Manuale di Conservazione dei Documenti Informatici di

Salerno Pulita S.p.A.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione		Carmela Fabiano	
Verifica			
Approvazione			Amministratore Unico Dott. V. Bennet

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Ver 1.0		Prima emissione	

La presente versione del Manuale della Conservazione è suscettibile di ulteriori modifiche qualora il mutato quadro normativo o l'evoluzione tecnologica ne rendano necessaria la revisione

Indice

1 INTRODUZIONE

1.1 Scopo e ambito del documento

Il presente documento è il *Manuale di conservazione* (d'ora in poi Manuale) dei documenti digitali applicato **da Salerno Pulita S.p.A. (**d'ora in poi **Ente)** come soggetto **produttore** (d'ora in poi ***Produttore***) che intende sottoporre a conservazione digitale alcune tipologie documentali, affidando il processo di conservazione ad **InfoCert S.p.a. *, conservatore accreditato AgID come da Circolare AgID N.65/2014,*** di seguito indicato come ***Conservatore.*** L'accordo tra **Salerno Pulita S.p.A.** e ***InfoCert S.p.A.*** per l'affidamento in *outsourcing* del processo di conservazione è stato formalizzato da parte dell' **Ente** mediante sottoscrizione del contratto di adesione al servizio **LegalDoc**.
Il presente Manuale integra, per le parti specifiche di competenza del Produttore e per quanto riguarda i rapporti tra questi ed il Conservatore, il Manuale di Conservazione dello stesso, allegato al presente documento.
L'indice rimanda ai capitoli e ai paragrafi del Manuale del Conservatore non modificati o integrati dal presente Manuale.
In particolare il presente Manuale descrive il modello organizzativo della conservazione adottato e illustra nel dettaglio l'organizzazione del processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di conservazione. Descrive inoltre il processo, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del Sistema di conservazione.
Per le tipologie degli oggetti sottoposti a conservazione e i rapporti con il soggetto che realizza il processo di conservazione, il presente Manuale è integrato con il **Disciplinare tecnico**, che definisce le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei Documenti informatici e delle Aggregazioni documentali informatiche oggetto di conservazione.
Il Disciplinare tecnico è formato da specifiche parti relative alle diverse **tipologie documentarie** oggetto di conservazione ed è compilato tenendo conto delle indicazioni contenute nella documentazione redatta da **InfoCert S.p.a**..

1.2 Principi di redazione

La redazione del Manuale di Conservazione è ispirata ai seguenti principi:

- **Principio di Trasparenza**, il Manuale mira a fornire una chiara spiegazione del sistema di conservazione documentale e dei processi erogati;
- **Ottica di processo**, il documento mira a descrivere le fasi del processo, non il dettaglio tecnico degli strumenti utilizzati, ad uso interno e a fini ispettivi;
- **Principio di Rilevanza**: nel Manuale sono contenute solamente le informazioni rilevanti, con un livello di dettaglio mirante ad agevolare le ispezioni, senza dettagli tecnici superflui;
- **Principio di Accuratezza**: le informazioni sono state revisionate da più persone, poste ai diversi livelli della catena decisionale.

1.3 Rimandi al Manuale della Conservazione redatto da InfoCert S.p.A.

Si rimanda al Manuale della Conservazione di ***InfoCert S.p.a.*** per i seguenti argomenti:

- *Glossario e termini di riferimento*
- *Ruoli e Responsabilità interne ad **InfoCert S.p.a.** del processo di conservazione*
- *Il sistema di conservazione – descrizione tecnica e tecnologica dell'architettura*
- *Descrizione delle procedure di verifica, monitoraggio e controllo*
- *Descrizione del processo di ricerca ed esibizione*
- *Misure di sicurezza fisiche e logiche.*

1.4 Normativa di riferimento

Vedi documento Allegato 1

2 MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE: RUOLI E RESPONSABILITÀ

2.1 Sistema e Attori

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile del servizio di conservazione	Funzione esercitata dal ***Conservatore Nicola Maccà***		A decorrere dall'adesione al servizio LegalDoc
Responsabile della conservazione del Produttore	Funzione esercitata dal Conservatore Carmela Fabiano		A decorrere dal 09/06/2021 condetermina n. AU10167
Responsabile della gestione documentale del Produttore	Funzione esercitata dal Conservatore Carmela Fabiano		A decorrere dal 09/06/2021 con determina n. AU10167
Responsabile Sicurezza dei sistemi per la conservazione	Funzione esercitata dal ***Conservatore Giovanni Belluzzo***		A decorrere dalla data di adesione al servizio LegalDoc
Responsabile funzione archivistica di conservazione	Funzione esercitata dal ***Conservatore***		A decorrere dalla data di adesione al servizio LegalDoc
Addetto funzione archivistica di conservazione del Conservatore	**Marta Gaia Castellan**	Esecuzione dei versamenti	A decorrere dalla data dell'atto interno d'individuazione del ruolo e della persona incaricata
Titolare del trattamento dei dati personali	**Salerno Pulita S.p.A.**		Dalla data del provvedimento d'individuazione del titolare
Responsabile esterno del trattamento dei dati personali	***Esposito Alfredo*** (nell'ambito delle funzioni esercitate dal ***Conservatore***)		Dalla data dell'atto di nomina
Responsabile sistemi informativi per la conservazione	Funzione esercitata dal ***Conservatore***		A decorrere dalla data di adesione al servizio LegalDoc
Responsabile sviluppo e manutenzione del sistema di conservazione	Funzione esercitata dal ***Conservatore***		A decorrere dalla data di adesione al servizio LegalDoc

2.2 Produttore

Nei Dati Tecnici e contrattuali allegati al presente Manuale il '**Produttore**' è il ***Soggetto Produttore*** dell'archivio digitale.
I recapiti e i riferimenti amministrativi e anagrafici del ***Produttore/Soggetto Produttore*** sono di seguito riportati:

Produttore/Soggetto Produttore	**Salerno Pulita S.p.A.**
Sede Amministrativa	**Via Tiberio Claudio Felice 18/bis – 84131 Salerno (SA)**
Recapiti	**+39 081 7722111**
Sito web	www.salernopulita.it
PEC	protocollo@pec.salernopulita.it
Partita IVA	**03306830658**

2.3 Conservatore

Ai fini dell'esecuzione del Servizio di conservazione dei documenti informatici del Produttore, la società **Infocert S.p.A.** è **identificata quale fornitore del Servizio di conservazione.**
Per ulteriori informazioni si rimanda al "Manuale del Sistema di Conservazione" di ***InfoCert S.p.A. in allegato.***

2.4 Utente

In base alla definizione del glossario allegato alle vigenti ***Regole tecniche*** si identifica come *Utente* una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione dei *Documenti informatici* al fine di fruire delle informazioni di interesse.
L'*Utente* richiede al *Sistema di conservazione* l'*accesso* ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il *Sistema di conservazione* permette ai soggetti autorizzati l'*accesso* diretto, anche da remoto, ai *Documenti informatici* conservati e consente la produzione di un *Pacchetto di distribuzione* direttamente acquisibile dai soggetti autorizzati.
In termini ***OAIS*** la comunità degli *Utenti* può essere definita come ***Comunità di riferimento***.
Nel ruolo dell'*Utente* si possono definire al momento solo specifici soggetti abilitati del *Produttore*, in particolare gli operatori indicati dal *Produttore* e riportati nel ***Disciplinare tecnico***, che possono accedere esclusivamente ai documenti versati dal *Produttore* stesso o solo ad alcuni di essi secondo le regole di visibilità e di *accesso* concordate tra ***InfoCert S.p.A*** e il *Produttore.*
Si identificano gli utenti del Sistema di conservazione nelle seguenti persone:
- Carmela Fabiano, responsabile della conservazione del Produttore;

Nel seguito del documento detti utenti sono referenziati nei ruoli "***Responsabile della Conservazione***" e "***Collaboratore Responsabile della Conservazione***".
L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione utenze indicate nel *Piano della sicurezza del sistema di conservazione* e nel rispetto delle misure di sicurezza previste negli articoli da 31 a 36 del D.lgs 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1 e dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B del medesimo decreto.

2.5 Responsabile della conservazione

Il ruolo di responsabile della conservazione del *Produttore* è in capo alla sig.ra ***Carmela Fabiano***.
Il responsabile della conservazione definisce le policies di conservazione del *Produttore*.
Il *Responsabile della conservazione* inteso come ente conservatore o come soggetto che svolge attività di conservazione, è identificato in ***InfoCert S.p.A***. , che svolge tale attività tramite il proprio servizio denominato **LegalDoc.**
Gli obiettivi di ***InfoCert S.p.A***.sono:

- ***Garantire la conservazione, archiviazione e gestione dei Documenti informatici e degli altri oggetti digitali;***
- ***Erogare servizi di accesso basati sui contenuti digitali conservati;***
- ***Fornire supporto, formazione e consulenza al Produttore per i processi di dematerializzazione.***

Di fatto, quindi ***InfoCert S.p.A***. si impegna alla *conservazione* dei documenti trasferiti e ne assume la funzione di *Responsabile della conservazione* ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione, e svolge, tramite la propria struttura organizzativa e di responsabilità, l'insieme

delle attività elencate nell'articolo 7 comma 1 delle ***Regole tecniche***, in particolare quelle indicate alle lettere a), b), c), d), e), f), g), h), i), j), k)e m).

2.6 Organismi di tutela e vigilanza

"Lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art. 21, c. 1, lettera b).
Anche "Il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e).
La disposizione si applica anche:

- *all' affidamento a terzi dell'archivio (outsourcing), ai sensi del D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e)*
- *al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico.*

In adempimento alle citate disposizioni normative, il presente Manuale di conservazione è assoggettato alla approvazione della Soprintendenza per i Beni culturali della Provincia di Salerno.
In base alle *Regole tecniche* i sistemi di conservazione delle pubbliche amministrazioni ed i sistemi di conservazione dei conservatori accreditati sono soggetti alla vigilanza dell'AGID, e per tale fine il *Sistema di conservazione* di *InfoCert S.p.A*. prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede del *Produttore*.

3 STRUTTURA ORGANIZZATIVA PER IL SISTEMA DI CONSERVAZIONE

3.1 Organigramma

Il versamento in conservazione dei documenti informatici gestiti nella fase corrente dalle articolazioni amministrative (UO) del Produttore è effettuato unicamente dai ruoli "Responsabile della conservazione" e "Collaboratore Responsabile della conservazione" del sistema di gestione documentale, all'interno dei quali sono configurati gli utenti indicati nel ***paragrafo 2.4*** .

3.2 Strutture organizzative

Il servizio di conservazione dei documenti informatici del *Produttore* è attivato sulla base dell'accordo stipulato con ***InfoCert S.p.A.*** mediante sottoscrizione del contratto di adesione al servizio **LegalDoc in data 14.12.2020.**

Il *Produttore* invia i pacchetti di versamento al sistema di conservazione utilizzando i ruoli 'Responsabile della conservazione' e 'Collaboratore Responsabile della conservazione' del sistema di gestione documentale in uso.

3.3 Compiti di InfoCert

3.3.1.1 Compiti Organizzativi

InfoCert provvede alla realizzazione di una base di dati relativa ai documenti informatici che il Produttore versa in conservazione, gestita secondo i principi di sicurezza illustrati nel proprio ***Manuale*** e nel ***Contratto LegalDoc*** ed attuati adottando procedure di tracciabilità tali da garantire la corretta conservazione, l'accessibilità a ogni singolo documento e la sua esibizione.
InfoCert si occupa altresì di definire:

- *le caratteristiche ed i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare e organizzare gli stessi in modo da garantire la corretta conservazione e la sicurezza dei dati, anche al fine di poterli prontamente produrre, ove necessario;*
- *le procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l'esecuzione operativa di conservazione.*
- *le procedure informatiche ed organizzative per la corretta tenuta dei supporti su cui vengono memorizzati i documenti informatici oggetto di conservazione.*

- *le procedure informatiche ed organizzative atte ad esibire la documentazione conservata, in caso di richieste formulate da chi ne abbia titolo.*

3.3.1.2 Compiti di Manutenzione e Controllo

InfoCert provvede a:

- *Mantenere un registro cronologico del software dei programmi in uso nelle eventuali diverse versioni succedute nel tempo ed un registro cronologico degli eventi di gestione delsistema di conservazione comprensivo delle risoluzioni adottate per rimuovere eventuali anomalie;*
- *Implementare specifici controlli di sistema per individuare e prevenire l'azione di software che possano alterare i programmi ed i dati;*
- *Verificare la corretta funzionalità del sistema e dei programmi in gestione;*
- *Analizzare e valutare periodicamente la registrazione degli eventi rilevanti ai fini della sicurezza (analisi del log di sistema);*
- *Definire e documentare le procedure di sicurezza darispettare per l'apposizione del riferimento temporale;*
- *Mantenere e gestire i dispositivi di firma in conformità con le procedure stabilite dal certificatore qualificato che ha rilasciato i relativi certificati;*
- *Verificare la validità delle marche temporali utilizzate dal sistema di conservazione;*
- *Verificare il buon funzionamento del file system.*

3.3.1.3 Compiti Operativi

InfoCert effettua le seguenti attività:

- *Supervisione dell'intero sistema di conservazione digitale, verificando accuratamente i processi di apposizione delle firme digitali, dei riferimenti temporali e delle marche temporali, in modo che la procedura rispetti la normativa, assicurandosi che tutto il processo si realizzi secondo le procedure descritte nel Manuale;*
- *Sincronizzazione dell'ora di sistema di tutti i sistemi utilizzati, verifica e controllo della sincronizzazione del clock di sistema per consentire registrazioni accurate e comparabili tra loro;*
- *Mantenimento della documentazione descrittiva del processo di conservazione aggiornata nel corso del tempo;*

3.3.1.4 Compiti per la protezione dei dati e delle procedure informatiche

InfoCert è garante, attraverso i suoi delegati, di tutte le misure necessarie per la sicurezza fisica, logica e ambientale dei dati e del sistema preposto alla loro conservazione, comprensivo delle copie di sicurezza dei supporti di memorizzazione, al fine di proteggere le informazioni da possibili violazioni in termini di riservatezza, integrità e disponibilità delle informazioni stesse.
Dovrà quindi predisporre e verificare che gli strumenti informatici in dotazione siano protetti secondo criteri che dovranno essere sempre aggiornati, con la tecnologia e la normativa di tutela della privacy, per garantirne il corretto funzionamento contro i cosiddetti ***malicious code*** e contro gli accessi non autorizzati sia logici che fisici.
E' altresì responsabile della definizione ed adozione, attraverso un'analisi del rischio, degli appropriati controlli di sicurezza delle informazioni.

