



Archivia!online

MANUALE DEL SERVIZIO DI CONSERVAZIONE DIGITALE GENESYS INFORMATICA S.R.L.



100% ENERGIA PULITA
GARANZIA DI FORNITURA CERTIFICATA



Manuale della conservazione digitale di Genesys Informatica S.r.l.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	01/03/2018	Marco Foligni	Responsabile applicativo della Conservazione
Verifica	01/03/2018	Francesco Leoncino	Responsabile tecnico
Approvazione	01/03/2018	Luigi Corbacella	Responsabile del servizio di conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
01.00.00	01/12/2016	prima stesura	
01.01.00	01/03/2018	attivato Web Service	
01.01.01	02/01/2020	ampliato contenuto di MoreInfo	
01.01.02	15/03/2021	rivista struttura del PdD	

INDICE DEL DOCUMENTO

.....	4
1.SCOPO E AMBITO DEL DOCUMENTO	4
2.TERMINOLOGIA (glossario/acronimi)	5
2.1.Glossario	5
2.2.Acronimi	9
3.NORMATIVA E STANDARD DI RIFERIMENTO.....	10
3.1.Normativa di riferimento.....	10
3.2.Standard di riferimento.....	11
4.RUOLI E RESPONSABILITÀ	12
4.1.Ruoli e responsabilità del cliente.....	12
4.2.Ruoli e responsabilità di Genesys Informatica Srl.....	13
5.STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	15
5.1.Organigramma.....	15
5.2.Strutture organizzative.....	17
6.OGGETTI SOTTOPOSTI A CONSERVAZIONE	18
6.1.Oggetti conservati.....	18
6.2.Pacchetto di versamento.....	18
6.3.Pacchetto di archiviazione.....	20
6.4.Pacchetto di distribuzione.....	21
7.IL PROCESSO DI CONSERVAZIONE	23
7.1.Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	23
7.2.Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti.....	24
7.3.Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico.....	24
7.4.Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie.....	24
7.5.Preparazione e gestione del pacchetto di archiviazione.....	25
7.6.Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione.....	25
7.7.Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	26
7.8.Scarto dei pacchetti di archiviazione.....	26
7.9.Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	27
7.10.Configurazione dei servizi di conservazione	27
8.IL SISTEMA DI CONSERVAZIONE	27
8.1.Componenti logiche.....	27
8.2.Componenti tecnologiche.....	28
8.3.Componenti fisiche.....	29
8.4.Procedure di gestione e di evoluzione	30
9.MONITORAGGIO E CONTROLLI	30
9.1.Procedure di monitoraggio	31
9.1.1.Monitoraggio funzionale.....	31
9.1.2.Monitoraggio operativo	32
9.1.3.Monitoraggio dello stato delle componenti infrastrutturali	32
9.2.Verifica dell'integrità degli archivi	33
9.3.Soluzioni adottate in caso di anomalie	33

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente manuale descrive il servizio di Conservazione a Norma che Genesys Informatica Srl eroga verso la propria clientela che intende sottoporre a conservazione a norma i propri documenti informatici in maniera tale che risultino disponibili nel tempo nella loro integrità e autenticità e che eventualmente ne venga mantenuta la validità legale e fiscale.

Il presente manuale ha anche lo scopo di descrivere:

- il modello organizzativo adottato da Genesys Informatica Srl per l'erogazione del Servizio, in cui sono evidenziati i ruoli e le responsabilità attribuite ad attori interni o affidate a soggetti esterni;
- i processi di erogazione del servizio, facendo riferimento anche a documentazione operativa esterna per la descrizione di attività di dettaglio;
- le attività di controllo sul processo e sugli archivi in modo da verificare la corretta gestione dei processi di erogazione del servizio;
- l'infrastruttura tecnologica a supporto del servizio;
- le misure di sicurezza logiche e fisiche;

Il documento rappresenta il riferimento principale relativo a qualsiasi aspetto che regola il corretto funzionamento del Servizio.

In particolare, il presente documento, rappresenta la linea guida per la gestione della comunicazione tra Genesys Informatica Srl e il Cliente ed è approvato dal Responsabile del Servizio di Conservazione.

Le responsabilità assegnate nell'erogazione del servizio di conservazione vengono riportate nel capitolo specifico di questo manuale.

Si riportano, sempre all'interno del presente documento, i dettagli degli oggetti che vengono conservati, le modalità con cui vengono mantenuti nel tempo, le infrastrutture su cui tali servizi si poggiano ed i sistemi di monitoraggio che controllano l'erogazione.

Eventuali modifiche e aggiornamenti a questo documento potranno essere effettuate dal Responsabile del servizio di Conservazione, previa condivisione con il Responsabile del trattamento dei dati personali, il Responsabile della Sicurezza e con il Responsabile dei Sistemi Informativi.

Qualora si concordi con uno specifico cliente o per uno specifico servizio di conservazione, di operare in modo differente rispetto a quanto riportato nel presente manuale, le particolarità definite saranno riportate in uno specifico allegato, riferito allo specifico contratto o servizio, denominato "specificità contrattuali".

[Torna al sommario](#)

2. TERMINOLOGIA (glossario/acronimi)

2.1. Glossario

In questo paragrafo sono riportate in ordine alfabetico le principali definizioni, termini, e concetti direttamente riferiti o collegati al processo di conservazione a norma.

I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.

Ai fini della fruizione del Servizio di conservazione digitale dei documenti informatici descritto nel presente Manuale, valgono ad ogni effetto anche le definizioni contenute nel Contratto, da intendersi, pertanto, qui interamente riportate e trascritte, nonché le seguenti:

Accesso: operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici conservati;

Accreditamento: riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato che svolge attività di conservazione o di certificazione del processo di conservazione;

Agente di Alterazione: sono agenti di alterazione le macro, i codici eseguibili nascosti, le formule di foglio di lavoro nascoste o difficili da individuare, sequenze di caratteri nascoste all'interno dei dati le quali sono ignorate dall'applicazione originalmente prevista per la presentazione, che però possono essere riconosciute quando i dati vengano elaborati con altre applicazioni;

Acquisizione: procedura di presa in carico dei documenti da parte del sistema di conservazione, previa verifica di coerenza di formato;

Aggregazione documentale informatica: raccolta di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione alle funzioni dell'ente;

Archivio: complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività;

Archivio informatico: archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico;

Autenticità: caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico;

Base di dati: collezione di dati registrati e correlati tra loro;

Certificato qualificato: certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciato da certificatore rispondente ai requisiti fissati dall'allegato II della medesima direttiva;

Certificatore accreditato: soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dell'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza;

Ciclo di gestione: arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo;

Chiusura del pacchetto di archiviazione: operazione consistente nella sottoscrizione del pacchetto di archiviazione con firma digitale apposta da un Firmatario Delegato di Genesys Informatica Srl e apposizione di una marca temporale;

Cliente: è il produttore, legittimo titolare degli oggetti/dati/documenti depositati in conservazione; e unico responsabile del caricamento e versamento in conservazione sostitutiva degli oggetti/dati/documenti; ed è l'entità giuridica che sottoscrive e accetta il Contratto per l'affidamento del servizio di conservazione digitale di documenti informatici;

Codice o CAD: decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni;

Codice eseguibile: insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici;

Conformità della copia: la conformità della copia di un documento informatico o di un documento analogico assicurata secondo le disposizioni del Codice dell'Amministrazione Digitale e del decreto attuativo D.P.C.M. 13/11/2014;

Conservatore accreditato: soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall’Agenzia per l’Italia Digitale o da un certificatore accreditato, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza;

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 e descritto nel Manuale di conservazione;

Contratto: è il Contratto per l’affidamento del servizio di conservazione digitale di documenti informatici perfezionato tra Genesys Informatica Srl ed il Cliente che regola gli aspetti generali dell’erogazione del Servizio di conservazione digitale dei documenti informatici del Cliente;

Copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

Copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

Copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

Copia di sicurezza: copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle Regole Tecniche per il sistema di conservazione;

Destinatario: identifica il soggetto/sistema al quale il documento informatico è indirizzato;

Documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

Documento analogico originale: documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

Documento originale unico: è quel documento analogico il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta, anche presso terzi e che non soddisfa, dunque, alcuna delle condizioni elencate nella definizione di “Documento analogico originale”;

Documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

Documento statico non modificabile: documento informatico redatto in modo tale per cui il contenuto risulti non alterabile durante le fasi di accesso e di conservazione nonché immutabile nel tempo; a tal fine il documento informatico non deve contenere macro o codice eseguibile tale da modificare i dati nello stesso rappresentati;

Duplicato Informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso supporto o su supporti diversi, della medesima sequenza di valori binari del documento originario;

Duplicazione dei documenti informatici: produzione di duplicati informatici;

Esibizione: operazione che consente di visualizzare un documento conservato e di ottenerne copia;

Evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;

Fascicolo informatico: aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento;

File di chiusura: insieme di metadati, su cui è apposta la firma digitale e marca temporale, in grado di fornire prova dell’integrità di un insieme di documenti informatici, ad esso associati, la cui conservazione decorre dal momento di apposizione della marca temporale;

Firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

Firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;

Firma elettronica qualificata: firma elettronica creata mediante un dispositivo sicuro, basata su un certificato qualificato che garantisce la connessione univoca al firmatario e la sua univoca identificazione e collegata ai dati ai quali si riferisce in modo tale da rilevare se i dati stessi siano stati successivamente modificati;

Fruibilità di un dato: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;

Firmatario delegato: Responsabile del servizio di conservazione o Persona formalmente delegata ad apporre la propria firma digitale sui file di chiusura per conto di Genesys Informatica Srl;

Formato: modalità di rappresentazione del documento informatico mediante codifica binaria; comunemente è identificato attraverso l’estensione del file e/o il tipo MIME;

Funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una sequenza di bit (impronta) in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l’evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti;

Identificativo univoco: sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione;

iPdV: Indice del Pacchetto di Versamento

Immodificabilità: caratteristica che rende la rappresentazione del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso;

Impronta: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;

Insieme minimo di metadati del documento informatico: complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta;

Integrità: insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato;

Interoperabilità: capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi;

Leggibilità: insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti;

Log di sistema: registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati;

Manuale di gestione: strumento che descrive il sistema di gestione informatica dei documenti;

Memorizzazione: processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici;

Marca temporale: evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority;

Metadati: insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione;

Normativa regolante la conservazione digitale di documenti informatici: si intende: il D.lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione Digitale "CAD") e i relativi decreti attuativi, le regole tecniche e aggiungendo, per il documento informatico a rilevanza tributaria, le disposizioni di cui al DMEF 17 giugno 2014 s.m.i., il DPR 26 ottobre 1972 n. 633 e s.m.i., il DPR 29 settembre 1973 n. 600 e s.m.i., linee guida Agid maggio 2021;

Originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

Pacchetto di archiviazione: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo lo standard UNI SinCRO 11386:2010 e 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;

Pacchetto di caricamento: pacchetto informativo utilizzato per inviare i documenti fisici al sistema di conservazione;

