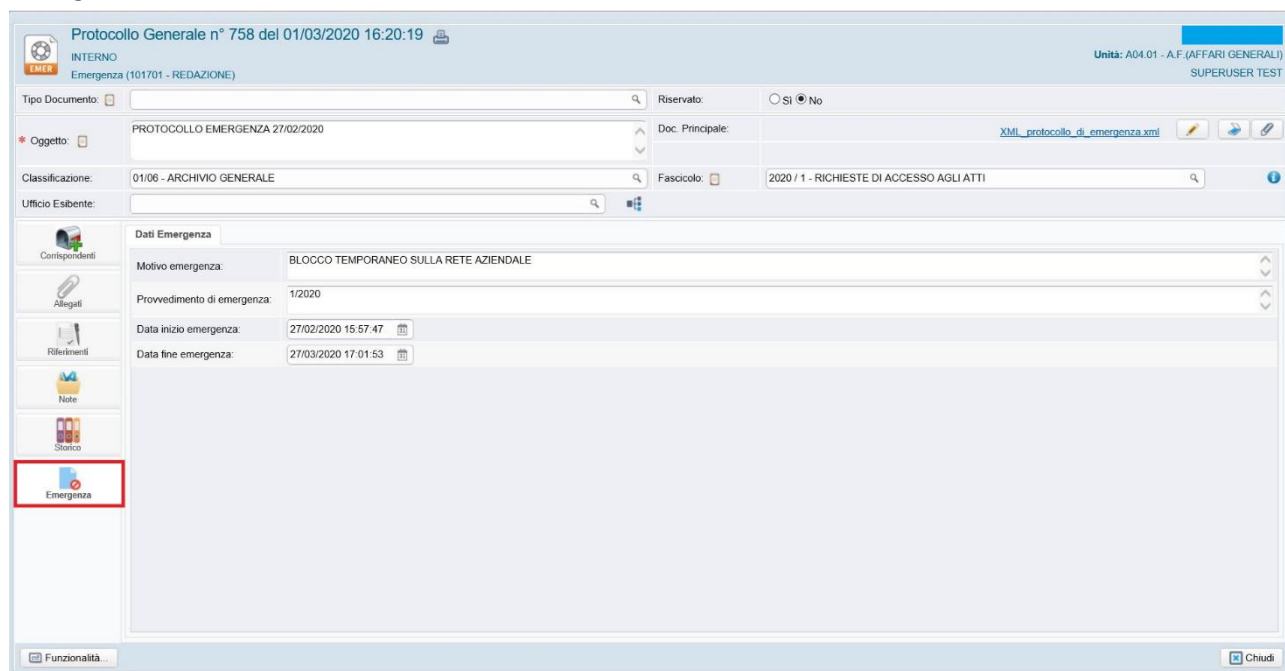
A...	N...	Data	Oggetto	Stato	Descr. Stato
2020	71	27/02/2020	COMUNICAZIONE INVIO NULLA OSTA UFFICIO ANAGRAFE	Inviato e Non Protocollato	Dati mancanti o non validi.
2020	72	27/02/2020	INVIO DOCUMENTAZIONE AVVIO LAVORI	Inviato e Non Protocollato	Dati mancanti o non validi.
2020	73	27/02/2020	COMUNICAZIONE LAVORI MANUTENZIONE RETE INTRANET	Inviato e Protocollato	