3.4 Pubblico ufficiale

Nei casi previsti dalla normativa, il ruolo di pubblico ufficiale è svolto dal Responsabile della Conservazione in qualità di dirigente dell'ufficio responsabile della conservazione dei documenti, o da altri dallo stesso formalmente designati, quale il Responsabile della Funzione archivistica di conservazione per l'attestazione di conformità all'originale di copie di *Documenti informatici* conservati.
Il ruolo di pubblico ufficiale, per i casi in cui è previsto l'intervento di soggetto diverso della stessa amministrazione, sarà svolto da altro dirigente all'uopo individuato o da altro soggetto da quest'ultimo designato.

4 TIPOLOGIE DEI DOCUMENTI POSTI IN CONSERVAZIONE

4.1 Premessa

L'**Ente** si è concentrato, in questa prima fase di redazione del documento, sulle modalità di conservazione sui seguenti tipi di documenti:

- ***Registro di protocollo informatico,***
- ***Documenti Protocollati.***

A regime <u>tutti</u> i documenti informatici trattati dall'Ente dovranno essere posti in conservazione.
Il presente documento sarà assoggettato ad aggiornamento sia per integrare le modifiche che si renderanno necessarie a seguito di modifiche alla normativa vigente sia per aggiungere altre tipologie di documenti, che per la loro natura procedimentale, non possono essere integrati con le procedure informatiche al momento adeguate per la conservazione a norma.

Nel ***Disciplinare Tecnico*** allegato sono riportate le informazioni di dettaglio per le tipologie documentali poste in conservazione.

4.2 Fasi del Processo di Conservazione e Responsabilità

Il servizio di conservazione digitale dei documenti informatici predisposto dal Conservatore risponde alla esigenza di conservare documenti informatici della Pubblica Amministrazione.
Il servizio permette di conservare i documenti informatici del Produttore, garantendone l'integrità e la validità legale nel tempo nonché la loro "esibizione a norma".

Il sistema di conservazione opera secondo i modelli organizzativi esplicitamente concordati che garantiscono la sua distinzione logica dal sistema di gestione documentale del Produttore.
Pertanto, la conservazione non viene svolta all'interno della struttura organizzativa del Produttore (soggetto titolare dei documenti informatici da conservare), ma è affidata ad InfoCert, che espleterà le attività per le quali ha ricevuto formale delega, nei limiti della stessa e per le quali opera in modo autonomo e ne è responsabile.

La sequenza di attività che vanno dalla fase propedeutica alla formazione dei documenti informatici alla fase di conservazione degli stessi è di seguito schematicamente rappresentata:

Sistemi	**Fase**	**Descrizione e MACRO FASI del processo di conservazione**	**Attività a carico di: Produttore/Conservatore**	
Sistema di gestione documentale del Produttore	1	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati	X	
	2	Produzione del pacchetto di versamento	X	
	3	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati	X	
Servizio di Fatturazione PA e PEC	1a	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati		X
	2a	Produzione del pacchetto di versamento		X
	3a	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati		X
Sistema di Firma Digitale	4	Servizio di Firma Automatica e di eventuale apposizione marca temporale, da effettuare sui documenti tributari prima dell'invio al sistema di conservazione.	X	X
Sistema di conservazione digitale dei documenti informatici	5	Acquisizione da parte del sistema di conservazione del pacchetto di versamento prodotto dal Produttore per la sua presa in carico		X

	6	Verifica che il pacchetto di versamento ed i documenti informatici in esso descritti siano coerenti e conformi alle prescrizioni stabilite dal Contratto di servizio		X
	7	Eventuale rifiuto del pacchetto di versamento o dei documenti informatici, nel caso in cui le verifiche di cui alla fase 6		X
	8	Generazione, in modo automatico, del rapporto di versamento relativo a ciascun pacchetto di versamento		X
	9	Invio al Produttore del rapporto di versamento		X
	10	Preparazione e gestione del pacchetto di archiviazione		X
	11	"Chiusura" del pacchetto di archiviazione mediante sottoscrizione con firma digitale di INFOCERT e apposizione di marca temporale		X
	12	Richieste di esibizione dei documenti informatici conservati	X	
	13	Preparazione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente con tutti gli elementi necessari a garantire l'integrità e l'autenticità degli stessi		X
	14	Richiesta del Produttore di duplicati informatici	X	
	15	Produzione di duplicati informatici su richiesta del Produttore	X	

4.3 Documenti informatici e aggregazioni documentali informatiche

Il *Sistema di conservazione* gestito da InfoCert (Sistema), conserva *Documenti informatici*, in particolare documenti amministrativi informatici, con i *metadati* ad essi associati e le loro *Aggregazioni documentali informatiche*.

I *Documenti informatici* e le loro *Aggregazioni documentali informatiche* sono trattati nel sistema nella forma di ***Unità documentarie*** e ***Unità archivistiche*** e sono inviati in conservazione sotto forma di *Pacchetti di versamento* (SIP), che contengono sia i documenti che i relativi *metadati*.

I *Documenti informatici* (***Unità documentarie***) sono suddivisi in ***tipologie documentarie***, che identificano gruppi documentali omogenei per natura e funzione giuridica, modalità di registrazione o di produzione.
Tale suddivisione è funzionale all'individuazione, per ogni singola ***tipologia documentaria***, di set di *metadati* standard e di articolazioni o strutture di composizione omogenee.
Per ogni tipologia documentaria InfoCert definisce:

- **il set dei metadati descrittivi da inserire nei SIP, ritenuti essenziali per la corretta conservazione dei documenti, in coerenza con quanto stabilito nell'Allegato 5 delle Regole tecniche;**
- **l'articolazione o struttura di riferimento della corrispondente Unità documentaria ai fini della predisposizione del SIP per l'invio al Sistema di conservazione;**
- **le indicazioni operative per la produzione del SIP e l'invio dello stesso al Sistema.**

Da tali documenti di analisi sono derivate le specifiche operative per la creazione e trasmissione dei SIP relativi alle varie tipologie documentarie contenute nel Disciplinare tecnico concordato con il Produttore.

5 PROCESSO DI CONSERVAZIONE

5.1 Premessa

Il Produttore, al momento dell'invio in conservazione, associa ad ogni documento informatico (Rif. Allegato 5 Metadati al DPCM del 2013), un file dei parametri di conservazione e un file di indici entrambi di tipo XML.
Al documento viene inoltre associato dal sistema di conservazione un file di ricevuta (file IPdA, ovvero un Indice del pacchetto di archiviazione) nonché un identificativo univoco generato dal sistema stesso, definito token.
Il file IPdA, firmato dal Responsabile della Conservazione e marcato temporalmente, attesta la correttezza del processo, e dà certezza al momento temporale
La struttura del file IPdA rispecchia quanto richiesto nell'Allegato 4 del DPCM del 2013.

Il documento rappresenta l'unità minima di elaborazione nel senso che viene memorizzato ed esibito come un tutt'uno; non è possibile estrarre dal sistema parti di un documento.

Un documento conservato presso il sistema di conservazione, quindi, ha le seguenti caratteristiche:

- è costituito da un file;
- è memorizzato sui supporti previsti dalla procedura di conservazione;
- è identificato in maniera univoca attraverso il token;
- è conservato insieme al file dei parametri di conservazione, al file di indici del documento e al file di ricevuta (file IPdA).

Come stabilito dai già citati Decreti del 3 dicembre 2013 e del 17 giugno 2014, i documenti sono statici e non modificabili, ovvero sono redatti in modo tale per cui il contenuto non è alterabile durante le fasi di conservazione ed accesso, e sono immutabili nel tempo.
In pratica, il documento non contiene macroistruzioni né codici eseguibili.
Le caratteristiche di staticità ed immodificabilità del documento inviato al sistema di conservazione digitale sono assicurate dal Produttore.
Per il formato dei file conservabili nel sistema di conservazione si rinvia al "Manuale del Sistema di conservazione" di InfoCert .

5.2 Definizione dei pacchetti

In generale si definisce *'pacchetto'* un contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
Nell'ambito del processo di conservazione distinguiamo tra:

a) "***Pacchetto di versamento***" - insieme di documenti che il Produttore invia al sistema di conservazione in una sessione, ognuno corredato dall'IPdA;
b) "***Pacchetto di archiviazione***" - un pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento. Ad ogni documento il Sistema di conservazione associa un file XLM, detto Indice del Pacchetto di Archiviazione (IPdA). L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto è detto ***rapporto di versamento***.
c) "***Pacchetto di distribuzione***" - un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta, ovvero è la risposta alla ricerca effettuata dal Produttore tramite interfaccia disponibile, che porta all'esibizione del documento conservato. Il documento da esibire è accompagnato sempre dall'IPdA.

5.3 Fasi del versamento e logiche di conservazione

Il *processo di conservazione* si basa su di una logica di conservazione caratterizzata dal ***versamento*** da parte del *Produttore* degli oggetti da conservare (*Documenti informatici* e *Aggregazioni documentali informatiche*) secondo la tempistica seguente:

1) la stampa giornaliera dei registri (di protocollo e di repertorio) entro la giornata lavorativa successiva a quella della registrazione;
2) le fatture attive, passive e gli altri documenti contabili entro i termini previsti dalla normativa di settore;
3) tutti gli altri documenti non oltre 12 mesi dalla data di registrazione degli stessi nel sistema di gestione documentale.

5.4 Presa in carico dei pacchetti di versamento

Relativamente alle funzioni di:

a) Invio al sistema di conservazione del pacchetto di versamento

b) Validazione del pacchetto di versamento
c) Descrizione del rapporto di versamento

si rimanda al "Manuale del Sistema di conservazione" di InfoCert.

5.4.1 Descrizione del processo di conservazione

Il sistema di conservazione permette di mantenere e garantire nel tempo l'integrità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

Il sistema consente le funzionalità di:

a) **Accettazione del pacchetto di versamento**;
b) **Conservazione del pacchetto di archiviazione**: il documento, ricevuto dal Conservatore in formato digitale statico non modificabile, viene conservato a norma di legge per tutta la durata prevista ed è contenuto in un pacchetto di archiviazione;
c) **Rettifica del pacchetto di archiviazione**: un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica è una modifica logica, nel pieno rispetto del principio di tracciabilità e si applica al pacchetto di archiviazione;
d) **Scarto/cancellazione del pacchetto di archiviazione**: un documento inviato in conservazione può essere cancellato. Il sistema di conservazione terrà comunque evidenza del documento all'interno dell'archivio a norma, nel rispetto del principio di tracciabilità; la cancellazione si applica al pacchetto di archiviazione, inoltre lo scarto è l'operazione concui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
e) **Esibizione del pacchetto di distribuzione:** il documento richiesto via web viene richiamato direttamente dal sistema di conservazione digitale ed esibito, con garanzia della sua opponibilità a terzi;
f) **Ricerca dei documenti informatici indicizzati**: il Produttore può eseguire una ricerca tra i documenti conservati trasversalmente sulle classi documentali;
g) Visualizzazione delle statistiche di conservazione.

Il sistema di conservazione del Conservatore integra il sistema di conservazione del Produttore e ne estende i servizi con funzionalità di stoccaggio digitale.
Le fasi di ***creazione, utilizzo e archiviazione dei documenti*** sono organizzate liberamente, in quanto il servizio di conservazione del Conservatore interviene solamente nella fase di conservazione e solamente per i documenti che il Produttore sceglie di conservare.

5.4.1.1 Indice del pacchetto di archiviazione e rapporto di versamento

Come già anticipato, l'Indice del Pacchetto di Archiviazione è un file in formato XML, marcato temporalmente e firmato digitalmente dal responsabile della conservazione, generato dal sistema di conservazione secondo la vigente normativa, che contiene le informazioni di conservazione del documento e viene con esso conservato.