Pacchetto di versamento: pacchetto informativo inviato dal produttore al sistema di conservazione per essere archiviato in modalità sostitutiva;

Pacchetto informativo: contenitore che racchiude uno o più oggetti da conservare (documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare;

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 nell'ambito dell'organizzazione di appartenenza;

Preso in carico: accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal Manuale di conservazione;

Processo di conservazione: insieme delle attività finalizzate alla conservazione dei documenti informatici;

Processo/servizio di marcatura temporale: è il processo/servizio che associa in modo affidabile un'informazione e un particolare momento, al fine di stabilire prove attendibili che indicano il momento in cui l'informazione esisteva;

Produttore: persona fisica o giuridica che produce i documenti da avviare alla conservazione e responsabile del contenuto dei pacchetti di caricamento e/o di versamento nel sistema di conservazione;

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 della corrispondenza in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti;

Repertorio informatico: registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica;

Responsabile della conservazione: è il Cliente, nella persona fisica dallo stesso formalmente incaricata quale responsabile dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici depositati in conservazione nell'ambito della fornitura del servizio fornito da Genesys Informatica Srl;

Responsabile del Servizio di conservazione: è Genesys Informatica Srl che opererà attraverso uno o più persone fisiche formalmente incaricate all'esecuzione dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici nell'ambito della fornitura del servizio di conservazione ai propri clienti;

Responsabile del trattamento dei dati: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Responsabile della sicurezza: soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza;

Riferimento temporale: informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento;

Scarto: operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse;

Servizio di conservazione dei documenti: è il Servizio di conservazione dei documenti informatici fornito da Genesys Informatica Srl che risponde all'esigenza di avere i documenti informatici del Cliente conservati nel rispetto della normativa vigente; è il Servizio a cui sono affidati i documenti informatici del Cliente per essere conservati in modo elettronico per un periodo di tempo specificato nel Contratto;

Sistema di conservazione: insieme di hardware, software, politiche, procedure, linee guida, regolamenti interni, infrastrutture fisiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti del Cliente almeno per il periodo di tempo specificato nel contratto di servizio di conservazione dei documenti in vigore. Detto sistema tratta i documenti informatici in conservazione in pacchetti informativi che si distinguono in: pacchetti di caricamento, versamento, pacchetti di archiviazione e pacchetti di distribuzione;

Staticità: caratteristica che indica l'assenza di tutti gli elementi dinamici, quali macro istruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione;

Transazione informatica: particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati;

Titolare del trattamento ¹: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Utente: 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;

Validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

[Torna al sommario](#)

2.2. Acronimi

AgID (già DigitPA): Ente pubblico non economico, con competenza nel settore delle tecnologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione. L'Ente, che ha ereditato le funzioni di DigitPA che, a sua volta, ha ereditato le funzioni del CNIPA, opera secondo le direttive per l'attuazione delle politiche e sotto la vigilanza del Ministro per la pubblica amministrazione e l'innovazione, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale;

ASP - Application Service Provider: Fornitore di Servizi Applicativi;

CAD: Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni - "Codice dell'amministrazione digitale";

CA - Certificatore Accreditato: soggetto autorizzato dall'Agenzia per l'Italia Digitale che garantisce l'identità dei soggetti che utilizzano la firma digitale;

C.M. - Circolare Ministeriale;

CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione: creato con l'articolo 176 del DL 196/03, il CNIPA ha incorporato le strutture e le funzioni dell'AIPA e del Centro Tecnico della RUPA ed è stato quindi sostituito da DigitPA e quindi dall'AgID - Agenzia per l'Italia Digitale;

D.LGS. - Decreto Legislativo;

D.M. - Decreto Ministeriale;

DNS – Domain Name System: Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet : Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http://www.....it)/ in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3).

D.P.C.M.: Decreto del Presidente del Consiglio dei Ministri;

D.P.R.: Decreto Presidente della Repubblica;

DPS: Documento Programmatico per la Sicurezza;

Internet Data Center o IDC: il centro servizi che ospita e gestisce l'insieme delle risorse hardware, il software di base, l'applicativo necessario a consentire l'utilizzo dei prodotti, dei software e delle procedure informatiche di proprietà di Genesys Informatica Srl, nonché i documenti informatici del Cliente;

HSM - Hardware Security Module: dispositivi hardware dedicati per la sicurezza crittografica e la gestione delle chiavi in grado di garantire un elevato livello di protezione;

HTTP (Hypertext Transfer Protocol): Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web;

HTTPS (Secure Hypertext Transfer Protocol): Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifratura dei dati trasmessi durante la consultazione di siti e pagine Internet. Corrisponde ad un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL;

ICT - Information and Communication Technology: Tecnologia dell'Informazione e delle Telecomunicazioni. Il dipartimento che gestisce i sistemi informatici e telematici;

INTERNET: Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. Lo sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW);

ISO – International Organization for Standardization: Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO;

MEF: Ministero dell'Economia e delle Finanze;

NTP – Network Time Protocol: Protocollo per la sincronizzazione del tempo;

PdV: Pacchetto di Versamento

PdA: Pacchetto di Archiviazione

PdD: Pacchetto di Distribuzione

PIN – Personal Identification Number: Codice di sicurezza riservato che permette l'identificazione del soggetto abbinato ad un dispositivo fisico. Permette ad esempio l'attivazione delle funzioni del dispositivo di firma;

POP – Point of Presence: Punto di accesso alla rete internet;

SSL – Secure Socket Layer: Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica;

SLA - Service Level Agreement: strumenti contrattuali che definiscono le metriche di servizio (es. qualità di servizio) che devono essere rispettate da un fornitore di servizi nei confronti dei propri clienti;

TSA - Time Stamping Authority;

TSS - Time Stamping Service;

URL – Uniform Resource Locator: Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http:, ftp:, file:, telnet:, news:) specifica il protocollo di accesso all'oggetto;

XML - Extensible Markup Language;

WWW – World Wide Web: insieme di risorse interconnesse da hyperlink accessibili tramite Internet

[Torna al sommario](#)

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1. Normativa di riferimento

Di seguito è riportata la normativa generale di riferimento per l'attività di conservazione a livello nazionale:

- 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 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 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Deliberazione CNIPA 21 maggio 2009 n. 45 e s.m.i. - Regole per il riconoscimento e la verifica del documento informatico;
- Decreto del Presidente del Consiglio dei Ministri 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 21 marzo 2013 - individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze, 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 con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.;
- Decreto del Presidente del Consiglio dei Ministri 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;
- Circolare AGID 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;
- Linee guida sulla formazione, gestione e conservazione dei documenti informatici maggio 2021.

[Torna al sommario](#)

3.2. Standard di riferimento

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information 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 elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

[Torna al sommario](#)

4. RUOLI E RESPONSABILITÀ

L'ente o il soggetto diretto interessato è il titolare dei documenti informatici posti in conservazione e, attraverso il proprio Responsabile della Conservazione, definisce e attua le politiche complessive del sistema di conservazione governandone la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo adottato affidata a Genesys Informatica Srl. la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia riguardo i Modelli organizzativi della conservazione - art. 5 nella figura del Responsabile del servizio di conservazione.

4.1. Ruoli e responsabilità del cliente

Nel sistema di conservazione di Genesys Informatica Srl. si individuano i seguenti ruoli:

Titolare dei documenti: è il soggetto responsabile del contenuto dei documenti informatici oggetto del Servizio, della loro autenticità dell'origine, emissione/formazione ed è il soggetto obbligato per legge o regolamenti alla conservazione dei documenti stessi. Ad esempio in ambito tributario è il soggetto Titolare della contabilità. La corretta e certa individuazione del Titolare dei documenti da parte del sistema di conservazione avviene nella fase di attivazione del Servizio e in ciascuna sessione di versamento tramite i dati identificativi contenuti nell'Indice del Pacchetto di Caricamento.

Produttore dei documenti: è il soggetto responsabile del versamento (trasferimento) del Pacchetto di Caricamento al sistema di conservazione di Genesys Informatica Srl e della verifica del buon esito dell'operazione di caricamento tramite la presa visione del Rapporto di Caricamento prodotto dal sistema di conservazione. Può coincidere con il Titolare dei documenti ovvero può essere delegato ad un soggetto terzo. La corretta e certa individuazione del Produttore dei documenti da parte del sistema di conservazione avviene nella fase di attivazione del Servizio e in ciascuna sessione di caricamento.

Responsabile della Conservazione: è il soggetto responsabile dell'insieme delle attività, di cui all'articolo 7, comma 1, del D.P.C.M. 3 dicembre 2013. Il Responsabile della Conservazione è una persona fisica che opera presso il Soggetto Produttore. Nelle Pubbliche Amministrazioni, il ruolo del Responsabile della Conservazione è svolto da un dirigente o da un funzionario formalmente designato. Il Responsabile della Conservazione, di una Pubblica Amministrazione o anche di un Soggetto Privato, sotto la propria responsabilità ai sensi dell'art. 6, comma 6, del D.P.C.M. 3 dicembre 2013 affida il processo di conservazione al Conservatore, e al suo Responsabile del Servizio di Conservazione.

Utente: è il soggetto autorizzato che richiede al sistema di conservazione di Genesys Informatica Srl l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.

[Torna al sommario](#)

4.2. Ruoli e responsabilità di Genesys Informatica Srl

Nel sistema di conservazione di Genesys Informatica Srl. si individuano i seguenti ruoli:

Responsabile del servizio di conservazione: è la persona fisica che all'interno di Genesys Informatica Srl si occupa di definire e attuare le politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione e di definire le caratteristiche e i requisiti del sistema di conservazione in conformità alla normativa vigente. Garantisce una corretta erogazione del servizio di conservazione all'ente produttore e gestisce le convenzioni, definisce gli aspetti tecnico - operativi e la validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

Responsabile sicurezza dei sistemi per la conservazione: si occupa di monitorare e rispettare i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. In caso di eventuali difformità si occupa di segnalarle al Responsabile del servizio di conservazione e, quindi, individua e pianifica le necessarie azioni correttive.

Responsabile della funzione archivistica di conservazione: si occupa di definire e gestire il processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato. Definisce, inoltre, il set di metadati di conservazione dei documenti e dei fascicoli informatici. Monitora il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema. Collabora con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

Responsabile del trattamento dei dati personali: si occupa di garantire il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. Garantisce, inoltre che il trattamento dei dati affidati dai Soggetti produttore avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Responsabile dei sistemi informativi per la conservazione: si occupa di gestire l'esercizio delle componenti hardware e software del sistema di conservazione e monitora il mantenimento dei livelli di servizio (SLA) concordati con il Soggetto produttore. Segnala le eventuali difformità degli SLA al Responsabile del servizio di conservazione e individua e pianifica le necessarie azioni correttive. Si occupa di pianificazione lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

Responsabile sviluppo e manutenzione del sistema di conservazione: si occupa di coordinare lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione. Pianifica e monitora i progetti di sviluppo del sistema di conservazione. Monitora inoltre gli SLA relativi alla manutenzione del sistema di conservazione. Si occupa di interfacciarsi con il Soggetto produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. Gestisce, inoltre lo sviluppo di siti web e portali connessi al servizio di conservazione.