1.3.7 Prisma: gestione protocollo di emergenza

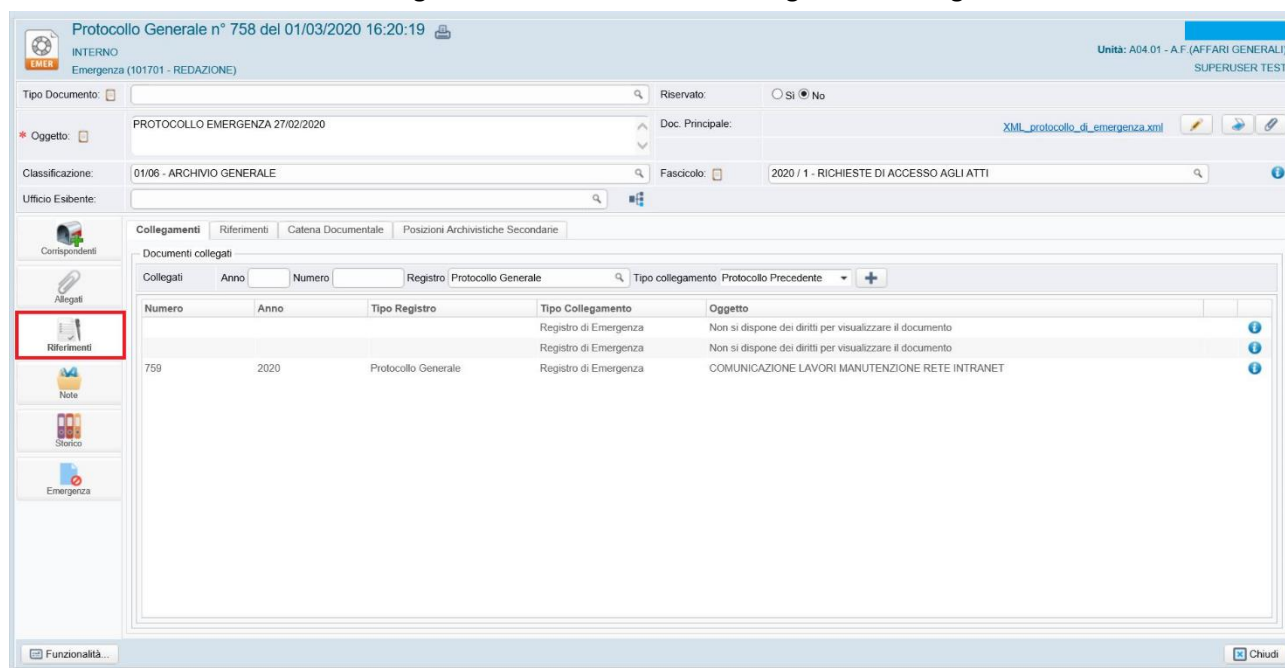
Nella Smart Desktop dell’utente che ha inviato i dati, viene notificata la creazione del protocollo di emergenza, nella quale si evidenzia che non tutti i documenti associati al registro di emergenza sono stati protocollati:



Aperto il dettaglio dell'attività (), nella sezione “Emergenza” sono riportati i dati del protocollo di emergenza:



Nella sezione “Riferimenti” i dettagli dei documenti associati al registro di emergenza:

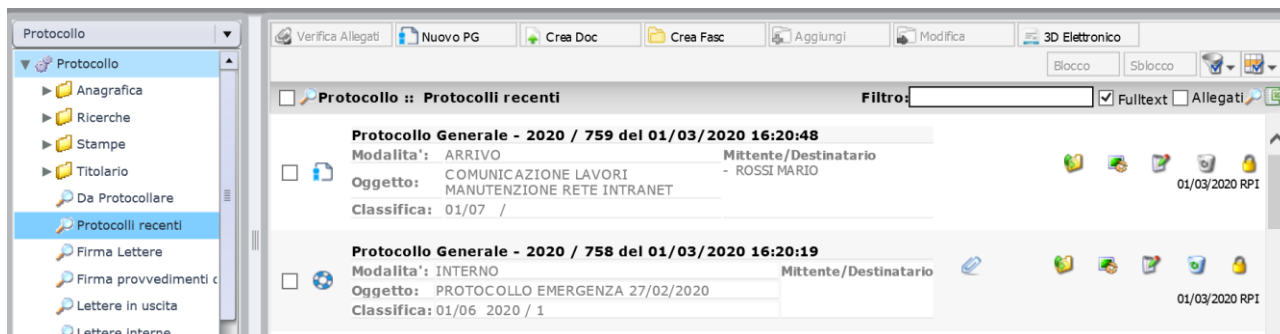


Numero	Anno	Tipo Registro	Tipo Collegamento	Oggetto
759	2020	Protocollo Generale	Registro di Emergenza	Non si dispone dei diritti per visualizzare il documento
759	2020	Protocollo Generale	Registro di Emergenza	Non si dispone dei diritti per visualizzare il documento
759	2020	Protocollo Generale	Registro di Emergenza	COMUNICAZIONE LAVORI MANUTENZIONE RETE INTRANET