In particolare nel file sono riportati:

- ***informazioni sull'applicazione che ha generato l'IPdA***
- ***il token del documento***
- ***l'operazione eseguita***
  - ✓ *conservazione,*
  - ✓ *rettifica,*
  - ✓ *scarto*
  - ✓ *cancellazione)*
- ***il bucket (area di conservazione) associato al Soggetto Produttore e la policy utilizzata***
- ***il nome dei file che compongono il documento, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte***
- ***eventuali informazioni relative al documento rettificante e rettificato***
- ***il tempo di creazione (timestamp) del file IPdA.***

L'insieme degli IPdA di un pacchetto formano il **rapporto di versamento** di cui all'art. 9, comma d) del DPCM del 3 dicembre 2013.
Il file IPdA è reso disponibile con il documento di riferimento ad ogni operazione di conservazione e richiesta di esibizione.
Per i dettagli sulle modalità di gestione delle fasi previste (memorizzazione, creazione del file IPDA e marcatura temporale dello stesso) **si rimanda al "Manuale del Sistema di conservazione" di InfoCert.**

5.4.1.2 Il processo di esibizione di un pacchetto di distribuzione

Le procedure di esibizione permettono di estrarre dal sistema di conservazione un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione, di rettifica o di cancellazione, utilizzando il relativo token.
Insieme ai file costituenti il pacchetto di distribuzione, sono rese disponibili anche le informazioni che qualificano il processo di conservazione, ossia il file IPdA.
Non è possibile esibire parti singole di documento.

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione.
In particolare ogni documento inserito nel sistema di conservazione è identificato in maniera univoca mediante una stringa denominata token.
Il token consente il reperimento di ciascun documento e la sua corretta esibizione, nonché la fruizione dei servizi di rettifica, di ricerca e di cancellazione logica.
Le procedure del sistema mantengono e aggiornano ad ogni nuovo invio il database di tutti i token; il database viene interrogato ad ogni richiesta di rettifica, scarto e cancellazione, ricerca ed esibizione confrontando il token inviato con quelli memorizzati.
La procedura assicura di agire solamente sul documento richiesto, e solamente se in possesso dei dovuti profili di autorizzazione.

5.4.1.3 Esibizione a norma

L'esibizione del pacchetto di distribuzione ottenuto tramite interrogazione al sistema di conservazione rappresenta un'esibizione completa, legalmente valida ai sensi del secondo comma dell'articolo 10 del DPCM 03/12/13 e dell'articolo 5 del DMEF 17/06/14.
Un apposito strumento di esibizione e verifica permette di richiamare agevolmente un documento conservato e consente di ottenere in modo automatico sia la verifica delle firme digitali e delle marche temporali apposte che le verifiche di integrità dei documenti conservati e di tutti gli altri elementi conservati.
Si rimanda al "Manuale del Sistema di conservazione" di InfoCert per il dettaglio delle funzionalità di verifica del sistema di conservazione.

5.4.2 Produzione copie e duplicati

Si rimanda al "Manuale del Sistema di conservazione" di InfoCert.

6 DESCRIZIONE DEL SISTEMA DI CONSERVAZIONE

Riferimento Cap. 8 "Manuale del Sistema di Conservazione" di InfoCert.

7 SICUREZZA DEL SISTEMA DI CONSERVAZIONE

Riferimento Cap. 10 "Manuale del Sistema di Conservazione" di InfoCert

8 MONITORAGGIO E CONTROLLI

Le funzionalità di controllo del buon funzionamento del sistema di conservazione adottate da InfoCert possono essere riassunte nei seguenti punti:

- ***Funzioni di monitoraggio complessivo sulle operazioni pianificate***
- ***Sistema di log ed errori***
- ***Invio di email***
- ***Sistema di tracciamento con revisioni***
- ***Controllo dei server***

8.1 Procedure di monitoraggio

InfoCert assicura la verifica periodica del funzionamento, nel tempo, del sistema di conservazione.
Il controllo della buona funzionalità del sistema di conservazione avviene tramite apposite funzionalità di monitoraggio del software. Esse mostrano l'esito delle operazioni automatiche eseguite sul sistema di conservazione come la generazione dei pacchetti di archiviazione, la chiusura dei pacchetti di archiviazione e la verifica dell'integrità degli archivi.
Unitamente all'esito delle predette operazioni vengono controllati anche i log delle operazioni medesime al fine di avere maggiore certezza di quanto effettivamente eseguito dal sistema di conservazione.
Il monitoraggio avviene inoltre anche a livello di processi di elaborazione sul sistema di conservazione. Questo permette di individuare eventuali casi di processi bloccati che potrebbero

inficiare il funzionamento del sistema stesso.
Un ultimo controllo del buon funzionamento del sistema avviene tramite il monitoraggio delle tracciature che vengono effettuate a livello di database. Tutte le operazioni eseguite determinano la creazione di apposite revisioni che registrano tutte le modifiche intervenute sul sistema permettendo eventualmente di ripristinare i dati a seguito di situazioni anomale.

8.2 Funzionalità per la verifica e il mantenimento dell'integrità degli archivi

InfoCert assicura la verifica periodica, **con cadenza non superiore all'anno**, dell'integrità degli archivi e della leggibilità degli stessi.
Assicura, inoltre, agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.
Il sistema di conservazione esegue periodicamente ed automaticamente le operazioni di controllo dell'integrità degli archivi. Tali operazioni vengono eseguite solo su una certa percentuale dell'archivio che viene definita nella configurazione del sistema di conservazione.

Il controllo eseguito è di due tipologie:

- Controllo di leggibilità: consiste nel verificare che i singoli bit degli oggetti siano tutti correttamente leggibili. Questo fornisce garanzia del buono stato del supporto di memorizzazione.
- Controllo di integrità: consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema. Questo fornisce una ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

La combinazione dei due tipi di controllo descritti non fornisce però garanzia di poter visualizzare correttamente il documento e che lo stesso sia effettivamente intellegibile dall'uomo.
Infatti questa garanzia non può essere fornita senza entrare nel merito del documento stesso.
La garanzia della corretta visualizzazione del documento è d'altro canto garantita dalla scelta del formato PDF/A per i documenti conservati. Questo formato possiede infatti la caratteristica intrinseca di fornire leggibilità a lungo termine oltre all'ulteriore garanzia di essere basato su specifiche pubbliche (ISO 19005-2005).

8.3 Pianificazione delle verifiche periodiche da effettuare

Il controllo periodico dell'integrità degli archivi avviene, da parte di InfoCert, con una frequenza di una volta al mese.

8.4 Mantenimento della firma per il periodo di conservazione

Il sistema di conservazione di InfoCert si avvale di un fornitore terzo (Certificatore accreditato) per le attività di firma digitale e di marcatura temporale. Questo fornitore garantisce che gli elaboratori che offrono il servizio di marcatura temporale e di firma digitale sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema garantiscegli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali.

9 NORMATIVE IN VIGORE NEI LUOGHI DOVE SONO CONSERVATI I DOCUMENTI

I documenti informatici sono conservati in Italia; pertanto al sistema di conservazione di InfoCert si rendono applicabili le norme Italiane.

10 TRATTAMENTO DEI DATI PERSONALI

10.1 Tutela e diritti degli interessati

In materia di trattamento dei dati personali InfoCert garantisce la tutela degli interessati in ottemperanza a quanto disposto del D.Lgs. 196/2003 così come rinovellato dal D.Lgs. 101/2018 per l'adeguamento al Regolamento UE 2016/679.
In particolare, agli interessati sono fornite le informative di cui all'art. 13 del richiamato Regolamento. Nella suddetta informativa il Produttore è informato sui diritti di accesso ai dati personali ed altri diritti (art. 15 e successivi del Regolamento UE 2016/679).

10.2 Modalità del trattamento

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Specifiche misure di sicurezza, come descritte nel "*Manuale del Sistema di Conservazione" di InfoCert* e nel *Contratto* LegalDoc sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

10.3 Finalità del trattamento

- **Erogazione del servizio di conservazione digitale dei documenti informatici:**
  I dati raccolti sono utilizzati per il perfezionamento del Contratto LegalDoc e per l'attivazione del Servizio di conservazione digitale dei documenti informatici. InfoCert utilizzerà i dati raccolti per lo svolgimento dell'attività connessa e/o derivante dal Servizio di conserva-zione digitale dei documenti informatici del Produttore.
- **Altre forme di utilizzo dei dati:**
  Per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e la difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati, i documenti informatici ed i dati forniti ad InfoCert potranno essere comunicati a soggetti pubblici, quali forze dell'ordine, Autorità pubbliche e autorità Giudiziaria per lo svolgimento delle attività di loro competenza.

10.4 Sicurezza dei dati

Come previsto dalle norme vigenti in materia, InfoCert adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo: i rischi di distruzione o perdita, anche accidentale, dei documenti informatici, di danneggiamento delle risorse hardware su cui i documenti informatici sono registrati ed i locali ove i medesimi vengono custoditi; l'accesso non autorizzato ai documenti stessi; i trattamenti non consentiti dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate da InfoCert assicurano:

1) *L'integrità dei documenti informatici, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;*
2) *La disponibilità dei dati e dei documenti informatici da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei documenti informatici, evitando la perdita o la riduzione dei dati anche accidentale utilizzando un sistema di backup;*
3) *La riservatezza dei documenti informatici da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni econtrollo degli accessi stessi.*

11 DISPOSIZIONI FINALI

Il presente manuale, come già precedentemente indicato, potrà essere modificato in qualsiasi momento ove ciò si rendesse necessario.
Le attività indicate nel presente documento si intendono integrate con quanto specificatamente indicato nel manuale di conservazione di InfoCert.

12 DOCUMENTI DI RIFERIMENTO E ALLEGATI

Allegato 1 – Normativa e Standard di Riferimento

Allegato 2 – Disciplinare Tecnico

Allegato 3 – Manuale della Conservazione di Infocert S.p.A.

Manuale di
Conservazione dei Documenti Informatici
di

Salerno Pulita S.p.A.

Allegato 1
Normativa e Standard di Riferimento

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione			
Verifica			
Approvazione			

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Ver 1.0		Prima emissione	

La presente versione dell'Allegato 1 al Manuale della Conservazione è suscettibile di ulteriori modifiche qualora il mutato quadro normativo o l'evoluzione tecnologica ne rendano necessaria la revisione

Indice

Introduzione

Il presente allegato riporta la principale normativa di riferimento per l'attività di conservazione a livello nazionale ed eventualmente quella a livello locale in vigore nei luoghi dove sono conservati i documenti.
Sono riportati inoltre gli standard a cui l'attività di conservazione si riferisce e che sono in qualche modo richiamati nel Manuale di Conservazione.
Tra essi anche gli standard indicati all'allegato 3 delle Regole Tecniche.
Viene periodicamente aggiornato in base agli eventuali aggiornamenti della normativa e degli standard di riferimento.

Normativa di riferimento

Normativa nazionale italiana

- **Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis** - Documentazione informatica;
- **Legge del 7 agosto 1990, n. 241 e s.m.i.** – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e s.m.i.** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo del 30 giugno 2003, n. 196 e s.m.i.** – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo del 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo del 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71
- **Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005
- **Circolare AGID del 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- **AGID** – Nuove linee guida del 9 settembre 2020 sulla Formazione, gestione e conservazione dei documenti informatici;
- **Risoluzione dell'Agenzia delle Entrate 25 settembre 2015, n.81/E**, *Interpello - ART. 11, legge 27 luglio 2000, n. 212 – Comunicazione del luogo di conservazione in modalità elettronica dei documenti rilevanti ai fini tributari, art. 5 D.M. 17 giugno 2014.*
- **Direttiva dell'Unione Europea (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016** relativa alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;*

- **Regolamento dell'Unione Europea (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016** relativo alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*.
- **Decreto Legislativo del 26 agosto 2016, n**. 179 e s.m.i. – Modifiche ed integrazioni al Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche;

Normativa regionale – Regione Campania

- **Legge Regionale n. 11 del 14 ottobre 2015** – Misure urgenti per semplificare, razionalizzare e rendere più efficiente l'apparato amministrativo, migliorare i servizi ai cittadini e favorire l'attività di impresa. Legge annuale di semplificazione 2015.