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	Luigi Corbacella	<ul style="list-style-type: none"> Definizione ed attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; Corretta erogazione del Servizio di Conservazione all'Ente Produttore; Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei Servizi di Conservazione. 	dal 01/12/2016	
Responsabile Sicurezza dei sistemi per la conservazione	Francesco Leoncino	<ul style="list-style-type: none"> Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; Segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive 	dal 01/12/2016	

Responsabile funzione archivistica di conservazione	Francesco Leoncino	<ul style="list-style-type: none"> Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'Ente Produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; Collaborazione con l'Ente Produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza. 	dal 01/12/2016	
Responsabile trattamento dati personali	Luigi Corbacella	<ul style="list-style-type: none"> Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza. 	dal 01/12/2016	
Responsabile sistemi informativi per la conservazione	Marco Foligni	<ul style="list-style-type: none"> Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'Ente Produttore; Segnalazione delle eventuali difformità degli SLA al Responsabile del Servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive; Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione. 	dal 01/12/2016	
Responsabile sviluppo e manutenzione del sistema di conservazione	Marco Foligni	<ul style="list-style-type: none"> Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; Interfaccia con l'Ente Produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; Gestione dello sviluppo di siti web e portali connessi al Servizio di Conservazione. 	dal 01/12/2016	

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1. Organigramma

Gli attori principali sono il responsabile della conservazione ed il responsabile del servizio di conservazione di Genesys Informatica S.r.l. che operano secondo gli accordi di servizio. Mentre i soggetti sono:

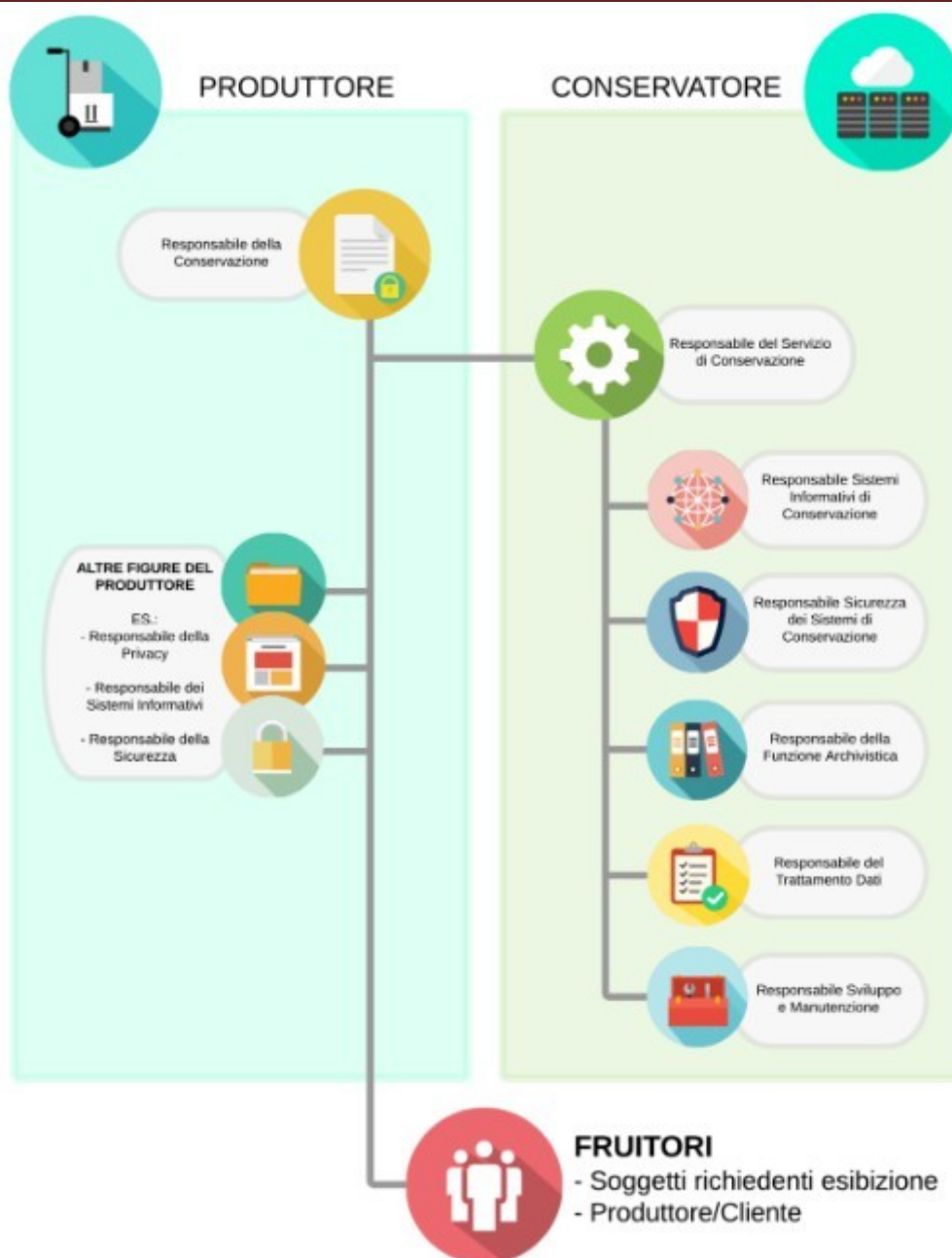
- l'ente produttore detto anche Titolare (è il ruolo svolto dalle persone fisiche o giuridiche o dai sistemi che forniscono le informazioni da conservare);
- il responsabile della conservazione (è la persona fisica interna all'organizzazione del titolare dei documenti informatici che definisce e attua le politiche complessive del sistema e ne governa la gestione con piena responsabilità e autonomia);
- l'utente (è il ruolo svolto da persone o sistemi che interagiscono con il sistema di conservazione al fine di accedere e ricercare le informazioni di interesse).

In pratica, il Titolare, attraverso il proprio Responsabile della Conservazione, affida a Genesys Informatica S.r.l. il servizio di conservazione dei propri dati e oggetti informatici, la quale, in veste di conservatore, assume le responsabilità del servizio di conservazione in accordo con quanto previsto dal Contratto di servizio, dai relativi allegati contrattuali e dal DPCM 3 dicembre 2013 e sue s.m.i.. Genesys Informatica S.r.l. provvede ad affidare il ruolo di Responsabile del servizio di conservazione ad una persona fisica interna alla propria organizzazione che, per competenza ed esperienza, garantisca la corretta esecuzione dei processi di conservazione definiti dalle norme, dal presente Manuale, dal Contratto di servizio e dagli allegati contrattuali.

Il Responsabile del Servizio di conservazione di Genesys Informatica S.r.l. può delegare lo svolgimento di parte del processo a una o più persone con adeguata competenza ed esperienza, secondo quanto previsto nella documentazione interna di organizzazione e gestione del sistema di conservazione. Le attività eventualmente affidate ai singoli soggetti interni all'organizzazione del conservatore sono definite nell'ordine di servizio che regola il rapporto tra Genesys Informatica S.r.l. ed i propri collaboratori.

In ogni caso, il conservatore garantisce che tutte le persone coinvolte, a qualsiasi livello, nei processi di conservazione hanno raggiunto un comprovato livello di competenza e/o esperienza tali da consentire un adeguato livello di autonomia, pur sotto la costante supervisione del diretto superiore gerarchico e/o del Responsabile del servizio di conservazione.

Di seguito si rappresenta l'organigramma adottato da Genesys Informatica S.r.l. per la gestione del servizio di conservazione digitale di dati e documenti informatici. Il Cliente che sceglie il Sistema di Conservazione Digitale di Genesys Informatica S.r.l. (Conservatore) mantiene all'interno della propria struttura organizzativa il ruolo di Responsabile della Conservazione mentre affida al Conservatore la responsabilità del relativo servizio e le funzioni a ciò correlate.



[Torna al sommario](#)

5.2. Strutture organizzative

Sono di seguito descritte le strutture organizzative, comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione.

Le attività proprie di ciascun contratto di servizio di conservazione sono svolte nella struttura organizzativa del Responsabile del servizio di conservazione, in particolare:

- l’attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto);
- la chiusura del servizio di conservazione (al termine di un contratto).

Tramite il “Sistema di conservazione dei documenti”, sono svolte le seguenti attività:

- acquisizione, verifica e gestione dei pacchetti di caricamento presi in carico;
- acquisizione e gestione dei pacchetti di versamento presi in carico, generazione del rapporto di versamento;
- preparazione e gestione del pacchetto di archiviazione;

- preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta;
- scarto dei pacchetti di archiviazione.

La struttura organizzativa del Responsabile dei sistemi informativi per la conservazione effettua le attività proprie di gestione dei sistemi informativi:

- conduzione e manutenzione del sistema di conservazione;
- monitoraggio del sistema di conservazione;
- change management;
- verifica periodica di conformità a normativa e standard di riferimento.

La fase di Attivazione si avvia con una richiesta di adesione al Servizio da parte del Cliente. Il Cliente può coincidere con il Titolare dei documenti (generalmente il caso di vendita diretta del Servizio) o può essere un Distributore del Servizio (caso della vendita indiretta) che ha l'obbligo di fornire tutti i dati relativi ai propri Clienti (Titolari e Produttori dei documenti) e ha l'obbligo di far accettare a quest'ultimi, tramite specifica modulistica, le condizioni generali di Servizio e le Specificità del Contratto (Scheda Servizio)

L'area di Attivazione del Servizio prende in carico l'ordine di acquisto ed i documenti contrattuali, ne verifica la correttezza ed in caso di esito positivo attiva la procedura di attivazione operativa del Servizio. Con la generazione delle anagrafiche, della predisposizione dell'area di conservazione, la generazione della prima login di accesso.

La seconda fase del Servizio riguarda la fase produttiva con l'insieme delle attività operative di cui è responsabile della corretta esecuzione l'Area di Produzione con supervisore il Responsabile del Servizio di Conservazione del Conservatore, previa affidamento da parte del Responsabile della Conservazione che opera presso il Produttore. I principali compiti sono eseguiti dai delegati operativi, che attraverso gli strumenti ed i sistemi aziendali a supporto del Servizio, eseguono e presidiano le seguenti attività:

- verifica dei Pacchetti di caricamento ricevuti, con controllo corrispondenza dei formati e scansione con antivirus. Con il conseguente esito di scarto o generazione dell'esito di presa in carico;
- pubblicazione web dei documenti e dei Pacchetti per la ricerca, consultazione ed esibizione;
- verifica dei PdV con generazione del Rapporto di Versamento (IdV) standard UNI SInCRO 11386:2010 quale esito delle verifiche di validità;
- generazione del Pacchetto di Archiviazione standard UNI SInCRO 11386:2010, firmato e marcato temporalmente secondo la normativa di riferimento;
- presidio, monitoraggio e controlli sulla conservazione degli oggetti digitali;
- generazione del Pacchetto di Distribuzione (PdD) standard UNI SInCRO 11386:2010 su richiesta espressa dell'Utente;
- produzione di copie e duplicati su richiesta dell'Utente

Terminato il periodo di conservazione concordato contrattualmente, e quello stabilito dal Cliente/Produttore per ogni documento o gruppo di documenti, il Conservatore può provvedere allo scarto dei pacchetti di archiviazione (tramite generazione dei Pacchetti di Scarto PdS), previa comunicazione informativa inviata al Produttore con un periodo di preavviso di 60 giorni, per permettere a quest'ultimo eventualmente di richiedere un'estensione del Servizio di Conservazione oltre il periodo concordato.