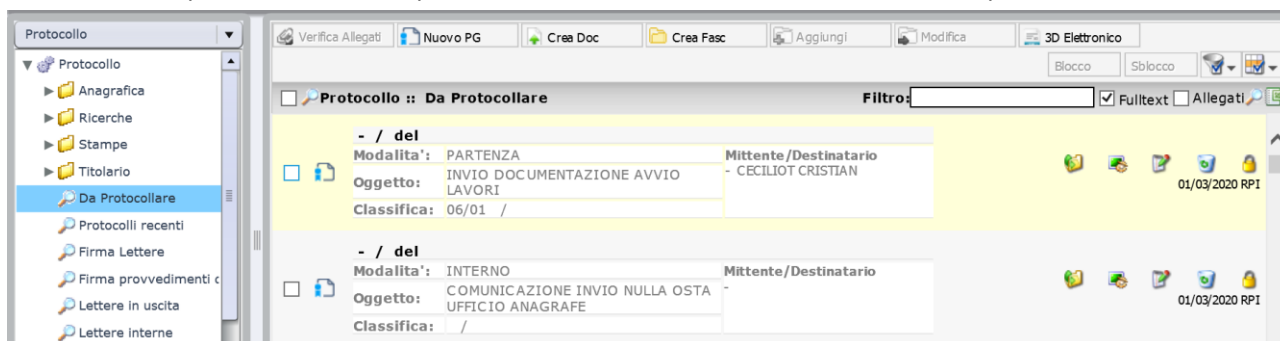
Cliccando sull'icona  posta alla destra di ogni singolo documento è possibile aprire la maschera di dettaglio; è possibile integrare con i dati mancanti (se ad esempio è settato l'obbligo dello smistamento e non è stato inserito in fase di emergenza è possibile farlo ora) e procedere alla protocollazione.

Gli stessi dati sono visibili accedendo al Sistema Documentale nella sezione Protocollo; dalla vista “Protocolli recenti” si evince che è stato creato il protocollo di emergenza INTERNO () e i protocolli con i dati sufficienti

alla loro registrazione, nell'esempio 1 protocollo in ARRIVO:



Nella vista "Da protocollare" sono presenti i dati inviati ma non sufficienti alla loro protocollazione:



Cliccando sull'icona  posta alla destra di ogni singolo documento è possibile aprire la maschera di dettaglio ed integrare con i dati mancanti per procedere alla protocollazione.



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

Settore SETTORE FINANZIARIO

PARERE DI REGOLARITA' CONTABILE

Sulla proposta n. 1214/2022 ad oggetto: APPROVAZIONE NUOVO MANUALE DI GESTIONE DEI DOCUMENTI E CONSERVAZIONE. si esprime ai sensi dell'art. 49, 1° comma del Decreto legislativo n. 267 del 18 agosto 2000, parere NON APPOSTO in ordine alla regolarita' contabile.

Note:

Casalgrande lì, 22/12/2022

Sottoscritto dal Responsabile
(GHERARDI ALESSANDRA)
con firma digitale



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

Certificato di Esecutività

Deliberazione di Giunta Comunale N. 200 del 22/12/2022

Oggetto: APPROVAZIONE NUOVO MANUALE DI GESTIONE DEI DOCUMENTI E CONSERVAZIONE..

Si dichiara che la presente deliberazione è divenuta esecutiva il giorno 07/01/2023, decorsi 10 giorni dall'inizio della pubblicazione all'Albo Pretorio on-line di questo Comune.

Li, 16/01/2023

L'INCARICATO DELLA PUBBLICAZIONE
IBATICI TERESINA
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e s.m.i.)



COMUNE DI CASALGRANDE

PROVINCIA DI REGGIO NELL'EMILIA

Cod. Fisc. e Partita IVA 00284720356 - Piazza Martiri della Libertà, 1 C.A.P. 42013

Certificato di Avvenuta Pubblicazione

Deliberazione di Giunta Comunale N. 200 del 22/12/2022

Oggetto: APPROVAZIONE NUOVO MANUALE DI GESTIONE DEI DOCUMENTI E CONSERVAZIONE..

Si dichiara l'avvenuta regolare pubblicazione della presente deliberazione all'Albo Pretorio on-line di questo Comune a partire dal 27/12/2022 per 15 giorni consecutivi, ai sensi dell'art 124 del D.lgs 18.08.2000, n. 267 e la contestuale comunicazione ai capigruppo consiliari ai sensi dell'art. 125 del D.lgs 18.08.2000, n. 267.

Li, 16/01/2023

L'INCARICATO DELLA PUBBLICAZIONE
IBATICI TERESINA

(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e s.m.i.)