Istruzioni – linee guida – documentazione informativa

- Istruzioni dell'Agenzia per l'Italia Digitale – AgID marzo 2015, *Produzione e conservazione del registro giornaliero di protocollo.*
- Linee guida dell'Agenzia per l'Italia Digitale – AgID dicembre 2015, *Linee guida sulla conservazione dei documenti informatici.*
- Linee guida dell'Agenzia per l'Italia Digitale – AgID 26 aprile 2016, *Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni – Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015).*
- *Linee guida AgID (settembre 2020)* Formazione, gestione e conservazione dei documenti informatici;
- European Commission, working party on the protection of individuals with regard to the
- processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016.*
- European Commission, working party on the protection of individuals with regard to the
- processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on the right to data portability Adopted on 13 December 2016.*
- Linee guida del Garante per la protezione dei dati personali 2 marzo 2011, n. 088 del registro dei provvedimenti, *Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web.*
- Linee guida del Garante per la protezione dei dati personali, 4 aprile 2013, n. 161 del registro dei provvedimenti, *Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach).*
- Linee guida del Garante per la protezione dei dati personali, 15 maggio 2014 n. 243 del registro dei provvedimenti, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati.*
- Scheda informativa del Garante per la protezione dei dati personali, 17 marzo 2016, *Scheda informativa sulla figura del Responsabile della protezione dei dati personali (Data Protection Officer).*
- Guida informativa del Garante per la protezione dei dati personali, giugno 2016, *Prima guida informativa al Regolamento europeo 2016/679 in materia di protezione dei dati personali.*

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)** - Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management.
- **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;
- **ICA - ISAD (G):** General International Standard Archival Description - Second Edition - Adopted by the Committee on Descriptive Standards Stockholm, Sweden, 19-22 September 1999. Traduzione italiana a cura di Stefano Vitali, con la collaborazione di Maurizio Savoja, Firenze 2000. Standard dell'ICA (International Council on Archives – Conseil International des Archives) che fornisce delle norme generali per l'elaborazione di descrizioni archivistiche.
- **ISO 14721:2012** – Open Archival Information System – Reference model (CCSDS 650.0-M-2, Recommend Practice, Magenta Book June 2012): definisce concetti, modelli e funzionalità inerenti agli archivi digitali e ciò che è richiesto per garantire una conservazione permanente, o per un lungo termine indefinito, di informazioni digitali. Questa versione sostituisce la prima (ISO 14721:2003 - CCSDS 650.0-B-1 – Blue Book, January 2002) di cui è disponibile una traduzione in italiano (Sistema informativo aperto per l'archiviazione: traduzione italiana: *OAIS. Sistema informativo aperto per l'archiviazione,* a cura di Giovanni Michetti, Roma, ICCU 2007).
- **ISO 16363:2012** - Space data and information transfer systems - Audit and certification of trustworthy digital repositories (CCSDS 652.0-M-1 Recommend Practice, Magenta Book September 2011).
- **ISO 15836:** 2009**:** Information and documentation – The Dublin Core metadata element set. Sistema di metadati del Dublin Core (questa versione sostituisce la precedente: ISO 15836:2003).
- **ISO 23081-1:2006**: Information and documentation – Records management processes – Metadata for records – Part 1- Principles. Quadro di riferimento per lo sviluppo di un Sistema di metadati per la gestione documentale.
- **ISO/TS 23081-2:2007**: Information and documentation – Records management processes – Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione.
- **ISO 23081-2:2009**: Information and documentation – Managing Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione.
- **LTO4:** standard "open" sviluppato alla fine del 1990. LTO 4 è una tecnologia di storage dei dati su nastro.
- **SAML:** Security Assertion Markup Language è uno standard informatico per lo scambio di dati di autenticazione e autorizzazione (dette asserzioni) tra domini di sicurezza distinti, tipicamente un identity provider (entità che fornisce informazioni di identità) e un service provider (entità che fornisce servizi). Il formato delle asserzioni SAML è basato su XML. SAML è mantenuto da OASIS Security Services Technical Committee.
- **SQL:** (Structured Query Language) è un linguaggio standardizzato per database basati sul modello relazionale (RDBMS).
- **UNI 11386:2010** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI SInCRO): Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali: definisce la struttura dell'insieme di dati a supporto del processo di conservazione; in particolare, precisa e integra alcune disposizioni contenute nella Deliberazione CNIPA 19 febbraio 2004, n. 11, individuando gli elementi informativi necessari alla creazione dell'indice di conservazione e descrivendone sia la

semantica sia l'articolazione per mezzo del linguaggio formale XML. L'obiettivo della norma è di consentire agli operatori del settore di utilizzare una struttura-dati condivisa al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, grazie all'adozione dello Schema XML appositamente elaborato.

- **UNI ISO 15489-1:2006:** Informazione e documentazione – Gestione dei documenti di archivio – Principi generali sul record management.
- **UNI ISO 15489-2:2007:** Informazione e documentazione – Gestione dei documenti di archivio – Linee guida sul record management.

Manuale di Conservazione dei Documenti Informatici di

Salerno Pulita S.p.A.

Allegato 2 Disciplinare Tecnico

EMISSIONE DEL DOCUMENTO

– Azione	– Data	– Nominativo	– Funzione
– Redazione	–	–	–
– Verifica	–	–	–
– Approvazione	–	–	–

REGISTRO DELLE VERSIONI

– N°Ver/Rev/Bozza	– Data emissione	– Modifiche apportate	– Osservazioni
– Ver 1.0	–	– Prima emissione	–

La presente versione dell'Allegato 2 al Manuale della Conservazione è suscettibile di ulteriori modifiche qualora il mutato quadro normativo o l'evoluzione tecnologica ne rendano necessaria la revisione.

.Indice

1. Introduzione

Il presente allegato riporta:

- L'elenco generale e la descrizione dei formati elettronici, delle classi documentali e le relative politiche di conservazione dei documenti gestiti dal Sistema di Conservazione di InfoCert;
- La tipologia dei pacchetti informativi (Versamento, Archiviazione, Distribuzione) gestiti dal Sistema di Conservazione di InfoCert;
- L'elenco delle *classi documentali* e definizione dei metadati gestiti dal **Sistema di Conservazione di InfoCert.**

Viene periodicamente aggiornato in base alla eventuale ridefinizione delle tipologie documentali che il Produttore intende portare in conservazione nel **Sistema di Conservazione di InfoCert.**

2. Formati Gestiti

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.
Il formato di un documento informatico è la convenzione usata per rappresentare il contenuto informativo mediante una sequenza di byte.
Nel seguito vengono fornite le indicazioni sui formati dei documenti informatici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con la conservazione digitale a lungo termine.
Infatti, una possibile soluzione al problema dell'obsolescenza, che porta all'impossibilità di interpretare correttamente formati non più supportati al fine di renderli visualizzabili, è quella di selezionare formati standard.
E' comunque opportuno premettere che per la natura stessa dell'argomento di cui trattasi, questa parte del Manuale, conformemente a quanto accadrà per il Manuale della Conservazione del Conservatore, potrà subire periodici aggiornamenti sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati.

2.1 Caratteristiche generali dei formati

	Caratteristica	***Descrizione della Caratteristica***
1	**APERTURA**	Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse. In relazione a questo aspetto, sono da privilegiarsi formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS.
2	**SICUREZZA**	La sicurezza di un formato dipende da due elementi: ▪ il grado di modificabilità del contenuto del file; ▪ la capacità di essere immune dall'inserimento di codice maligno.
3	**PORTABILITÀ**	Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto si ottiene mediante l'impiego fedele di standard documentati e accessibili e dalla loro diffusione sul mercato.
4	**FUNZIONALITÀ**	Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti in-ormatici, che prevedono una varietà di funzioni messe a disposizione del Produttore per la formazione e gestione del documento informatico.
5	**SUPPORTO ALLO SVILUPPO**	Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
6	**DIFFUSIONE**	La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

2.2 Formati per la Conservazione

Oltre al soddisfacimento delle caratteristiche precedentemente elencate, la scelta dei formati idonei alla conservazione si è orientata verso formati capaci di far assumere al documento le fondamentali caratteristiche di immodificabilità e staticità.
Pertanto, alla luce delle suddette considerazioni, **i formati adottati** per la conservazione delle diverse tipologie di documenti informatici, in accordo con quanto previsto dal Conservatore, sono i seguenti:

Formato PDF/A	**Descrizione**	
	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. Questo formato è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.	
Caratteristiche e dati informativi		
	Informazioni gestibili	testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.
	Sviluppato da	Adobe Systems - http://www.adobe.com/
	Estensione	.pdf
	Tipo MIME	Application/pdf
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 19005-1:2005 (vesr. PDF 1.4)
	Altre caratteristiche	assenza di collegamenti esterni assenza di codici eseguibili assenza di contenuti crittografati il file risulta indipendente da codici e collegamenti esterni che ne pos-sono alterare l'integrità e l'uniformità nel lungo periodo Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A Sono disponibili prodotti per la verifica della conformità di un docu-mento PDF al formato PDF/A.
	Software necessario alla visualizzazione	Adobe Reader

Formato XML	**Descrizione**	
	Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio: SVG usato nella descrizione di immagini vettoriali, XBRL usato nella comunicazione di dati finanziari, ebXML usato nel commercio elettronico, SOAP utilizzato nello scambio dei messaggi tra Web Service	
Caratteristiche e dati informativi		
	Informazioni gestibili	Contenuto di evidenze informatiche, dei pacchetti di versamento, ar-chiviazione e distribuzione, ecc.
	Sviluppato da	W3C - http://www.w3.org/
	Estensione	.xml
	Tipo MIME	Application/xml Text/xml
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da W3C – http://www.w3.org/XML/
	Altre caratteristiche	è un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	Qualsiasi editor di testo. Inoltre è possibile, concordando con il Cliente le caratteristiche di un

		opportuno file xslt, produrne una copia human readable con Microsoft Internet Explorer / Firefox / Google Chrome o altri browser

Formato	**Descrizione**	
EML	Electronic Mail Message (EML) è un formato di testo che definisce la sintassi di messaggi di posta elettronica scambiati tra utenti -	
Caratteristiche e dati informativi		
	Informazioni gestibili	Messaggi di posta elettronica e PEC
	Sviluppato da	Internet Engineering Task Force (IETF) - http://www.ietf.org/
	Estensione	.eml
	Tipo MIME	Message/rfc2822
	Formato aperto	SI
	Specifiche tecniche	
	Altre caratteristiche	è un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	La maggior parte dei client di posta elettronica supportano la visualizzazione di file eml

3. La tipologia dei pacchetti informativi gestiti

3.1 Specifiche del Pacchetto di Versamento

Riferimento paragrafo 6.2 "Manuale del Sistema di Conservazione" di InfoCert.

3.2 Specifiche del Rapporto di Versamento

Riferimento paragrafo 7.3 "Manuale del Sistema di Conservazione" di InfoCert.

4. Tipologie dei documenti posti in conservazione

L'**Ente** intende portare in conservazione i seguenti tipi di documenti:

- Registro di protocollo informatico,
- Documento Protocollato.

A regime tutti i documenti informatici trattati dall'Ente dovranno essere posti in conservazione. Il presente documento sarà assoggettato ad aggiornamento sia per integrare le modifiche che si renderanno necessarie a seguito di modifiche alla normativa vigente sia per aggiungere altre tipologie di documenti, che per la loro natura procedimentale, non possono essere integrati con le procedure informatiche al momento adeguate per la conservazione a norma.

Nel seguito sono riportate le informazioni di dettaglio per le tipologie documentali sia già poste in conservazione sia da porre in conservazione nel breve termine.

4.1 Conservazione del Registro Giornaliero di Protocollo

Tipologia di documento	Registro Giornaliero del protocollo informatico
Natura del documento	Documento digitale in forma statica (formato PDF/A) e un file XML con i metadati per lo scambio e la lettura tra sistemi automatizzati
Modalità di invio	Caricamento automatico nel sistema di conservazione tramite specifico connettore dal Protocollo Informatico fornito da Datagraf Servizi S.r.l. E' disponibile anche la modalità manuale di generazione del Pacchetto di Versamento e il relativo caricamento manuale tramite interfaccia web. La prima modalità è certamente più immediata e semplice (un singolo click) mentre la seconda potrebbe richiedere qualche secondo in più ed un minimo di competenze informatiche, in particolare per la gestione del file e il suo upload sul portale web. In adesione alle linee guida per la conservazione del registro giornaliero di protocollo pubblicate da AgId il 6 ottobre 2015 ed aggiornate successivamente in data 13 ottobre 2015, il Pacchetto di Versamento generato automaticamente e trasferito in forma statica in conservazione non viene firmato digitalmente. Viceversa l'uso della firma digitale si rende obbligatorio quando la generazione e l'invio non sono automatizzati
Data di decorrenza del processo di conservazione	12 ottobre 2015
Descrizione del flusso	Il documento viene estratto in formato PDF con la periodicità prevista dalla normative (giornaliera) e inviato in conservazione dai Servizi competenti sui relativi procedimenti. L'unico registro da porre in conservazione è quello del protocollo informatico. Con ordine di servizio saranno individuati gli operatori preposti all'operazione

4.2 Conservazione dei Documenti Protocollati

Tipologia di documento	D***ocumento Protocollato***
Natura del documento	Documento digitale in forma statica (formato PDF/A) e un file XML con i metadati per lo scambio e la lettura tra sistemi automatizzati
Modalità di invio	Caricamento automatico nel sistema di conservazione tramite specifico connettore dal Protocollo Informatico fornito da Datagraf Servizi S.r.l. E' disponibile anche la modalità manuale di generazione del Pacchetto di Versamento e il relativo caricamento manuale tramite interfaccia web. La prima

	modalità è certamente più immediata e semplice (un singolo click) mentre la seconda potrebbe richiedere qualche secondo in più ed un minimo di competenze informatiche, in particolare per la gestione del file e il suo upload sul portale web. Il pacchetto di Versamento generato automaticamente e trasferito in forma statica in conservazione non viene firmato digitalmente. Viceversa l'uso della firma digitale si rende obbligatorio quando la generazione e l'invio non sono automatizzati
Data di decorrenza del processo di conservazione	8 aprile 2021
Descrizione del flusso	Il documento viene estratto in formato PDF con la periodicità prevista dalla normative (giornaliera) e inviato in conservazione dai Servizi competenti sui relativi procedimenti. Con ordine di servizio saranno individuati gli operatori preposti all'operazione

5. Metadati da associare alle diverse tipologie di documenti

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento informatico, escluse quelle che costituiscono il contenuto del documento stesso.
I metadati riguardano principalmente, ma non esclusivamente, i modi, i tempi ed i soggetti coinvolti nel processo della formazione del documento informatico, della sua gestione e della sua conservazione.
Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento.
I metadati che seguono devono essere associati al documento dal Produttore prima del versamento in conservazione.
I metadati, seppur chiaramente associati al documento informatico, possono essere gestiti indipendentemente dallo stesso. In relazione ai diversi tipi di documenti informatici posti in conservazione, è previsto un "**set minimo"** di metadati come specificato nel capoverso seguente.