Nel caso di archivi pubblici o privati, che rivestono interesse storico particolarmente importante, il Conservatore ed il Produttore dei documenti concordano preventivamente nella Scheda Servizio che lo Scarto del Pacchetto di Archiviazione debba avvenire esclusivamente previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al Produttore secondo quanto previsto dalla normativa vigente in materia.

La fase di scarto si attiva inoltre al termine di validità del contratto o nei casi di disdetta o di recesso anticipato, con l'attivazione da parte di Genesys Informatica S.r.l. della procedura di chiusura del Servizio di Conservazione per quel determinato Produttore.

[Torna al sommario](#)

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Di seguito sono descritti gli oggetti conservati e i pacchetti informativi gestiti dal sistema di conservazione.

6.1. Oggetti conservati

Gli oggetti dati gestiti dal sistema di conservazione di Genesys Informatica S.r.l. possono essere costituiti da:

- documenti informatici (di varia natura quale ad esempio tributaria, civilistica, assicurativa, bancaria, ecc.);
- documenti informatici amministrativi;
- fascicoli informatici o aggregazioni documentali informatiche (che a loro volta contengono oggetti quali le unità documentarie);
- repertori informatici registri informatici cronologici che raccolgono i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti.

Per garantire l'autonomia nella gestione conservativa degli oggetti dati rispetto alle soluzioni tecnologiche, il Conservatore Genesys Informatica S.r.l. include nei pacchetti informativi (PdV, PdA e PdD) le informazioni di descrizione della conservazione in base alla natura dell'oggetto da conservare.

Per garantire l'interoperabilità nella conservazione e nel recupero degli oggetti digitali in caso di migrazioni da un sistema di conservazione all'altro, è stata adottata la struttura dati conforme allo standard UNI SInCRO per tutti gli Indici XML dei pacchetti informativi PdV, PdA, PdD ed anche per il Rapporto di Versamento (IdV) e l'Indice del Pacchetto di Scarto (IPdS) generato dalla procedura di scarto.

Di seguito sono riportati i formati idonei alla conservazione che accetta il sistema di conservazione e possono quindi essere utilizzati dal Produttore dei documenti per il versamento al sistema predetto.

visualizzatore	formato	estensione	tipo mime	standard	formato aperto
adobe reader	PDF	.pdf	application/pdf	ISO32000-1	SI
adobe reader	PDF/A	.pdf	application/pdf	ISO19005-2:2011	SI
web browser	XML	.xml	application/xml text/xml		SI

[Torna al sommario](#)

6.2. Pacchetto di versamento

Il pacchetto di versamento – nel seguito PdV – è un pacchetto informativo richiesto dal produttore dei documenti al sistema di conservazione per avviare alla conservazione sostitutiva un insieme di documenti con le caratteristiche concordate nel contratto di servizio. Responsabile del contenuto del PdV è il produttore del documento, che deve formarlo e trasmetterlo al sistema di conservazione secondo le modalità operative definite nel presente Manuale. Ogni PdV può contenere esclusivamente documenti della stessa Classe Documentale. In questo senso l'elenco dei metadati dei singoli documenti è omogeneo.

I metadati sono di carattere diverso a seconda che descrivano proprietà e qualità del pacchetto in genere o dei singoli documenti.

Per consentire l'elaborazione automatica dei metadati il sistema di conservazione richiede l'incapsulamento degli stessi in un determinato formato XML, che di fatto costituisce l'Indice del pacchetto di versamento ed il rapporto di versamento – nel seguito IdV.

L'IdV è un'evidenza informatica, ovvero un file, che descrive il versamento e i documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

Di seguito è descritta la struttura dati del IdV UNI-SInCRO adottato dal sistema e contiene le seguenti principali informazioni nel suo Vocabolario.

STRUTTURA DELL'INDICE DEL PACCHETTO DI VERSAMENTO

Nome nodo	Nome elemento	Descrizione
SelfDescription		Informazioni relative all'indice di versamento
	ID	identificativo univoco dell'indice del pacchetto
SelfDescription /CreatingApplication		Informazioni sull'applicazione software che lo ha generato
	Name	nome dell'applicazione software che lo ha generato
	Version	versione dell'applicazione software che lo ha generato
	Producer	produttore dell'applicazione software che lo ha generato
IdV		informazioni relative al pacchetto di versamento
	ID	identificativo univoco del pacchetto
PVolume		informazioni applicative al volume
	Label	etichetta dell'oggetto (IdV)
	ID	identificativo applicativo
	Description	descrizione (Rapporto di versamento)
FileGroup		informazioni sul documento (raggruppamenti di file contenuti)
	label	identificativo del documento
	ID	identificativo del documento
FileGroup/File		informazioni sul file oggetto di versamento
	sincro:extension - sincro:format	informazioni sulla tipologia del file versato
	ID	identificativo del file
	Path	nome del file
	Hash	impronta calcolata con algoritmo SHA-256
FileGroup/File/MoreInfo		contiene informazioni relative al documento oggetto di conservazione (indici)
Process		informazioni sul processo di generazione del pacchetto
Process/Submitter		informazioni sul soggetto che versa i documenti
	sincro:role - sincro:type	informazioni sul ruolo e la tipologia del soggetto
	Agent_ID	identificativo, codice fiscale del soggetto
Process/Submitter/AgentName		nome/denominazione soggetto
	FormalName	denominazione o ragione sociale del soggetto
Process/Submitter/AgentName/NameAndSurname		nome e cognome soggetto (persona fisica)
	Name	nome
	Surname	cognome
Process/Holder		informazioni sul soggetto proprietario e produttore dei documenti
	sincro:role - sincro:type	informazioni sul ruolo e la tipologia del soggetto
	Agent_ID	identificativo, codice fiscale del soggetto
Process/Holder/AgentName		nome/denominazione soggetto
	FormalName	denominazione o ragione sociale del soggetto
Process/Holder/AgentName/NameAndSurname		nome e cognome soggetto (persona fisica)
	Name	nome
	Surname	cognome
Process/AuthorizedSigner		informazioni sui soggetti che intervengono nella conservazione e relativo ruolo
	sincro:role - sincro:type	informazioni sul ruolo e la tipologia del soggetto
	Agent_ID	identificativo, codice fiscale del soggetto
Process/AuthorizedSigner/AgentName/NameAndSurname		nome e cognome soggetto (persona fisica)
	Name	nome
	Surname	cognome
Process/TimeReference	TimeInfo	informazioni relative al riferimento temporale

DEFINIZIONE DEGLI ITEM MoreInfo

Nome nodo	Nome elemento	Descrizione
DocInfo		informazioni relative al documento
	ID	identificativo del documento
ObjectInfo		Indici relativi al documento
	ScadenzaConservazione	mese ed anno di scadenza del periodo di conservazione
	Tipo	codice tipologia documento
	Tipodescr	descrizione tipologia documento
	Oggetto	oggetto del documento
	Anno	anno di riferimento
	Mese	mese di riferimento
	Dal	periodo di riferimento, giorno di inizio
	Al	periodo di riferimento, giorno di fine
	Data	data di riferimento
	Serie	sezionale, serie dei numerazione del documento
	Numero	numero del documento (protocollo)
	NumeroOrig	numero originale del documento del fornitore
	Nominativo	nominativo del cliente/fornitore
	Partitalva	partita iva del cliente/fornitore
CodiceFiscale	codice fiscale del cliente/fornitore	
Paginalni	pagina iniziale del documento	
PaginaFin	pagina finale del documento	
	IdentificativoSDI	Identificativo attribuito da SDI alle fatture in esso transitate

[Torna al sommario](#)

6.3. Pacchetto di archiviazione

Il pacchetto di archiviazione – nel seguito PdA – è un pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento.

Il PdA è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualificata. Oltre alla firma elettronica qualificata è apposta anche una marcatura temporale per darne data certa. Responsabile del contenuto del PDA è il sistema di conservazione.

Per consentire l'elaborazione automatica dei metadati il sistema di conservazione richiede l'incapsulamento degli stessi in un determinato formato XML, che di fatto costituisce l'Indice del pacchetto di archiviazione – in seguito IdC. L'IdC è un'evidenza informatica, ovvero un file, che descrive l'archiviazione e i documenti che ne fanno parte attraverso l'uso di metadati.

La struttura dell'indice del pacchetto di archiviazione IdC è quella prevista dallo standard SInCRO (UNI 11386) ed adottata dal sistema e contiene le seguenti principali informazioni nel suo Vocabolario.

STRUTTURA DELL'INDICE DEL PACCHETTO DI ARCHIVIAZIONE

Nome nodo	Nome elemento	Descrizione
SelfDescription		Informazioni relative all'indice di versamento
	ID	identificativo univoco dell'indice del pacchetto
SelfDescription /CreatingApplication		Informazioni sull'applicazione software che lo ha generato
	Name	nome dell'applicazione software che lo ha generato
	Version	versione dell'applicazione software che lo ha generato
	Producer	produttore dell'applicazione software che lo ha generato
IdC		informazioni relative al pacchetto di conservazione
	ID	identificativo univoco del pacchetto
PVolume		informazioni applicative al volume
	Label	etichetta dell'oggetto (IdC)
	ID	identificativo applicativo
	Description	descrizione (Rapporto di versamento)

FileGroup		informazioni sul documento (raggruppamenti di file contenuti)
	label	identificativo del documento
	ID	identificativo del documento
FileGroup/File		informazioni sul file oggetto di versamento
	sincro:extension - sincro:format	informazioni sulla tipologia del file versato
	ID	identificativo del file
	Path	nome del file
	Hash	impronta calcolata con algoritmo SHA-256
FileGroup/File/MoreInfo		contiene informazioni relative al documento oggetto di conservazione (indici)
Process		informazioni sul processo di generazione del pacchetto
Process/Submitter		informazioni sul soggetto che versa i documenti
	sincro:role - sincro:type	informazioni sul ruolo e la tipologia del soggetto
	Agent_ID	identificativo, codice fiscale del soggetto
Process/Submitter/AgentName		nome/denominazione soggetto
	FormalName	denominazione o ragione sociale del soggetto
Process/Submitter/AgentName/NameAndSurname		nome e cognome soggetto (persona fisica)
	Name	nome
	Surname	cognome
Process/Holder		informazioni sul soggetto proprietario e produttore dei documenti
	sincro:role - sincro:type	informazioni sul ruolo e la tipologia del soggetto
	Agent_ID	identificativo, codice fiscale del soggetto
Process/Holder/AgentName		nome/denominazione soggetto
	FormalName	denominazione o ragione sociale del soggetto
Process/Holder/AgentName/NameAndSurname		nome e cognome soggetto (persona fisica)
	Name	nome
	Surname	cognome
Process/AuthorizedSigner		informazioni sui soggetti che intervengono nella conservazione e relativo ruolo
	sincro:role - sincro:type	informazioni sul ruolo e la tipologia del soggetto
	Agent_ID	identificativo, codice fiscale del soggetto
Process/AuthorizedSigner/AgentName/NameAndSurname		nome e cognome soggetto (persona fisica)
	Name	nome
	Surname	cognome
Process/TimeReference	TimeInfo	informazioni relative al riferimento temporale

[Torna al sommario](#)

6.4. Pacchetto di distribuzione

Il pacchetto di distribuzione – nel seguito PdD – è un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.

Responsabile del contenuto del PdD è il sistema di conservazione a seguito di una richiesta da parte di un utente. Il PdD è un insieme di metadati e documenti corrispondenti alla richiesta di esibizione effettuata da un utente.

Il PdD è un archivio compresso in formato .zip che contiene i seguenti elementi:

- indice del pacchetto di distribuzione – IPdD;
- la copia dei file relativi ai documenti richiesti (in formato originale firmato e/o meno);
- il foglio di stile .xslt per i file di formato XML;
- il file dell'indice firmato e marcato temporalmente relativo al PdA del documento (uno o più in base ai documenti oggetto della richiesta di esibizione);
- il software di ricerca e visualizzazione dei documenti.

Il pacchetto di distribuzione è firmato con firma elettronica dal sistema di conservazione.

L'IPdD è un'evidenza informatica, ovvero un file, che descrive la distribuzione e i documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

La struttura dell'indice del pacchetto di distribuzione è di seguito definita.

STRUTTURA DELL'INDICE DEL PACCHETTO DI DISTRIBUZIONE

Nome nodo	Nome elemento	Descrizione
SelfDescription		Informazioni relative all'indice di distribuzione
	ID	identificativo univoco dell'indice del pacchetto
SelfDescription /CreatingApplication		Informazioni sull'applicazione software che lo ha generato
	Name	nome dell'applicazione software che lo ha generato
	Version	versione dell'applicazione software che lo ha generato
	Producer	produttore dell'applicazione software che lo ha generato
IdC		informazioni relative al volume
	ID	identificativo univoco del pacchetto
PVolum		informazioni applicative del PdD
	Label	etichetta dell'oggetto (PdD)
	ID	identificativo applicativo
	Description	descrizione (pacchetto di distribuzione)
FileGroup		informazioni sul pacchetto di archiviazione e sul documento
	label	identificativo del pacchetto di archiviazione
FileGroup/File		informazioni sul file oggetto di archiviazione
	sincro:extension - sincro:format	informazioni sulla tipologia del file archiviato
	ID	identificativo del file
	Path	nome del file
	Hash	impronta calcolata con algoritmo SHA-256
FileGroup/File/MoreInfo/EmbeddedMetadata		contiene informazioni relative al pacchetto di archiviazione
Process		informazioni sul processo di generazione del pacchetto
Process/Submitter		informazioni sul soggetto che versa i documenti
	sincro:role - sincro:type	informazioni sul ruolo e la tipologia del soggetto
	Agent_ID	identificativo, codice fiscale del soggetto
Process/Submitter/AgentName		nome/denominazione soggetto
	FormalName	denominazione o ragione sociale del soggetto
Process/Submitter/AgentName/NameAndSurname		nome e cognome soggetto (persona fisica)
	Name	nome
	Surname	cognome
Process/Holder		informazioni sul soggetto proprietario e produttore dei documenti
	sincro:role - sincro:type	informazioni sul ruolo e la tipologia del soggetto
	Agent_ID	identificativo, codice fiscale del soggetto
Process/Holder/AgentName		nome/denominazione soggetto
	FormalName	denominazione o ragione sociale del soggetto
Process/Holder/AgentName/NameAndSurname		nome e cognome soggetto (persona fisica)
	Name	nome
	Surname	cognome
Process/AuthorizedSigner		informazioni sui soggetti che intervengono nella conservazione e relativo ruolo
	sincro:role - sincro:type	informazioni sul ruolo e la tipologia del soggetto
	Agent_ID	identificativo, codice fiscale del soggetto
Process/AuthorizedSigner/AgentName/NameAndSurname		nome e cognome soggetto (persona fisica)
	Name	nome
	Surname	cognome
Process/TimeReference	TimeInfo	informazioni relative al riferimento temporale

DEFINIZIONE DEGLI ITEM MoreInfo

Nome nodo	Nome elemento	Descrizione
DocInfo		informazioni relative al documento
	ID	identificativo del documento
ObjectInfo		Indici relativi al documento
	ScadenzaConservazione	mese ed anno di scadenza del periodo di conservazione
	Tipo	codice tipologia documento
	Tipodescr	descrizione tipologia documento
	Oggetto	oggetto del documento
	Anno	anno di riferimento
	Mese	mese di riferimento
	Dal	periodo di riferimento, giorno di inizio
	Al	periodo di riferimento, giorno di fine
	Data	data di riferimento
	Serie	sezionale, serie dei numerazione del documento
	Numero	numero del documento (protocollo)
	NumeroOrig	numero originale del documento del fornitore
	Nominativo	nominativo del cliente/fornitore
	Partitalva	partita iva del cliente/fornitore
CodiceFiscale	codice fiscale del cliente/fornitore	
PaginaIni	pagina iniziale del documento	
PaginaFin	pagina finale del documento	
	IdentificativoSDI	Identificativo attribuito da SDI alle fatture in esso transitate

[Torna al sommario](#)

7. IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione è conforme a quanto disposto dall'art. 9 delle Regole Tecniche ed ha la finalità di assicurare i requisiti di autenticità dell'origine, integrità, leggibilità, disponibilità e reperibilità degli oggetti sottoposti al processo per tutto il periodo di conservazione.

Il processo di conservazione si svolge secondo una serie di fasi, come segue:

- predisposizione dei documenti da avviare alla conservazione sostitutiva: rappresenta la fase iniziale, che viene svolta dal Produttore e dal Responsabile del Sistema di Conservazione, nella quale vengono selezionati i documenti da avviare alla conservazione. Il sistema segnala eventuali anomalie che non ne consentono l'archiviazione. In questa fase il sistema verifica che il file sia nel formato pdf, xml (fattura PA) anche se firmato dal Produttore (p7m) e che gli indici minimi siano presenti. Selezionati i file il Produttore invia la richiesta di versamento al sistema.
- Presa in carico del PdV: rappresenta la fase di presa in carico del pacchetto di versamento da parte del sistema di conservazione, l'esito positivo dei controlli formali è confermato dalla redazione del IdV. In caso di esito negativo dei controlli formali il pacchetto di versamento non è preso in carico.
- Firma dell'IdV: rappresenta la fase di firma dei rapporti di versamento da parte dei Tecnici della conservazione apportano la firma digitale per attestare la corretta formazione.
- Assemblaggio dei PDA: rappresenta la fase di assemblaggio dei documenti in pacchetti di archiviazione secondo le regole di archiviazione previste per ciascun servizio di conservazione. E si completa con la creazione dell'IdC.
- Firma dell' IdC: rappresenta la fase di firma dei pacchetti di archiviazione assemblati. È la fase manuale del processo di conservazione in cui i Tecnici della conservazione apportano la firma digitale sui pacchetti di archiviazione per attestare il corretto svolgimento del processo di conservazione.

Di seguito sono descritte nel dettaglio le modalità tramite sono svolte le attività del processo di conservazione.

[Torna al sommario](#)

7.1. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

L'operazione di versamento consiste nella richiesta da parte del produttore dei documenti da conservare.

Il versamento prevede una selezione dei documenti presenti nel sistema di archiviazione.

Il versamento è effettuato tramite i PdV.

L'invio dei PdV prevede i seguenti passi da parte del produttore:

- Selezione dei documenti da conservare, che abbiano le caratteristiche di formato previste e che siano forniti degli indici minimi previsti dalla natura del documento.
- Richiesta di versamento.

[Torna al sommario](#)

7.2. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Il sistema di Conservazione, ricevuti dal Produttore i Pacchetti di Versamento, esegue su di essi delle verifiche di coerenza ed una serie di controlli di validità rispetto alle specifiche concordate nel Disciplinare Specificità del Contratto che consistono nella:

- Verifica credenziali Utente e stato Utente attivo ed autorizzato;
- Verifica dell'idoneità del formato del file;
- Verifica di quadratura tra il numero di files fisici ed il numero di record logici che li classificano;
- Verifica della integrità del documento mediante il confronto tra l'impronta associata al file in ingresso e l'impronta ricalcolata dal sistema di conservazione;
- Verifica della eventuale presenza nel corrispondente archivio informatico di un documento o oggetto identico;
- Verifica della presenza dei dati anagrafici dei soggetti Produttore, Affidante, Titolare dei documenti, Responsabile della Conservazione nel sistema di conservazione;

- Verifica della avvenuta compilazione dei metadati obbligatori per ogni tipo di documento o in generale oggetto digitale.

Tutte le azioni di controllo eseguite e di comunicazione dell'esito sono tracciate nel data base log del Sistema Conservazione con l'indicazione nei log dell'impronta dei documenti verificati, con la registrazione di un riferimento temporale, l'individuazione dell'Utente che ha richiesto la generazione e l'esito della verifica.

In caso di esito positivo, viene generato il IdV normalizzato standard UNI SInCRO.

Il sistema prende in carico il PdV normalizzato e verifica la sua coerenza e valida la conformità sintattica del XML allo schema UNI SInCRO di riferimento, eseguendo le ulteriori seguenti verifiche

- verifica che il PdV normalizzato contenga l'indice IPdV e gli oggetti dati da esso referenziati;

- controllo di validità del file XML IdV;

- verifica di coerenza tra i nomi degli oggetti dati presenti nel PdV e i nomi degli oggetti dati dichiarati nel IdV;

- controllo della corretta valorizzazione dei campi ID e MIMEType dei files dichiarati nel IdV

Quale esito definitivo del versamento del PdV da parte del Produttore dei documenti, il sistema genera un Rapporto di Versamento che ha lo scopo di rappresentare una ricevuta di presa in carico per l'erogazione del Servizio in caso di esito positivo delle verifiche o una ricevuta di rifiuto e scarto dei PdV elaborati in caso di esito negativo delle verifiche.

[Torna al sommario](#)

7.3. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Il sistema Conservazione accetta i PdV e quindi il Conservatore si assume la responsabilità contrattuale di erogare il Servizio della Conservazione secondo gli SLA previsti dalla normativa e/o da quanto concordato con il Produttore nel Disciplinare Specificità del Contratto, esclusivamente se i Rapporti di Versamento prodotti sono con esito positivo in tal caso la sessione di acquisizione e presa in carico del processo è definitivamente conclusa e tracciata nel sistema di log.

Il IdV è un file XML, firmato digitalmente dal Responsabile del Servizio di Conservazione ovvero dei Delegati del Conservatore e a cui è stato associato un Riferimento Temporale riferito al Tempo Universale Coordinato (UTC), che viene generato automaticamente da un job con una periodicità che può essere settata e configurata nel profilo di conservazione del sistema Conservazione e per quel determinato Produttore.