5.1 Metadati Minimi da associare a qualsiasi documento informatico

I metadati che seguono, devono, essere associati ad ogni documento informatico, a prescindere dalla specializzazione che questo assume (amministrativo, fiscale, ecc.).
Al documento informatico immodificabile, il Produttore dovrà associare i metadati che sono stati generati durante la sua formazione.

L'insieme minimo dei metadati è costituito da:

1. l'identificativo univoco e persistente;
2. il riferimento temporale (data di chiusura);
3. l'oggetto;
4. il soggetto che ha formato il documento
    a. nome
    b. cognome
    c. Codice Fiscale
5. l'eventuale destinatario
    a. nome
    b. cognome
    c. Codice Fiscale (unico dato obbligatorio del destinatario) .

5.2 Metadati Minimi del documento informatico amministrativo

Le pubbliche amministrazioni, ai sensi dell'articolo 40, comma 1, del CAD, formano gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici riportati nel *Manuale* di gestione.
Detto documento amministrativo informatico, di cui all'art 23-ter del CAD, formato mediante una delle modalità di cui all'articolo 3, comma 1, del CAD, è identificato e trattato nel sistema di gestione informatica dei documenti del Produttore.
Pertanto, al documento amministrativo informatico, il Produttore deve associare, oltre ai metadati di cui al punto precedente, anche l'insieme minimo dei metadati di cui all'articolo 53 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.. :

1. ***numero di protocollo del documento;***
2. ***data di registrazione di protocollo;***
3. ***mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti;***
4. ***oggetto del documento;***
5. ***data e protocollo del documento ricevuto, se disponibile;***
6. ***l'impronta del documento informatico.***

5.3 Metadati Minimi del documento informatico avente rilevanza tributaria

Anche sulla scorta di quanto disposto dall'art. 3, del decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004, devono essere consentite le funzioni di ricerca e di estrazione delle informazioni dagli archivi contenenti documenti informatici rilevanti ai fini delle disposizioni tributarie in relazione ai metadati di seguito riportati:

1. ***cognome;***
2. ***nome;***
3. ***denominazione;***
4. ***codice fiscale;***
5. ***partita Iva;***
6. ***data documento;***
7. ***periodo d'imposta di riferimento;***
8. ***tipo documento (si veda in merito il Par. 15.1 del " Manuale del Sistema di Conservazione" - Appendice 1 "Documenti rilevanti ai fini delle disposizioni tributarie: Elenco tipi documento".***

5.4 Metadati Minimi Registro Giornaliero di Protocollo

Si rimanda in merito a quanto previsto dalle linee guida AgID.

5.5 Metadati Minimi Documento Protocollato

Si rimanda in merito a quanto previsto dalla normativa vigente.

Manuale della Conservazione

di InfoCert S.p.A.

Firmato digitalmente da: Danilo Cattaneo

REGISTRO DELLE VERSIONI

N° versione	Data emissione	Modifiche apportate
01	Luglio 2014	Prima versione
02	Novembre 2015	Utilizzo dello schema proposto da AgID
03	Febbraio 2016	Correzioni formali e di layout
04	Marzo 2016	Correzioni formali e di layout
05	Settembre 2017	Glossario, Normativa, Mission, Comunità di riferimento, Riferimenti a policy aziendali interne
05.1	Novembre 2017	Specificità del contratto
06	Luglio 2018	Normativa GDPR, semplificazione glossario e nuovi Responsabili
07	Gennaio 2019	Nuovo logo aziendale
08	Maggio 2019	Nuovo Responsabile sistemi
09	Ottobre 2020	Glossario, nuovi Responsabili, aggiornamento procedure di monitoraggio, semplificazione delle Specificità del contratto
10	Novembre 2020	Ampliamento servizi di storage

INDICE DEL DOCUMENTO

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale della Conservazione di InfoCert S.p.A. (Società soggetta a direzione e controllo di TecnoInvestimenti S.p.A.), ai sensi del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005 pubblicato in GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20.
Il Manuale della Conservazione illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.
In caso di ispezione da parte delle autorità di vigilanza preposte, il Manuale della Conservazione permette un agevole svolgimento di tutte le attività di controllo.

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

TERMINE	DEFINIZIONE
ACCESSO	Operazione che consente di prendere visione dei documenti informatici.
AFFIDABILITÀ	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
AGGREGAZIONE DOCUMENTALE INFORMATICA	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
ARCHIVIO	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
AREA ORGANIZZATIVA OMOGENEA	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
ATTESTAZIONE DI CONFORMITÀ DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITÀ	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
CERTIFICAZIONE	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
CLASSIFICAZIONE	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
CLOUD DELLA PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
CODEC	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un *wrapper* (codifica), così come di estrarli da esso (decodifica).
CONSERVATORE	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
CONSERVAZIONE	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti

CONVENZIONI DI DENOMINAZIONE DEL FILE	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
COORDINATORE DELLA GESTIONE DOCUMENTALE	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
DESTINATARIO	Soggetto o sistema al quale il documento informatico è indirizzato.
DIGEST	Vedi Impronta crittografica.
DOCUMENTO AMMINISTRATIVO INFORMATICO	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
DOCUMENTO ELETTRONICO	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
DOCUMENTO INFORMATICO	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
DUPLICATO INFORMATICO	Vedi art. 1, comma 1, lett) i quinquies del CAD.
ESEAL	Vedi sigillo elettronico.
ESIBIZIONE	operazione che consente di visualizzare un documento conservato
ESIGNATURE	Vedi firma elettronica.
ESTRATTO DI DOCUMENTO INFORMATICO	Parte del documento tratto dal documento originale
ESTRATTO PER RIASSUNTO DI DOCUMENTO INFORMATICO	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
ESTRAZIONE STATICA DEI DATI	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc…), attraverso metodi automatici o semi-automatici
EVIDENZA INFORMATICA	Sequenza finita di *bit* che può essere elaborata da una procedura informatica.
FASCICOLO INFORMATICO	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
FILE	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
FILE CONTAINER	Vedi Formato contenitore.
FILE WRAPPER	Vedi Formato contenitore.
FILE-MANIFESTO	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
FILESYSTEM	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
FIRMA ELETTRONICA	Vedi articolo 3 del Regolamento eIDAS.
FIRMA ELETTRONICA AVANZATA	Vedi articoli 3 e 26 del Regolamento eIDAS.
FIRMA ELETTRONICA QUALIFICATA	Vedi articolo 3 del Regolamento eIDAS.
FLUSSO (BINARIO)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.

FORMATO CONTENITORE	Formato di file progettato per consentire l'inclusione ("imbustamento" o *wrapping*), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
FORMATO DEL DOCUMENTO INFORMATICO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
FORMATO "DEPRECATO"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
FUNZIONI AGGIUNTIVE DEL PROTOCOLLO INFORMATICO	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
FUNZIONI MINIME DEL PROTOCOLLO INFORMATICO	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
FUNZIONE DI *HASH* CRITTOGRAFICA	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
GESTIONE DOCUMENTALE	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
HASH	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
IDENTIFICATIVO UNIVOCO	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
IMPRONTA CRITTOGRAFICA	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.
INTEGRITÀ	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
INTEROPERABILITÀ	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
LEGGIBILITÀ	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
MANUALE DI CONSERVAZIONE	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
MANUALE DI GESTIONE	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

METADATI	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
NAMING CONVENTION	Vedi Convenzioni di denominazione
OGGETTO DI CONSERVAZIONE	Oggetto digitale versato in un sistema di conservazione.
OGGETTO DIGITALE	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
PACCHETTO DI ARCHIVIAZIONE	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
PACCHETTO DI DISTRIBUZIONE	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
PACCHETTO DI FILE (*FILE PACKAGE*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
PACCHETTO DI VERSAMENTO	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
PACCHETTO INFORMATIVO	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
PATH	Percorso (*vedi*).
PATHNAME	Concatenazione ordinata del percorso di un file e del suo nome.
PERCORSO	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
PIANO DELLA SICUREZZA DEL SISTEMA DI CONSERVAZIONE	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
PIANO DELLA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
PIANO DI CLASSIFICAZIONE (TITOLARIO)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
PIANO DI CONSERVAZIONE	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
PIANO DI ORGANIZZAZIONE DELLE AGGREGAZIONI DOCUMENTALI	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si

	declinano le funzioni svolte dall'ente
PIANO GENERALE DELLA SICUREZZA	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
PRESA IN CARICO	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
PROCESSO	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
PRODUTTORE DEI PDV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
QSEAL	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
QSIGNATURE	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
RAPPORTO DI VERSAMENTO	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
REGISTRO DI PROTOCOLLO	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
REGISTRO PARTICOLARE	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
REGOLAMENTO EIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
REPERTORIO	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
RESPONSABILE DEI SISTEMI INFORMATIVI PER LA CONSERVAZIONE	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLA CONSERVAZIONE	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID

RESPONSABILE DELLA GESTIONE DOCUMENTALE	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.
RESPONSABILE DELLA PROTEZIONE DEI DATI	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
RESPONSABILE DELLA SICUREZZA DEI SISTEMI DI CONSERVAZIONE	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLO SVILUPPO E DELLA MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RIFERIMENTO TEMPORALE	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
RIVERSAMENTO	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
SCARTO	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
SERIE	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
***SIDECAR* (FILE)**	File-manifesto (*vedi*).
SIGILLO ELETTRONICO	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
SISTEMA DI CONSERVAZIONE	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
TIMELINE	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
TITOLARE DELL'OGGETTO DI CONSERVAZIONE	Soggetto produttore degli oggetti di conservazione.
TRASFERIMENTO	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.

UFFICIO	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
UTENTE ABILITATO	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Di seguito l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti:

- 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 ss.mm.ii. – 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 ss.mm.ii – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) – Codice dell'amministrazione digitale (CAD);
- 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, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- 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;

- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- 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.
- eIDAS (electronic IDentification Authentication and Signature) EU Regulation 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market.
- GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici del settembre 2020.

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle citate Regole

Tecniche ai sensi del Codice:

- UNI EN ISO 9001:2015 Sistemi di gestione per la Qualità;
- ISO 14001:2015 Sistema di Gestione Ambientale;
- Norma ETSI 319 401 - Reg. UE 910/2014 – eIDAS (electronic IDentification Authentication and Signature);
- ISO 15489:2014 (cap. 5 Regulatory Environment; cap. 7 Records Management Requirements);
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud service;
- ISO/IEC 27018:2019 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- 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;
- ISO/IEC 20000-1: 2018 Service Management System Requirements
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element

set, Sistema di metadata del Dublin Core.

- UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

Torna al sommario

3.3 Procedure aziendali interne

Si riportano di seguito i riferimenti alle procedure aziendali interne e alle principali politiche aziendali applicate anche al sistema di conservazione:

- PR/225- Change Management InfoCert
- MG231 – Modello di Gestione e Organizzazione D.Lgs 231/01
- PR/235 Progettare e sviluppare un servizio informatico InfoCert
- MG294 Capacity Management
- MG/325 Gestire Verifiche Ispettive InfoCert
- MG445 – Gestione Documentale InfoCert
- PR456 Problem Management
- Procedura Service Management System – SMS
- Processo MG115/TB02_Processi e Responsabilità_Integrated Management System
- Procedura di hand-over tra conservatori e scarto archivistico in LegalDoc.

Torna al sommario

4. RUOLI E RESPONSABILITÀ

Si riportano di seguito i profili professionali di Responsabilità legate al servizio di conservazione e le rispettive attività di competenza.
Tutti i Responsabili sono assunti a tempo indeterminato.