Il IdV è univocamente identificato come tutti gli oggetti del sistema, contiene il riferimento al PdV verificato, contiene l'esito della verifica e contiene negli elementi agent tutti i soggetti che intervengono nella fase di generazione del IdV e sono parte del processo. I Rapporti di Versamento sono documenti informatici ed il Conservatore programma di portarli in conservazione periodicamente al fine di mantenere la prova della verifica eseguita.

I Rapporti di Versamento sono messi a disposizione del Produttore e degli Utenti autorizzati attraverso l'apposita interfaccia web based del sistema Conservazione, che tramite un filtro di ricerca, ne consente la visualizzazione attraverso un viewer dedicato e il download del file firmato digitalmente.

[Torna al sommario](#)

7.4. Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Il rifiuto di un Pacchetto di Versamento avviene attraverso la produzione di una mail di notifica trasmessa al Produttore tramite mail.

L'esito, invece, delle verifiche riepilogative sul PdV UNI SInCRO sono comunicate attraverso la generazione del IdV. La comunicazione avviene attraverso la produzione di una mail di notifica trasmessa al Produttore.

Il Produttore dei documenti ha l'obbligo di verificare il buon o cattivo esito del versamento attraverso la presa visione del IdV che il sistema mette a disposizione del Produttore e degli Utenti autorizzati attraverso l'apposita interfaccia web based del sistema Conservazione.

[Torna al sommario](#)

7.5. Preparazione e gestione del pacchetto di archiviazione

Il Pacchetto di Archiviazione (PdA) costituisce l'elemento indispensabile per il sistema di conservazione, in quanto rappresenta il contenitore di tutti gli elementi necessari per una conservazione a norma e di lungo termine. Secondo il piano di conservazione, configurato nel profilo del sistema in corrispondenza di ciascun Titolare e di ciascuna tipologia documentale, il processo di conservazione quindi si realizza appieno nel momento in cui viene apposta la firma digitale da parte del Responsabile del Servizio di Conservazione ovvero dei Delegati del Conservatore e la marca temporale sull'Indice del Pacchetto di Archiviazione.

La corretta generazione del Pacchetto di Archiviazione è presidiata e monitorata dai delegati operativi di Genesys Informatica Srl attraverso gli strumenti della console di controllo.

La firma digitale e la marca temporale apposte sull'IdC sono emesse, in conformità alla normativa vigente, da Certification Authority (CA) e da Time Stamping Authority, certificate da AgID e in conformità alla normativa vigente. Il sistema di conservazione sovrintende a tutte le fasi del processo tracciandone ogni attività svolta ed ogni azione nei file di log.

Il sistema controlla automaticamente la validità dei certificati al momento dell'apposizione della firma.

Ogni qualvolta sia eseguita un'operazione significativa ed a richiesta del delegato operatore viene controllata la validità delle firme, del certificato e l'integrità del documento informatico oggetto di sottoscrizione.

La connessione con la TSA per l'emissione delle marche temporali avviene tramite protocollo [HTTPS/SSL] cifrato per garantire la sicurezza e la riservatezza dell'operazione.

La marca temporale viene apposta dopo la firma del Responsabile del Servizio di Conservazione ovvero dei Delegati del Conservatore al fine di garantire una data opponibile a Terzi in cui la conservazione dei documenti era già avvenuta.

Il presidio operativo ed i controlli automatici del sistema Conservazione a completamento delle generazione del IdC garantiscono un intervento immediato degli operatori in caso di errori nell'apposizione della marca temporale.

[Torna al sommario](#)

7.6. Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

L'esibizione deve essere garantita dal sistema di conservazione e conforme a quanto previsto dall'articolo 10 del D.P.C.M. del 3 Dicembre 2013 e da ulteriore normativa di riferimento settoriale.

Ai fini della distribuzione agli Utenti autorizzati il Sistema di Conservazione deve permettere l'accesso diretto ai documenti conservati, anche da remoto, mediante specifica azione di ricerca e selezione dei documenti conservati, richiesta del PdD e successiva produzione di un Pacchetto di Distribuzione (PdD) firmato digitalmente dal Responsabile del Servizio di Conservazione ovvero di un delegato del medesimo.

In maggior dettaglio, tramite apposito accesso web accreditato, l'Utente può richiedere la visualizzazione di uno o più documenti conservati oppure può richiedere di scaricare il Pacchetto di Distribuzione.

Il Servizio richiede l'inserimento delle credenziali di accesso dell'utente e dei seguenti dati:

- Soggetto Titolare dei documenti;
- tipo di documento conservato da esibire;
- compilazione del filtro di ricerca, attraverso i metadati con cui i documenti sono stati indicizzati.

Il risultato della ricerca viene esposto in una vista che consente di:

- visualizzare i documenti ed i relativi metadati (eventualmente per consentire i controlli sulla leggibilità dei documenti) l'impronta hash di ciascuno (per permettere di controllare che il documento non sia stato modificato)
- selezionare i documenti da scaricare per comporre il Pacchetto di Distribuzione.

Quando l'Utente richiede il Pacchetto di Distribuzione, i documenti selezionati vengono resi disponibili, per un periodo di tempo prestabilito, come download (zippati), nella destinazione nota e condivisa per il recupero da parte del produttore.

Sull'Indice del Pacchetto di Distribuzione (IPdD) viene apposta la firma digitale del Responsabile del Servizio di Conservazione ovvero di un delegato del medesimo.

[Torna al sommario](#)

7.7. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

Il sistema di conservazione produce i duplicati informatici dei documenti conservati nel momento in cui genera il pacchetto di distribuzione e li inserisce al suo interno.

Tra le informazioni inserite nell'indice del pacchetto di distribuzione è presente l'impronta del file del documento conservato calcolata in fase di ricezione nel sistema di conservazione ed archiviazione nel dispositivo W.O.R.M ed il relativo algoritmo di calcolo.

Il sistema di conservazione rende disponibile una funzione per il prelievo dei PDD tramite il download dell'intero pacchetto.

L'utente che ne ha fatto richiesta può autonomamente confrontare l'impronta del file conservato duplicato ed inserito nel pacchetto di distribuzione con l'impronta inizialmente calcolata per accertarsi della correttezza.

Per quanto riguarda le copie informatiche e l'attestazione di conformità all'originale sono disciplinate interamente dalla normativa in materia con riferimento all'articolo 6 del 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.

Il sistema documentale in uso presso il Sistema Informativo della Fiscalità implementa una serie di funzionalità per supportare l'utente nella gestione di tale processo.

Nei casi è prevista, il responsabile della conservazione assicura la presenza di un pubblico ufficiale secondo l'Art. 7 delle regole tecniche in materia di conservazione al fine di dichiarare la conformità della copia all'originale conservato.

[Torna al sommario](#)

7.8. Scarto dei pacchetti di archiviazione

Il sistema di conservazione prevede specifiche funzionalità per effettuare lo scarto dei pacchetti di archiviazione in ordine al massimario di scarto.

Le attività di scarto dei documenti dal sistema di conservazione avvengono secondo le norme in materia ed in particolare, nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo.

Tali funzionalità supportano le operazioni previste per l'eliminazione di quei contenuti dell'archivio per i quali sono decorsi i termini di conservazione. Lo scarto è effettuato rispetto ai pacchetti di archiviazione. Le funzionalità disponibili permettono di effettuare le seguenti attività:

- Definire le strutture informative per memorizzare le operazioni di scarto;
- Analizzare l'archivio per individuare i pacchetti di archiviazione da scartare;
- Predisporre il report di scarto da sottoporre alla validazione del produttore dei documenti;
- Effettuazione dello scarto.

Da un punto di vista concettuale, un documento transita nella fase di scarto quando si avvicina la conclusione del periodo di conservazione previsto per quella tipologia di documento.

I pacchetti di archiviazione sono omogenei per tipologia di documento pertanto sono individuati in base ai medesimi criteri temporali.

Una volta che il pacchetto di archiviazione / documento è scartato non è più visibile nell'archivio di conservazione.

[Torna al sommario](#)

7.9. Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

Ai fini dell'interoperabilità tra i sistemi di conservazione sono stati adottati i seguenti criteri.

I formati adottati per gli oggetti documentali predisposti dal Sistema di conservazione e quelli ammessi per i documenti di cui è richiesta la conservazione da parte del produttore sono tutti presenti nell'allegato "Formati" delle regole tecniche a garanzia dei principi dell'interoperabilità tra i sistemi di conservazione

I pacchetti di archiviazione sono realizzati secondo i requisiti previsti nell'allegato "Specifiche tecniche del pacchetto di archiviazione", tali specifiche fanno riferimento allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che è lo standard nazionale riguardante la

struttura dell'insieme dei dati a supporto del processo di conservazione. In analogia allo standard SInCRO, la struttura utilizzata prevede una specifica articolazione per mezzo del linguaggio formale XML.

Tutti gli ulteriori pacchetti informativi progettati e realizzati per il Sistema di conservazione nonché le ricevute prodotte dal sistema, sono derivate da tale struttura standard e personalizzate per gli utilizzi specifici nel rispetto delle medesime regole adottate per i pacchetti di archiviazione.

[Torna al sommario](#)

7.10. Configurazione dei servizi di conservazione

Il Responsabile del servizio di conservazione dei documenti in collaborazione con il Responsabile della conservazione definisce le regole e le modalità di erogazione dei servizi di conservazione descritte nel documento "Specificità del contratto".

La definizione di tali regole prevede:

- la definizione dei profili da attribuire agli utenti delegati dal Responsabile della conservazione e le regole di visibilità degli oggetti conservati;
- ogni utente è associato ad un insieme di risorse che consentono di operare nel sistema di conservazione secondo particolari attività;
- le risorse associate a ciascun profilo possono essere all'occorrenza disattivate o riattivate;
- gli utenti sono delegati alle funzionalità di esibizione in relazione agli ambiti di competenza;
- la determinazione dei singoli servizi di conservazione caratterizzati da un insieme di tipologie documentali omogenee, ed in particolare devono essere definiti:
 - la natura ed eventuali specificità dei documenti da conservare;
 - i metadati dei documenti, obbligatori e opzionali;
 - le regole di assemblaggio dei pacchetti di archiviazione.

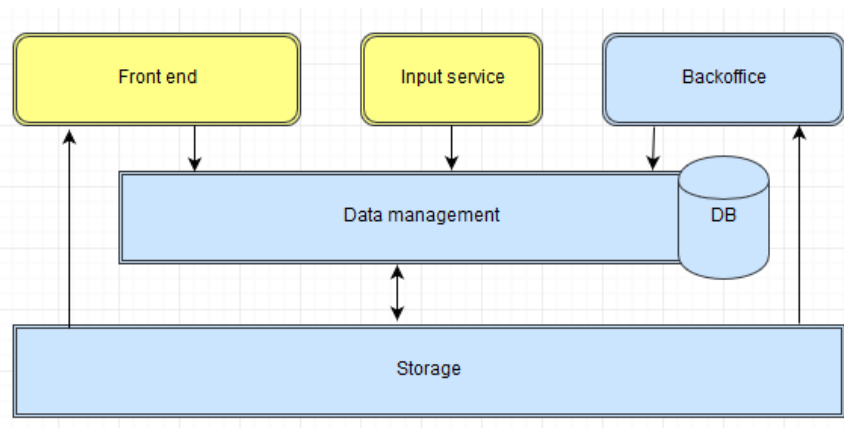
[Torna al sommario](#)

8. IL SISTEMA DI CONSERVAZIONE

Di seguito sono descritte le componenti del sistema di conservazione.

8.1. Componenti logiche

Di seguito è riportata la descrizione delle componenti logiche del sistema di conservazione rappresentata schematicamente nella figura seguente.

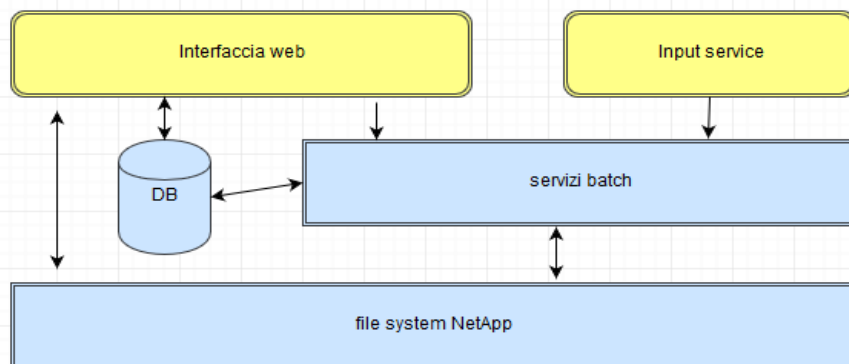


- Front-end Produttore/Utente; si tratta di un'interfaccia utente web che consente le interazioni da parte del Produttore/Utente con il sistema. Le funzioni del modulo di input sono presenti anche nel front-end, le due funzioni si completano a vicenda. Il front-end offre anche funzionalità di interrogazione del sistema e di esibizione.
- Input service; implementano le interfacce con le quali inviare i documenti al sistema di conservazione.
- Backoffice; si tratta di un'interfaccia web che consente le interazioni da parte del Conservatore e dei suoi delegati con il sistema. Per il monitoraggio e l'esecuzione di tutte le attività demandate al Conservatore.
- Data management; è l'entità funzionale dedicata alla interazione fra il Front-end ed il Backoffice con lo Storage. Gestisce l'indicizzazione dei documenti e successiva ricerca, memorizza su database i metadati e mantiene l'associazione tra ogni documento ed il pacchetto di pertinenza. Esplora il database ed esibisce la lista dei riferimenti corrispondenti. Produce i PdV, genera i PdA corredati di un PdD in formato UNI-SInCRO. E' sempre compito del Data management la generazione e messa a disposizione dei PdD richiesti dal Produttore
- Storage; è l'area di memorizzazione, basata su file system, in cui vengono memorizzati i documenti, i PdA con tutti i relativi file di cui sono composti.

[Torna al sommario](#)

8.2. Componenti tecnologiche

Di seguito è riportata la descrizione dell'infrastruttura tecnologica con la quale espletato il servizio:

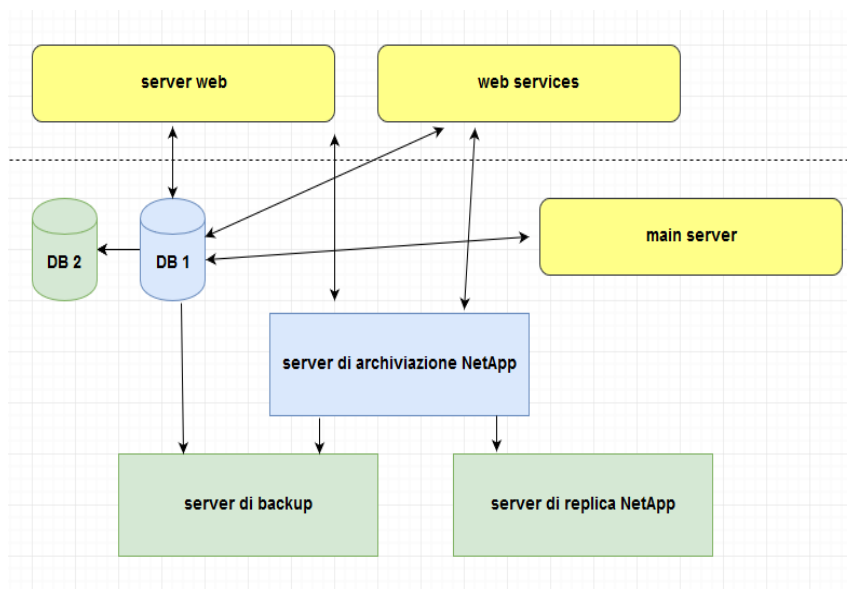


- l'interfaccia WEB è sviluppata in linguaggio PHP con un'interfaccia HTML, operante su protocollo HTTPS all'interno del web server Apache2. L'autenticazione è effettuata tramite un sistema di gestione di chiavi (criptate) ed utenze.
- input service si tratta delle funzionalità accessibili da applicazioni di terze parti per l'acquisizione di documenti ;
- DB all'interno del quale sono memorizzati i metadati, gli indici dei documenti, le anagrafiche dei vari soggetti interessati al processo e tutte le informazioni necessarie al funzionamento del sistema. Compresa la memorizzazione dei log degli eventi;
- servizi batch si tratta dei processi batch sono sviluppati in linguaggio PHP e messi in esecuzione su server ospitati nella farm. Preposti alla esecuzione di alcune attività massive che richiedono un dispendio di risorse e una attesa prolungata da parte dell'utente. Tutti i processi e attività di generazione dei PdA e dei PdD, nonché le funzioni di controllo di coerenza dei dati memorizzati. Il monitoraggio dei servizi viene effettuato attraverso il sistema di log e delle relative interfacce di controllo;
- file system è l'area di conservazione su supporti digitali dei file oggetto di conservazione e degli altri file generati dal sistema a corredo delle attività di espletazione del servizio.

[Torna al sommario](#)

8.3. Componenti fisiche

L'infrastruttura del Sistema di Conservazione dei documenti è realizzata sulla rete interna del Conservatore e dislocata nelle server farm di Genesys Informatica Srl. Essa è progettata per garantire i più elevati standard di qualità e sicurezza.



- server web; è il server esposto in internet al quale accedono i produttori/utenti, su questo server girano gli applicativi ad essi rivolti, è basato sull'utilizzo di soluzioni di virtualizzazione, operante su protocollo HTTPS collocato nella server farm primaria di Firenze;
- web services; è il server sulle quali girano le applicazioni API ad uso di altri software per colloquiare con il servizio di conservazione ed automatizzare alcune funzionalità, operante su protocollo HTTPS collocato nella server farm primaria di Firenze;
- main server; è il server principale, è basato sull'utilizzo di soluzioni di virtualizzazione, operante su protocollo HTTPS, è accessibile solamente dalla rete interna ed collocato nella server farm primaria di Firenze. Su questo server girano gli applicativi di manutenzione e controllo del servizio di archiviazione, nonché tutte le applicazioni di elaborazione batch;
- server di archiviazione; è il server dove sono memorizzati i file documenti e quelli generati dal sistema conservazione, basato su software e sistemi storage NetApp collocato nella server farm secondaria di Firenze;
- DB 1; è il server del data base primario, è basato sull'utilizzo di soluzioni di virtualizzazione (Xen), su di esso sono memorizzate tutte le informazioni necessarie al funzionamento del sistema. Vi girano i servizi di accesso e manutenzione del medesimo. Esso è collocato nella server farm primaria di Firenze;
- DB 2; è la replica sincrona del data base primario, è basato sull'utilizzo di soluzioni di virtualizzazione (Xen). Esso è collocato nella server farm primaria di Firenze;
- server di replica; è la replica sincrona del server di archiviazione, è basato su software e sistemi NetApp collocato nella server farm secondaria di Roma;
- server di backup; è il server che gestisce gli snapshot dei server virtualizzati (web server e DB 1), ed i backup del data base (di DB 1) e la copia dei documenti archiviati. I volumi di memorizzazione sono collocati nella server farm secondaria di Roma.

[Torna al sommario](#)

8.4. Procedure di gestione e di evoluzione

Tra le attività previste per la predisposizione del servizio di conservazione vengono effettuati i controlli miranti a verificare che siano state rispettate le specifiche definite e che il sistema di conservazione sia disponibile all'uso.

La verifica viene effettuata sotto la supervisione dal Responsabile del servizio di conservazione e da tutte le componenti organizzative appartenenti al Conservatore in base alle competenze specifiche.

I controlli consistono nella verifica:

- del software necessario all'erogazione del servizio in un ambiente di validazione funzionalmente analogo a quello di esercizio;
- della corretta esecuzione della configurazione dei singoli sistemi, secondo quanto riportato nell'apposita documentazione aziendale;
- della corretta apposizione delle firme digitali e delle marche temporali;
- della rispondenza del sistema di conservazione ai requisiti del sistema di gestione della sicurezza delle informazioni;
- dei test di funzionamento del sistema di Disaster Recovery esteso, per il quale in particolare si controlla la copertura della funzionalità di esibizione dei documenti conservati.

Il Responsabile dell'Infrastruttura, il Responsabile della Sicurezza dei sistemi per la conservazione e il Responsabile dei sistemi informativi per la conservazione vengono informati dei risultati dell'attività.

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

Il Conservatore programma ed attua meccanismi di monitoraggio e controllo ed esegue un processo di gestione degli incidenti, assicurando l'individuazione delle soluzioni tecniche e operative per la prevenzione, la rilevazione, la pronta reazione ed il monitoraggio degli incidenti fino alla loro risoluzione.

L'attività di monitoraggio applicativo sull'intero sistema di archiviazione prevede il controllo su di un apposito cruscotto che evidenzia il numero di documenti presenti e lo stato di elaborazione dei pacchetti, con la presenza di eventuali segnalazioni di anomalie. In caso di anomalie l'operatore innesca tutte le attività di verifica e risoluzione. Il Sistema prevede la tracciamento sui log del servizio delle attività svolte dagli Utenti, dagli Operatori e le attività svolte in automatico dal sistema di conservazione. Gli Operatori hanno accesso a tali informazioni in modo tale da monitorare il funzionamento del sistema e prevenire criticità del servizio.

Inoltre il servizio controlla in automatico:

- la scadenza del periodo di conservazione, indicata nel pacchetto, segnalando l'evento al Produttore in modo tale che questi possa richiedere l'estensione del periodo;
- per i documenti che necessitano di un periodo di conservazione superiore ai 20 anni, sotto la responsabilità del Responsabile della funzione archivistica di conservazione, è previsto il monitoraggio e aggiornamento delle scadenze delle marche temporali: poiché le marche temporali apposte dal processo di conservazione hanno validità di 20 anni, occorre monitorare la scadenza delle marche apposte sui pacchetti di archiviazione e apporre nuove marche a quelle in scadenza;
- verifica dell'integrità e della consistenza dei pacchetti e dei documenti;
- verifica dell'integrità dei meta dati e dei collegamenti con il documento ad essi abbinati;
- verifica dell'effettiva leggibilità dei documenti inseriti all'interno dei pacchetti. Per questa seconda procedura, il Conservatore, sotto la supervisione del Responsabile della Conservazione, con cadenza annuale verificherà che, per i formati dei file utilizzati per la conservazione dei documenti, sia disponibile un visualizzatore aggiornato e con forme al fine di garantire accesso e leggibilità.