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
Responsabile del servizio di Conservazione	Nicola Maccà	• Definizione e 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. • Definizione delle condizioni generali del contratto di servizio in coordinamento con la funzione legale e la funzione commerciale e funzione	da luglio 2018

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		marketing di InfoCert.	
Responsabile Sicurezza dei sistemi per la conservazione	Giovanni Belluzzo	• 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.	da luglio 2018
Responsabile funzione archivistica di conservazione	Marta Gaia Castellan	• Definizione e descrizione archivistica dei documenti e delle aggregazioni documentali per la fruizione del patrimonio documentario e informativo conservato. • Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici. • Analisi archivistica per lo sviluppo di 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. • Definizione delle condizioni	da settembre 2015

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		generali del contratto di servizio in coordinamento con la funzione legale e la funzione commerciale e funzione marketing di InfoCert. • Controlli periodici a campione sulla leggibilità dei documenti conservati.	
Responsabile trattamento dati personali	Ilenia Gentilezza	• 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.	da marzo 2020
Responsabile sistemi informativi per la conservazione	Francesco Griselda	• Presidio ed evoluzione dei sistemi informativi per la conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000. • Gestione dell'esercizio delle componenti hardware e software di base del sistema di conservazione. • Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore in collaborazione con Il Responsabile della	da ottobre 2020

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		manutenzione del sistema di conservazione. • 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. • Coordinamento dello sviluppo e manutenzione delle componenti hardware e software di base del sistema di conservazione.	
Responsabile sviluppo e manutenzione del sistema di conservazione	Lucia Bortoletto	• Sviluppo e manutenzione del sistema di conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000. • Coordinamento dello sviluppo e manutenzione delle componenti software del sistema di conservazione. • Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione.	da luglio 2018

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		• 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 in collaborazione con il Responsabile funzione archivistica di conservazione. • Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	

Di seguito sono storicizzate le figure professionali che hanno ricoperto ruoli di responsabilità precedentemente:

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile sistemi informativi per la conservazione	Stefano Mameli	da maggio 2019 a ottobre 2020
Responsabile trattamento dati personali	Valentina Zoppo	da luglio 2018 a marzo 2020

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile sistemi informativi per la conservazione	Nicolò Poniz	da luglio 2018 a maggio 2019
Responsabile sviluppo e manutenzione del sistema di conservazione	Nicola Maccà	da gennaio 2013 a luglio 2018
Responsabile sistemi informativi per la conservazione	Massimo Biagi	da marzo 2014 a luglio 2018
Responsabile funzione archivistica di conservazione precedente	Silvia Loffi	da dicembre 2014 ad agosto 2015
Responsabile trattamento dati personali	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile Sicurezza dei sistemi per la conservazione	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile del servizio di Conservazione	Antonio Dal Borgo	da luglio 2008 a luglio 2018
Responsabile del servizio di Conservazione	Pio Barban	da luglio 2007 a luglio 2008

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Profilo di InfoCert

Denominazione sociale	InfoCert S.p.A.
Sede Legale:	Piazza Sallustio, 9, 00187 Roma Tel.+39 06 836691
Sedi Operative:	• Piazza da Porto, 3, 35131 Padova • Via Via Carlo Bo, 11, 20143 Milano • Via Marco e Marcelliano, 45, 00147 Roma Tel: +39 06836691
Sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
Codice Fiscale / Partita IVA	07945211006
Numero REA	RM – 1064345

InfoCert si pone sul mercato europeo come Trust Service Provider altamente specializzato, leader del mercato italiano nei servizi di digitalizzazione e dematerializzazione, nonché una delle principali Certification Authority a livello europeo, fornendo servizi di Posta Elettronica Certificata, Firma Avanzata e Digitale, Conservazione Digitale dei documenti e gestore accreditato AgID dell'identità digitale di cittadini e imprese, in conformità ai requisiti regolamentari e tecnici dello SPID (Sistema Pubblico per la gestione dell'Identità Digitale).

Da sempre la mission aziendale è credere nel futuro e nella trasformazione digitale, per questo dedichiamo la nostra esperienza, la nostra capacità di innovazione e la nostra passione per l'eccellenza, a tutti coloro che, in Italia e nel mondo, ricercano sicurezza e affidabilità nelle soluzioni digitali. Investiamo in ricerca e sviluppo per dare vita a nuove idee che supportino i nostri clienti nella costruzione di modelli e processi di business innovativi e conformi alle

normative, guidandoli verso una efficace trasformazione digitale e un futuro maggiormente sostenibile per le aziende, le persone e la realtà sociale.

La mission aziendale si declina anche nel servizio di Conservazione digitale: innovazione, sicurezza, affidabilità e conformità normativa, con lo scopo di assicurare la corretta gestione, archiviazione e conservazione dei documenti informatici di diversi soggetti produttori, assicurando l'esibizione a norma dei documenti conservati e la consulenza specialistica su progetti di paperless design.

InfoCert dal 2014 è tra le prime aziende italiane accreditate dall'Agenzia per l'Italia Digitale (AgID) come Conservatore, requisito normativo necessario per erogare servizi di Conservazione digitale per la Pubblica Amministrazione.

Inoltre, dal 2019, InfoCert ha ottenuto la qualifica AgID Cloud Marketplace (CSP Tipo B Infrastruttura e SaaS per LegalDoc).

La comunità di riferimento del servizio di Conservazione digitale di InfoCert è un gruppo identificato di clienti e di potenziali utenti in grado di comprendere un determinato set di informazioni: si tratta di un'unica comunità, ben definita, ma con alcune differenziazioni interne (multiple user communities), a seconda del mercato di riferimento (Pubblica Amministrazione centrale e locale, Sanità, Industry, Banking, Pharma, Utilities, Insurance, Ordini e Associazioni, PMI, liberi professionisti).

Il fine ultimo del servizio di Conservazione digitale è rendere i Pacchetti di Distribuzione ricercabili, esibibili, leggibili, integri, affidabili, autentici e fruibili dagli utenti della comunità di riferimento, attraverso la mediazione del soggetto produttore, in ottemperanza ai principali standard internazionali di records management (OAIS ISO14721 e ISO15489).

InfoCert è costantemente impegnata nel monitoraggio della propria comunità designata, al fine di acquisire nuove informazioni o esigenze o standard tecnologici, anche con lo scopo di combattere l'obsolescenza tecnologica. Per maggiori dettagli si rimanda al Service Management System.

InfoCert, inoltre, nello svolgimento delle proprie attività, ha conseguito le seguenti certificazioni:

- ISO 14001:2015 (Sistema di Gestione Ambientale)
- ISO/IEC 20000-1:2011 (Gestione dei Servizi Informatici)
- UNI EN ISO 9001:2015 (Sistemi di gestione per la qualità);
- ISO/IEC ISO 27001:2013 (Sistemi di gestione della sicurezza delle informazioni).
- ISO/IEC ISO 27017 e ISO/IEC ISO 27018 relativamente al Servizio di conservazione digitale a norma di documenti informatici erogato in modalità Cloud (SaaS) e relativi servizi di infrastruttura (IaaS privato).

InfoCert ha adottato il modello di organizzazione e controllo [MG231/01] di cui al D.lgs. del 08 giugno 2001 n.231 allo scopo di prevenire i reati per i quali la legge in questione prescrive la responsabilità amministrativa dell'impresa.

Il modello adottato da InfoCert rappresenta un'ulteriore garanzia dell'azienda in termini rigore, trasparenza e senso di responsabilità nella gestione dei processi interni e nei rapporti con il mondo esterno.

Il modello prevede l'istituzione di un Organismo di Vigilanza, la gestione di un processo formativo/informativo, la adozione di un Codice Etico e la definizione di un Sistema Sanzionatorio.

InfoCert si è dotata, inoltre, di un Integrated Management System per la gestione dei processi e delle responsabilità aziendali. Il documento MG115/TB02 descrive la mappatura dei processi aziendali in termini di ambiti di processo, procedure, ownership, modelli di gestione, pianificazioni, erogazioni, approvvigionamenti, controlli, governance e sicurezza.

Torna al sommario

5.2 Organigramma

L'organigramma di InfoCert è stato depositato presso AgID durante le procedure di accreditamento. Di seguito sono riportate le figure di responsabilità che intervengono nei processi e nelle attività di Conservazione.

Torna al sommario

5.3 Strutture organizzative

Nel processo di conservazione digitale intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità, sintetizzate nella tabella seguente e dettagliate per singola attività.

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
1. Condizioni Generali di Contratto	R						
2. Richiesta di attivazione	R	V	V	V	V	V-E	
3. Atto di affidamento	R						
4. Specifiche Tecniche di integrazione	V			A	A	R-E	
5. Impegno alla riservatezza	V		R	A			
6. Acquisizione del documento da conservare	R				E	V	
7. Metadatazione ed archiviazione	A	R			E	V	
8. Eventuale attestazione della conformità di quanto memorizzato nel documento d'origine da parte di un PU	R						

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
9. Creazione del pacchetto di versamento							R
10. Invio al sistema di conservazione del pacchetto di versamento							R
11. Validazione Del pacchetto di versamento	R				E	V	
12. Generazione del pacchetto di archiviazione	R				E	V	
13. Memorizzazione e creazione “copia di sicurezza”	R			V	E	V	
14. Invio dell'IPdA al soggetto Produttore	R					E	
15. Scarto dei pacchetti di archiviazione	R	V			A	E	
16. Chiusura del servizio di conservazione al termine di un contratto	R	V			A	E	
17. Conduzione e manutenzione del	A				R	E	

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
sistema di conservazione							
18. Monitoraggio del sistema di conservazione	**A**	**V**			**R**	**E**	
19. Change management		**V**		**V**	**A**	**R**	
20. Verifica periodica di conformità a normativa e standard di riferimento	**A**	**R**	**V**	**V**	**A**		

[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]

I Soggetti Produttori affidano in outsourcing il servizio di conservazione a InfoCert S.p.A., che assume le responsabilità della conservazione in accordo con quanto previsto dai documenti contrattuali descritti al capitolo 10 'Specificità del Contratto' e dagli articoli 5 e 6 del DPCM del 3 dicembre 2013.

Tutte le verifiche in carico al Responsabile del servizio della Conservazione sono garantite anche dal servizio di auditing interno. Il processo di conservazione è normalmente effettuato da procedure totalmente automatizzate, che non necessitano dell'intervento di altri soggetti o delegati. InfoCert si riserva, come specificato nelle Condizioni generali del Contratto, la possibilità di avvalersi di partner tecnologici per l'esecuzione di operazioni, singole attività, servizi relativi a funzioni o fasi del processo di conservazione, a terzi soggetti, fornitori esterni, che per conoscenza, esperienza, capacità e affidabilità forniscano idonee garanzie.

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

In generale si definisce 'pacchetto' un contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.

I pacchetti (versamento/archiviazione/distribuzione) sono contrattualizzati con il Soggetto Produttore e si basano sui documenti che fanno parte delle 'Specificità del Contratto'.

Per "pacchetto di versamento" si intende l'insieme di documenti che il Soggetto Produttore invia al sistema di conservazione in un'unica sessione (login/logout).

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione. Ad ogni documento il Sistema di conservazione associa un file XML, detto Indice del Pacchetto di Archiviazione (Indice di Conservazione UNI SInCRO). L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

Per "pacchetto di distribuzione" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta, ovvero è la risposta alla ricerca effettuata dal Soggetto Produttore tramite interfaccia disponibile, che porta all'esibizione del documento conservato. Il documento da esibire è accompagnato sempre dall'IPdA.

Nel sistema, ad oggi, il "pacchetto di distribuzione" coincide con il "pacchetto di archiviazione".

Eventuali specificità sono concordate con il Soggetto Produttore e descritte nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione e AL/NDOC – Allegato Tecnico al Contratto LegalDoc.

Torna al sommario

6.1 Oggetti conservati

Tipologie documentali, metadati e formati sono sempre concordati con il Soggetto Produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Dati Tecnici di attivazione'.

I visualizzatori dei formati standard, previsti nell'allegato 2 del DPCM 3 dicembre 2013, sono automaticamente assegnati all'atto dell'attivazione del proprio ambiente di conservazione e sono forniti da InfoCert al Soggetto Produttore all'atto di attivazione del servizio. Tutti i documenti inviati in conservazione saranno associati al visualizzatore configurato per il particolare formato.

Formato	Estensione	MIME-Type	Standard
PDF o PDF/A	.pdf	application/pdf;NA	ISO 32000-1 (PDF), ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	.tif	image/tiff;NA	ISO 12639(TIFF/IT); ISO 12234 (TIFF/EP)
XML	.xml	text/xml;1.0	
TXT	.txt	text/plain;NA	

Conservare documenti in altri formati (jpeg, Open Document Format, eml, DICOM, ecc..) è sempre possibile.

Qualora un Soggetto Produttore necessiti di formati aggiuntivi rispetto a quelli standard, dovrà segnalarlo nei 'Dati Tecnici di attivazione' (compresi nelle 'Specificità del Contratto') ed eventualmente conservare gli appositi visualizzatori in una sezione predefinita dell'ambiente assegnato.

I formati aggiuntivi devono essere concordati, dunque, tra il Soggetto Produttore e InfoCert in fase contrattuale e non è possibile caricare visualizzatori per formati non preventivamente concordati e configurati nel sistema.

I visualizzatori di formati aggiuntivi ai predefiniti devono essere inviati dal Soggetto Produttore prima di iniziare la conservazione dei documenti (il sistema accetta i documenti in conservazione anche se il visualizzatore non è caricato, ma finché non viene caricato non è possibile effettuare l'esibizione dei documenti). Il caricamento di un visualizzatore per un particolare mime/type va effettuato una sola volta, ulteriori caricamenti per lo stesso mime/type verranno identificati come aggiornamenti di versione del visualizzatore.

Di seguito è riportata la tabella di sintesi del processo di caricamento dei visualizzatori, inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema: input\dettaglio delle attività\output.

Responsabilità **Attività**	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
1. Creazione del file dei parametri di upload, del file della scheda tecnica e predisposizione dei file del visualizzatore.							**R**
2. Invio della richiesta al sistema di conservazione.							**R**
3. Validazione delle informazioni presenti nei file della richiesta	**R**				**E**	**V**	
4. Caricamento del visualizzatore, creazione del file IPdA, marcatura temporale e firma digitale	**R**				**E**	**V**	

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
dello stesso ed invio al soggetto Produttore.							