I controlli di accesso logico adottati dall'Organizzazione del Conservatore per salvaguardare la sicurezza delle informazioni gestite all'interno del sistema di conservazione sono molteplici:

- l'accesso alla piattaforma Web del sistema di conservazione (front end Conservazione Cloud) è protetto da un modulo di autenticazione, basato sull'utilizzo di credenziali di accesso (username e password), a cui si accede esclusivamente utilizzando il protocollo HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer);
- gli Utenti sono responsabili della scelta, gestione, utilizzo e modifica delle proprie credenziali di accesso, nel rispetto dei vincoli imposti dalla password policy che rappresenta lo standard di sicurezza aziendale per la gestione delle password. I principi definiti all'interno di tale documento sono in linea con quanto richiesto anche dal Codice in

materia di protezione dei dati personali (D. Lgs. 196/03). Il sistema impone che le password abbiano dei requisiti minimi di sicurezza;

la piattaforma genera in autonomia i log necessari per monitorare la correttezza delle attività eseguite, sia a livello utente, sia a livello di utenze privilegiate, tracciando eventuali tentativi di compromissione. Tali log, oltre a consentire il monitoraggio delle operazioni di login e logout, come per altro richiesto anche dal Codice in materia di protezione dei dati personali (D. Lgs. 196/03), permettono anche la verifica delle operazioni eseguite dagli Amministratori di Sistema (e.g. modifica dei metadati, modifica parametri di configurazione);

- in casi specifici (e.g., 5 tentativi login falliti) è prevista la generazione di allarmi automatici che consentono di intervenire tempestivamente nelle fasi di contenimento e contrasto di un eventuale incidente di sicurezza informatica. Ulteriori dettagli sono riportati nel Piano della Sicurezza;
- i sistemi anti-intrusione, come i Firewall, sono posizionati all'interno del segmento di rete che collega la piattaforma Conservazione Cloud con internet, al fine di intercettare ogni eventuale azione malevola volta a degradare, parzialmente o totalmente, l'erogazione del Servizio;
- il fornitore della connettività fornisce anche protezione da attacchi volumetrici "ddos";
- la generazione dell'utenza avviene in conformità con le direttive indicate all'interno della procedura di controllo accessi, garantendo il rispetto dei principi di Segregation of Duties e Need to Know, come illustrato anche all'interno del Piano della Sicurezza;

o la fase di inserimento di una nuova utenza interna (e.g., Operatore, Amministratore), avviene previa richiesta formale da parte di una figura individuata e riconosciuta come responsabile dell'utente, la quale ha l'obbligo di specificare alcuni dati tra i quali il ruolo ed il profilo richiesto nel rispetto delle regole definite all'interno dell'apposita "Matrice ruoli – profili – attività" predisposta dall'Organizzazione;

o per le utenze esterne (e.g., Clienti), a seguito dell'adesione al Servizio e il controllo di integrità e correttezza della documentazione contrattuale firmata, si procede con l'invio delle credenziali agli Utenti, ponendo l'obbligo del cambio password al primo

[Torna al sommario](#)

9.1. Procedure di monitoraggio

I log del servizio

Conservazione Cloud vengono gestiti in accordo alla procedura di log management, in cui sono dettagliate le misure tecniche ed organizzative previste per una corretta gestione dei log stessi.

Sulla base di quanto definito all'interno di tale procedura, i file di log sono classificati al fine di differenziarne la gestione, in base alla categoria di appartenenza.

Sono previsti tre livelli di classificazione in funzione della natura degli eventi/attività tracciate. La piattaforma centralizzata garantisce una serie di requisiti tecnici per la gestione sicura dei log, tra i quali:

- completezza, inalterabilità dei log;
- completa tracciabilità di tutti gli accessi (Login) e di tutte le disconnessioni (Logout) eseguite da tutte le utenze;
- conservazione, per almeno 12 mesi;
- replica del data base contenente i log.

[Torna al sommario](#)

9.1.1. Monitoraggio funzionale

monitoraggio funzionale è svolto tramite un'applicazione di data warehouse che consente il monitoraggio del processo di conservazione, in base alle fasi principali:

- Ingestion dei documenti;
- Acquisizione dei documenti nel W.O.R.M.;
- Firma dei pacchetti di archiviazione;
- Conservazione dei documenti;

con l'obiettivo di fornire, per mezzo di statistiche predefinite, un punto di vista sulla situazione corrente (ultimo mese elaborato) e storica (tutto il periodo di tempo della gestione del processo) del fenomeno osservato.

L'applicazione di monitoraggio è accessibile dopo l'identificazione dell'utente e, in relazione al profilo, è possibile accedere alle diverse aree di consultazione ed alla reportistica.

Il monitoraggio è disponibile a tutti i Responsabili della conservazione e relativi delegati, al Responsabile del servizio di conservazione e alle strutture organizzative del Responsabile del servizio di conservazione.

[Torna al sommario](#)

9.1.2. Monitoraggio operativo

Il monitoraggio operativo è svolto dal Responsabile dei sistemi informativi per la conservazione e dai Tecnici della conservazione ed ha l'obiettivo di tenere sotto controllo le fasi di acquisizione, assemblaggio nei pacchetti di archiviazione, apposizione della firma digitale e conservazione dei documenti.

In particolare i controlli effettuati si dividono in:

- Monitoring, effettua i controlli rispetto alla permanenza negli stati di lavorazione e relativamente ai documenti che si trovano nello stato acquisito, da firmare e firmato;
- Quadratura, sulla base di un intervallo temporale, calcola il totale dei documenti per i quali è stato richiesto il processo di conservazione, evidenziando il numero di documenti acquisiti, assemblati, firmati, conservati e cancellati;
- integrità referenziale, esegue i controlli di bilanciamento dei pacchetti di archiviazione, dei documenti e dei relativi metadati presenti nelle basi dati memorizzate. Le statistiche e l'esito dei controlli sono messi a disposizione del Responsabile del servizio di conservazione, del Responsabile dei sistemi informativi per la conservazione e del Responsabile della Sicurezza dei sistemi per la conservazione. Il Responsabile dei sistemi informativi per la conservazione e i Tecnici della conservazione dispongono di un cruscotto riferito allo stato della conservazione che permette di monitorare il processo che governa i documenti per i quali è stata richiesta la conservazione digitale dalla fase di acquisizione fino alla fase di conservazione dei pacchetti di archiviazione: La composizione del cruscotto prevede la suddivisione in più parti sia a livello di report statistici, che delle informazioni necessarie al controllo del processo elaborativo, in particolare:
 - numero dei documenti presenti, indicazione degli incrementi rispetto alla fine del mese precedente ed alla fine dell'anno precedente;
 - classificazione ed indicazione del numero dei pacchetti prodotti alla data corrente, suddivisi nei diversi stati di lavorazione:
 - richiesta archiviazione;
 - RdV generato;
 - RdV in firma;
 - RdV firmato;
 - PdA generato;
 - PdA in firma;
 - PdA firmato e marcato;
 - PdA completato;
 - gli Operatori hanno a disposizione ulteriori schermate nelle quali per ciascun item può essere ulteriormente esploso, visualizzando il singolo pacchetto con le relative informazioni per verificare la presenza di anomalie ed i tempi di esecuzione delle singole attività.

Effettuando l'analisi delle informazioni dei report è possibile per l'addetto e per gli utenti interni interessati, verificare l'andamento dell'intero processo della conservazione digitale.

[Torna al sommario](#)

9.1.3. Monitoraggio dello stato delle componenti infrastrutturali

L'infrastruttura del sistema di conservazione è sottoposta ad un sistema di monitoraggio dedicata alle strutture organizzative del Responsabile della conservazione e del Responsabile dell'infrastruttura con i seguenti obiettivi:

- controllo delle componenti di base come riempimento filesystem, carico elaborativo, guasti device HW;
- controllo del database gestito attraverso procedure in uso per il monitoraggio dei data server delle applicazioni in esercizio;

- controllo dello stato delle macchine virtuali attraverso i sistemi di gestione e monitoraggio dell'interfaccia di XenCenter;
- controllo automatico dei sistemi NetApp tramite i propri meccanismi di controllo ed allarme e del monitoraggio effettuato dalla centrale di controllo di NetApp.

Il verificarsi di criticità software ed hardware viene comunicato automaticamente dal sistema agli operatori mediante avvisi, con la relativa memorizzazione nello storico degli eventi. Il tracciamento di login e logout è effettuato dalla struttura organizzativa del Responsabile dell'infrastruttura.

[Torna al sommario](#)

9.2. Verifica dell'integrità degli archivi

Il sistema di conservazione per la verifica periodica degli archivi prevede le tipologie di verifica seguenti:

- Calcolo dell'impronta e confronto con l'ultima memorizzata;
- Verifica del formato.

Ciascuna delle tipologie di verifica è effettuata da un apposito componente di sistema che effettua la verifica secondo l'anzianità di acquisizione ed il periodo di conservazione richiesto. La verifica viene effettuata a discrezione del Responsabile della conservazione. Può essere eseguita a campione oppure in maniera totale, ogni pacchetto viene comunque verificato totalmente almeno una volta all'anno.

L'esecuzione delle verifiche è registrata nell'archivio delle verifiche periodiche del sistema di conservazione con il relativo esito. In caso di esito non positivo viene inviata una mail al Responsabile del servizio di conservazione e ad un Delegato del medesimo.

Ogni qualvolta il Sistema riscontra una non conformità in merito alla leggibilità o all'integrità di un documento memorizzato, si attivano le procedure interne di sicurezza, che prevedono la verifica dei supporti e dell'infrastruttura interessata, con la successiva ricostruzione degli indici e dei pacchetti a partire dalla copia ancora integra.

[Torna al sommario](#)

9.3. Soluzioni adottate in caso di anomalie

Si definisce incidente di sicurezza, qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell'organizzazione o l'integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite, o le leggi in vigore (con particolare riferimento al D. lgs. 196/2003, alla L. 547/1993 ed alla L. 38/2006).

In merito alle anomalie che si potessero verificare per il servizio di conservazione erogato le procedure adottate sono conformi al piano aziendale di sicurezza secondo le procedure ISO 27001/2013 nel quale sono analizzate le criticità e le attività pianificate di intervento. Allo scopo di assicurare che i disservizi siano gestiti in modo rapido, efficiente e con il minimo disagio per l'Utente del servizio.

L'Utente ha a disposizione il sistema di ticketing di Genesys Informatica Srl per segnalare anomalie o problemi di funzionamento, il sistema traccia le comunicazioni intercorse fra Utenti ed Operatori sino alla risoluzione. Periodicamente questi vengono valutati per frequenza e criticità dal Responsabile del servizio di conservazione che predispone le contromisure necessarie.

[Torna al sommario](#)