[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]

Torna al sommario

6.2 Pacchetto di versamento

Di seguito è riportata la tabella di sintesi del processo di versamento del pacchetto, inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema input\dettaglio delle attività\output.

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
1. Invio al sistema di conservazione del pacchetto di versamento.							**R**
2. Validazione del pacchetto di	**R**				**E**	**V**	**R**

Responsabilità Attività	Responsabile del servizio della Conservazione	Responsabile della funzione archivistica	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto Produttore
versamento.							
3. Generazione del pacchetto di archiviazione.	**R**				**E**	**V**	
4. Memorizzazione e creazione “copia di sicurezza”.	**R**			V	**E**	**V**	
5. Invio dell'IPdA al Soggetto Produttore.	**R**						

L'art. 7 comma c) del DPCM del 3 dicembre 2013 introduce, inoltre, l’obbligo di generare il Rapporto di Versamento.

L’insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

Il Rapporto di Versamento attesta l'avvenuta presa in carico da parte del sistema di conservazione del pacchetto di versamento inviato dal Produttore ed è l’insieme degli Indici dei Pacchetti di Archiviazione prodotti per ogni singolo documento oggetto di versamento (per i dettagli tecnici si rimanda a ‘Specificità del Contratto’ SPT/NDOC- Specifiche tecniche per l’integrazione).

Il rifiuto dei pacchetti di versamento avviene nella modalità descritta nelle ‘Specificità del Contratto’ SPT/NDOC- Specifiche tecniche per l’integrazione e con le casistiche definite SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc.

Le eventuali personalizzazioni specifiche di un contratto sono descritte nei documenti elencati e descritti nel capitolo 10 - 'Specificità del Contratto'.

Torna al sommario

6.3 Pacchetto di archiviazione

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione. Ad ogni documento il Sistema di conservazione associa un file XML, detto Indice del Pacchetto di Archiviazione. L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto di versamento è detto Rapporto di Versamento.

L'Indice del Pacchetto di Archiviazione è un file in formato XML, marcato temporalmente e firmato digitalmente dal Responsabile del servizio della Conservazione, generato dal sistema, che contiene i metadati in formato UNI SInCRO e le informazioni di conservazione del documento e viene con esso conservato.

In particolare, nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA
- il token del documento (ovvero il suo identificativo univoco)
- l'operazione eseguita (conservazione, rettifica, scarto e cancellazione)
- il bucket (ovvero l'area di conservazione) associato al Soggetto Produttore e la policy utilizzata
- il nome dei file che compongono il pacchetto, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte
- eventuali informazioni relative al documento rettificante e rettificato
- il tempo di creazione (timestamp) del file IPdA
- l'impronta di Hash del documento.

L'insieme degli IPdA di un pacchetto di versamento formano il Rapporto di versamento di cui all'art. 9, comma d) del DPCM del 3 dicembre 2013.

Il file IPdA è reso disponibile con il documento di riferimento ad ogni operazione di conservazione e richiesta di esibizione.

Torna al sommario

6.4 Pacchetto di distribuzione

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione.

Le procedure di esibizione permettono di estrarre dal sistema un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione, utilizzando il relativo token (ovvero l'identificativo univoco del documento da esibire) o utilizzando uno o più metadati versati.

Insieme ai file costituenti il pacchetto di distribuzione, sono rese disponibili anche le informazioni che qualificano il processo di conservazione, ossia il file IPdA e un'Attestazione di corretta conservazione e datacertazione firmata dal Responsabile del servizio di Conservazione.

Non è possibile esibire parti singole di documento.

L'esibizione può restituire i pacchetti in tre modalità differenti: in un pacchetto di distribuzione in formato zip contenente al suo interno tanti pacchetti quanti sono i documenti da esibire, in un unico pacchetto di distribuzione in formato zip, oppure un file alla volta (quest'ultima modalità deve essere compatibile con il client di esibizione dell'utente).

Le procedure del sistema mantengono e aggiornano ad ogni nuovo invio il database di tutti i token; il database viene interrogato ad ogni richiesta di rettifica, scarto e cancellazione, ricerca ed esibizione confrontando il token inviato con quelli memorizzati. La procedura assicura di agire solamente sul documento richiesto, e solamente se in possesso dei dovuti profili di autorizzazione.

L'esibizione del pacchetto di distribuzione ottenuto tramite interrogazione al sistema di conservazione rappresenta un'esibizione completa, legalmente valida ai sensi del secondo comma dell'articolo 10 del DPCM del 03 dicembre 2013 e dell'articolo 5 del DMEF del 17 giugno 2014.

Un apposito strumento di esibizione e verifica, anche detto “Esibitore a Norma”, permette di richiamare agevolmente un documento conservato e consente di ottenere in modo automatico sia la verifica delle firme digitali e delle marche temporali apposte che le verifiche di integrità dei documenti conservati e di tutti gli altri elementi conservati.

Si rimanda al ‘MU/ESIB Manuale Utente Esibitore LegalDoc’ – ‘Specificità del Contratto’ per il dettaglio delle funzionalità di verifica del sistema.

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

Il sistema di conservazione è erogato in modalità SaaS (Software as a Service) secondo uno schema di Business Process Outsourcing (BPO) e permette di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

Il sistema consente le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati;
- **conservazione del pacchetto di archiviazione**: il documento, ricevuto nei Data Center di InfoCert in formato digitale statico non modificabile, viene conservato a norma di legge per tutta la durata prevista ed è contenuto in un pacchetto di archiviazione;
- **rettifica del pacchetto di archiviazione**: un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica è una modifica logica, nel pieno rispetto del principio di tracciabilità e la rettifica si applica al pacchetto di archiviazione;
- **scarto/cancellazione del pacchetto di archiviazione:** in caso un documento sia stato versato per errore. La cancellazione è una modifica logica, nel pieno rispetto del principio di tracciabilità e si applica al pacchetto di archiviazione; per la cancellazione fisica di pacchetti di archiviazione ritenuti privi di valore amministrativo e di interesse storico-culturale dal Produttore, occorre formulare apposita richiesta a InfoCert (scarto archivistico);
- **ricerca dei documenti conservati**: l'utente autorizzato può eseguire una ricerca tra i documenti conservati trasversalmente sulle classi documentali, utilizzando uno o più metadati popolati in fase di caricamento;
- **esibizione del pacchetto di distribuzione:** il documento richiesto via web viene richiamato direttamente dal sistema di conservazione digitale ed esibito, con garanzia della sua opponibilità a terzi; attraverso l'Esibitore di LegalDoc è possibile visualizzare e scaricare sia il documento conservato che gli altri documenti a corredo della corretta conservazione (file di indici, file di parametri, Indice del Pacchetto di Archiviazione);
- **visualizzazione delle statistiche di conservazione**;
- **caricamento dei visualizzatori**: è previsto il deposito dei visualizzatori da parte del Soggetto Produttore qualora la tipologia dei file conservati non sia quella standard, definita in fase di attivazione del sistema.

Il sistema di conservazione, quindi, integra il sistema di gestione del Soggetto Produttore, sia esso un'azienda o un ente locale, e ne estende i servizi con funzionalità di stoccaggio digitale (archivio di deposito).

Le fasi di creazione, utilizzo e archiviazione dei documenti sono organizzate liberamente, in quanto il servizio interviene solamente nella fase di conservazione e solamente per i documenti che il Soggetto Produttore sceglie di conservare.

Torna al sommario

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

Di seguito è riportata la tabella che descrive l'acquisizione dei pacchetti, seguendo lo schema: input\dettaglio delle attività\output.

ATT.1 Invio al sistema di conservazione del pacchetto di versamento

INPUT	*Documento da inviare al sistema di conservazione tramite il pacchetto di versamento*	
Sistema di gestione documentale del Soggetto Produttore		Invocazione del sistema di conservazione da parte del sistema di gestione, secondo lo standard descritto nelle SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc.
		Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di sessione (IdSessionId)
		Trasmissione del pacchetto di versamento costituente il documento (file di dati, il file di indici del documento e il file dei parametri di conservazione) secondo le modalità di trasmissione descritte nelle SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc.
OUTPUT	*pacchetto di versamento inviato*	

Per maggiori dettagli si rimanda al documento “SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc” – ‘Specificità del Contratto’.

Torna al sommario

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

ATT.1 Validazione del pacchetto di versamento

INPUT	*Pacchetto di versamento*
Sistema di conservazione	Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal Soggetto Produttore, a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema di gestione del Soggetto Produttore dell'errore intercorso. In questo caso, termine del flusso.
	Controllo dei valori indicati dal Soggetto Produttore nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
	Controllo dei valori indicati dal Soggetto Produttore nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione, non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.
	Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.

OUTPUT	*pacchetto di versamento verificato*

Torna al sommario

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

Le fasi previste sono la memorizzazione, la creazione del file IPDA e la marcatura temporale dello stesso.

ATT.1 Generazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*
Sistema di conservazione	Eventuale apposizione della firma digitale sul file di dati, cioè sul documento da conservare (se prevista da accordi contrattuali appositi esplicitati nei 'Dati Tecnici di attivazione', che fanno parte delle 'Specificità del contratto')
	Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy ed il bucket (area di conservazione) utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo (token) assegnato al documento,
	Marcatura e firma da parte del Responsabile del servizio della Conservazione del file IPdA. Copia del file sul supporto primario.
	Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.

OUTPUT	*pacchetto di archiviazione*

ATT.2 Memorizzazione e creazione copia di sicurezza

INPUT	*Pacchetto di archiviazione*	
		Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali
		Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito.
		La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
OUTPUT	*Documenti conservati*	

ATT.3 Invio dell'IPdA al soggetto Produttore

INPUT	*File IPdA*	
		Invio dell'esito e del file IPdA al soggetto Produttore.
OUTPUT	*Esito conservazione inviato*	

Torna al sommario

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

All'interno delle 'Specificità del Contratto' SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc è presente la griglia riassuntiva dei codici errore che il servizio LegalDoc restituisce

in seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto. La griglia riporta le seguenti informazioni:

- Codice di errore - codifica abbreviata dell'errore avvenuto
- Messaggio di errore - breve descrizione dell'errore avvenuto

I campi codice e descrizione vengono inseriti nel corpo della risposta HTTP.

L'assistenza LegalDoc è contattabile mediante ticket https://help.infocert.it/

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Di seguito è riportata la tabella che descrive la gestione dei pacchetti di archiviazione, seguendo lo schema: input\dettaglio delle attività\output.

ATT.1 Verifica del pacchetto di versamento

INPUT	*Pacchetto di versamento*	
Sistema di conservazione	1	Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal soggetto Produttore, a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema di gestione del soggetto Produttore dell'errore intercorso. In questo caso, termine del flusso.
	2	Controllo dei valori indicati dal soggetto Produttore nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
	3	Controllo dei valori indicati dal soggetto Produttore nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione,

		non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.
	4	Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.
OUTPUT	*pacchetto di versamento verificato*	

ATT.2 Formazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*	
Sistema di conservazione	1	Eventuale apposizione della firma digitale sul file di dati (se prevista da accordi contrattuali)
	2	Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy ed il bucket (area di conservazione) utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo assegnato al documento,
	2	Marcatura e firma da parte del Responsabile del servizio di Conservazione del file IPdA. Copia del file sul supporto primario.
	3	Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
	4	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.
OUTPUT	*pacchetto di archiviazione*	

ATT.3 Memorizzazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*	
Sistema di conservazione	1	Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali
	2	Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito.
	3	La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
OUTPUT	*Documenti conservati*	

Torna al sommario

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

ATT1. Ricerca del documento da esibire

INPUT	*Lista di token archiviati dal sistema*	
Sistema di Gestione documentale del Soggetto Produttore		Ricerca negli archivi del sistema del token relativo al documento da esibire attraverso le procedure previste dai sistemi di gestione.
		Restituzione del token corretto.
OUTPUT	*Token relativo al documento da esibire*	

ATT2. Richiesta di esibizione del documento conservato

INPUT	*Richiesta di esibizione da eseguire*
Sistema di Gestione documentale del Soggetto Produttore	Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di session (ldSessionId).
	Invocazione del servizio di esibizione del sistema di conservazione secondo le modalità descritte nelle 'Specificità del Contratto' SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc. In questa chiamata viene utilizzato il token ricavato in precedenza.
OUTPUT	*Richiesta di esibizione eseguita*

ATT.3 Accettazione della richiesta da parte del sistema di conservazione

INPUT	*Richiesta di esibizione*
Sistema di conservazione	Ricezione della richiesta di esibizione del documento.
	Controllo di corrispondenza tra il token inviato dal Soggetto Produttore e quelli dei documenti conservati.
OUTPUT	*Richiesta di esibizione presa in carico*

ATT.4 Risposta del sistema di conservazione ed esibizione del documento

INPUT	*Richiesta di esibizione acquisita*
	Ricerca dei file costituenti il documento e dei file attestanti il processo di conservazione corrispondenti al token inviato e preparazione del pacchetto di distribuzione.
	Invio della risposta al sistema del Soggetto Produttore.

OUTPUT	*Documento esibito*

Torna al sommario

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

Per duplicato si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Per copia si intende il documento informatico avente contenuto identico al documento da cui è tratto, ma con forma diversa.

La conservazione avviene su supporto primario e su supporto secondario, quindi con duplicazione automatica. Come descritto in seguito, tali supporti sono magnetici ad alte capacità e performance, che garantiscono la ridondanza interna del dato. È inoltre eseguito un backup periodico su tape magnetico.

La creazione di copie informatiche, invece, in caso di adeguamento del formato rispetto all'evoluzione tecnologica sarà presa in carico dal Responsabile del servizio della Conservazione e dalle figure professionali coinvolte nel processo di conservazione in base alle specifiche del formato in questione e al know-how tecnologico a disposizione. A fronte di questa analisi sarà progettata una soluzione di concerto con il Soggetto Produttore del formato più idoneo per permettere la leggibilità del documento conservato.

Possono essere generati anche duplicati o copie attraverso l'Esibitore o su supporto ottico, su specifica richiesta del Soggetto Produttore. Nel primo caso il Produttore/Utente agisce autonomamente con apposite credenziali attraverso l'Esibitore di LegalDoc. Nel secondo caso il Soggetto Produttore inoltra la richiesta ai suoi riferimenti abituali (help desk o account) che poi provvedono alla veicolazione verso gli operatori interni.

L'intervento di un Pubblico Ufficiale per attestare la conformità di una copia all'originale avviene secondo quanto previsto dagli articoli 22 e 23 del Codice e dalle Regole Tecniche del DPCM del 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.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

In LegalDoc esistono due diverse metodologie di 'cancellazione':

1. Cancellazione logica: eliminazione di un documento versato in conservazione per errore materiale, gestita in autonomia solo dal Soggetto Produttore (attraverso apposite chiamate WS), per cui il documento cancellato è ancora consultabile dall'Utente (compare con lo 'stato': 'cancellato'), in ossequio al principio di tracciabilità informatica.

2. Cancellazione fisica o scarto archivistico: eliminazione vera e propria di un documento o di un pacchetto di archiviazione e di qualsiasi duplicato prodotto durante le attività di conservazione, sia dal punto di vista logico che dal punto di vista fisico, per cessata rilevanza ai fini amministrativi, legali o di ricerca storica, ai sensi del Codice Privacy, del GDPR e del Codice dei beni culturali. Questa attività è espressamente richiesta a InfoCert dal Soggetto Produttore, mediante apposita lista debitamente firmata (anche attraverso apposite chiamate WS).

Per gli enti pubblici e per gli archivi privati dichiarati di notevole interesse storico, le proposte di scarto sono sottoposte a nulla osta delle soprintendenze archivistiche o delle commissioni di sorveglianza di competenza. La stesura di 'Piani di Conservazione' (detti anche 'Massimari di selezione e scarto'), la selezione dei documenti da scartare e la procedura di sdemanializzazione e approvazione ministeriale sono in capo al Soggetto Produttore, che può avvalersi del supporto della Digital Consulting di InfoCert.

La distruzione degli eventuali supporti ottici rimovibili di back-up è effettuata mediante strumentazione adeguata e seguendo le procedure definite per lo smaltimento dei rifiuti prodotti.

Il Responsabile del servizio della Conservazione mantiene traccia delle richieste di scarto ricevute e correttamente eseguite, e vengono redatti Attestati di scarto firmati digitalmente dal Responsabile del servizio.

Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di hand-over tra conservatori e scarto archivistico in LegalDoc'.

Torna al sommario

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

Nel caso il Soggetto Produttore decida di rescindere o interrompere il contratto di affidamento del servizio di conservazione, il Responsabile del servizio della Conservazione provvede a comunicare al Soggetto Produttore la lista dei pacchetti di archiviazione conservati.

Il soggetto produttore può effettuare il download dei propri Pacchetti di Distribuzione in autonomia, attraverso la procedura di esibizione, o richiedendo il servizio di restituzione al proprio commerciale di riferimento (su supporto da concordare in base a volume ed esigenze).

Se i supporti sono removibili, i documenti contenuti sono criptati e compressi con password apposita e non devono contenere nel dorso o nella custodia nessun riferimento al soggetto produttore o al contenuto.

Il soggetto produttore provvederà a inviare anche copia della liberatoria denominata 'MODULO DI RESTITUZIONE DATI – SERVIZIO LEGALDOC' sottoscritta digitalmente dal Responsabile della Conservazione interno. Al termine della procedura di hand over verso il nuovo Conservatore per rescissione o risoluzione del contratto di servizio, i pacchetti conservati verranno cancellati da LegalDoc.

Insieme ai veri e propri documenti conservati, sono rese disponibili anche le informazioni e i documenti a corredo della corretta conservazione.

Gli archivi di conservazione generati dal sistema InfoCert sono conformi allo standard di interoperabilità UNI SInCRO: l'interrogazione di tali archivi restituisce le informazioni secondo il suddetto standard.

L’adozione di tale standard permette l’interoperabilità e la trasferibilità dei dati in modo semplificato.

Per ulteriori dettagli si rimanda all’apposito documento interno ‘Procedura di hand-over tra conservatori e scarto archivistico in LegalDoc’.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

La descrizione dell'architettura generale del sistema di conservazione è stata depositata in AgID in fase di accreditamento.

Il sistema è organizzato su più siti (Padova, Modena, Milano).

Il sistema di conservazione è implementato da un'applicazione software appositamente sviluppata a tale scopo (applicazione Java in architettura distribuita, ossia costituita da molteplici componenti) e da una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, PEC).

Il sistema è reso in modalità SaaS (Softwareas a Service) e consente al Soggetto Produttore di accedere ai sistemi di conservazione dei documenti informatici su un elaboratore elettronico, gestito da InfoCert e fisicamente posto nei locali di quest'ultima, in conformità a quanto descritto nei documenti delle 'Specificità del Contratto'.

Il sistema è accessibile dalla apposita URL di rete e il Soggetto Produttore richiama il sistema di conservazione secondo le modalità concordate.

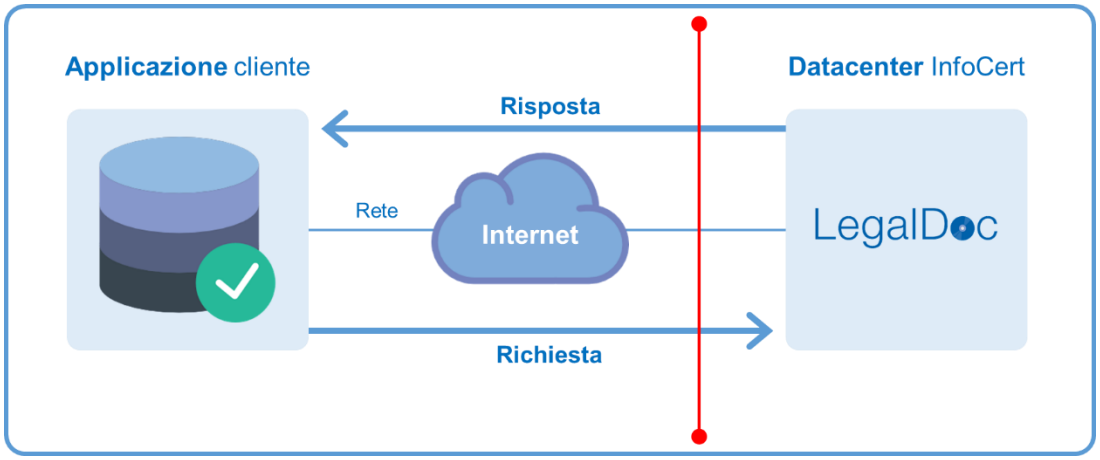

Figura 1 Rappresentazione del servizio attraverso la rete

Dal punto di vista architetturale LegalDoc è realizzato utilizzando la tecnologia dei Web Services.

I Web Services di LegalDoc sono implementati secondo architettura REST su protocollo HTTPS.

LegalDoc è dotato anche di un'interfaccia (LegalDoc WEB) utilizzata sia per il versamento manuale di alcune tipologie documentali, sia per la ricerca e l'esibizione a norma di documenti conservati.

L'esibitore è un'applicazione in tecnologia web, che permette ad un utente, precedentemente definito e in possesso delle debite autorizzazioni e credenziali, di accedere al sistema di conservazione LegalDoc da un qualsiasi computer, purché collegata in rete.

Attraverso l'esibizione a norma diventa possibile:

- estrarre un documento e visualizzarlo a video;
- produrre copia cartacea o su altro supporto informatico del documento;
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione;
- prendere visione dei file a corredo che formano il pacchetto di distribuzione e che qualificano il processo di conservazione attestandone il corretto svolgimento (Indice di Conservazione UNI SINCRO, altrimenti detto Indice del Pacchetto di Archiviazione, File di parametri, File di indici, File di dati, Attestato di conservazione);
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione;
- verificare l'integrità del documento.

Il sistema è protetto da firewall ed implementa un sistema di back-up dei dati memorizzati.

Torna al sommario

8.1 Componenti Logiche

Il servizio LegalDoc è basato su tecnologia REST e svolge le operazioni di conservazione, esibizione, rettifica, cancellazione e ricerca.

Torna al sommario

8.2 Componenti Tecnologiche

8.2.1 Firewall

I firewall assicurano la difesa del perimetro di sicurezza tra il sistema e il mondo esterno, nonché tra i sistemi dedicati all'erogazione del sistema e i sistemi che interfacciano i dispositivi sicuri per la generazione della firma digitale.

I firewall sono configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile.

Torna al sommario

8.2.2 Back-up

L'intero sistema di conservazione viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria per la sicurezza.

Torna al sommario

8.2.1 Dispositivo HSM di firma digitale dei pacchetti

Al buon esito del processo di conservazione, il Responsabile del servizio della Conservazione di InfoCert appone la propria firma digitale su ogni pacchetto di archiviazione, mediante un sistema di firma digitale automatica erogato dalla Certification Authority InfoCert, che si avvale di un dispositivo crittografico ad altre prestazioni Hardware Security Module e di un certificato qualificato di firma appositamente generato e su cui ha pieno controllo.

Torna al sommario

8.2.2 Servizio di marcatura temporale dei pacchetti

Per l'emissione delle marche temporali il sistema si avvale del servizio di marcatura di InfoCert, Certification Authority accreditata, compliant eIDAS. La marca temporale viene richiesta al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert. Il root-certificate della TSA è depositato presso AgID. Il TSS è sincronizzato via radio con l'I.N.RI.M di Torino (Istituto Nazionale di Ricerca Metrologica, già Istituto Elettrotecnico Nazionale "Galileo Ferraris") ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

Torna al sommario

8.3 Componenti Fisiche

InfoCert, in accordo con i Soggetti Produttori e come previsto dalle Condizioni Generali del Contratto si avvale di partner tecnologici per le componenti fisiche del data center.

Torna al sommario

8.3.1 Sistema Storage

Il sistema di conservazione di InfoCert e dei suoi partner tecnologici supporta la memorizzazione dei file sia su storage magnetici ad alte performance che su sistema *Object Storage S3*. Tali storage, scelti tra i primari fornitori di tecnologie presenti sul mercato, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato e rispondono all'esigenza di memorizzazione a lungo termine dei *fixed content*, ossia dei file che devono essere conservati con garanzia nel tempo di integrità e disponibilità del contenuto.

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni che prevedano la cifratura dei documenti che contengono dati sensibili ed eventualmente anche degli altri.

I sistemi di storage sono stati valutati da InfoCert e dai suoi partner tecnologici sotto molteplici profili e, in virtù delle loro caratteristiche fisiche e architetturali, sono ritenuti idonei ad essere utilizzati nel sistema di conservazione.

Nell'ambito del sistema di conservazione, lo storage magnetico ad alte performance rappresenta sia il supporto primario di conservazione posto fisicamente presso la sede InfoCert di Padova, sia il supporto secondario posto nel sito di *disaster recovery* di Modena.

I due sistemi sono interconnessi mediante collegamenti ad alta velocità dedicati, completamente ridondati e protetti da misure di sicurezza. I collegamenti consentono la replicazione dei dati conservati eliminando il rischio di distruzione di tutte le copie delle informazioni in caso di danno irreparabile a livello di sito.

Questo secondo sistema funge anche da copia di sicurezza.

L'allineamento tra il sito primario e il sito secondario avviene coerentemente con le politiche generali di *Disaster Recovery* definite in InfoCert che garantiscono RTO e RPO inferiori alle 48 ore.

Per il sistema di *Object Storage S3* InfoCert si avvale dei servizi cloud computing *Amazon Web Services (AWS)* che garantisce la ridondanza e il rispetto delle misure di sicurezza.

Torna al sommario

8.3.2 Sincronizzazione dei sistemi

Tutti i server di InfoCert, attraverso il protocollo NTP (Network Time Protocol), sono sincronizzati sul “tempo campione” fornito dall’Istituto di Ricerca Metrologica – INRIM (già Istituto Elettrotecnico Nazionale “Galileo Ferraris”), abilitato a fornire il “tempo campione” ai sensi dell’articolo 2, comma 2, lettera b) del D.M. 30 novembre 1993, n. 591 “Regolamento concernente la determinazione dei campioni nazionali di talune unità di misura del Sistema internazionale (SI) in attuazione dell’art. 3 della L. 11 agosto 1991, n.273. La sincronizzazione è protetta da misure di sicurezza fisiche e logiche documentate per impedirne la manomissione.

Il meccanismo di allineamento temporale tra i sistemi fornisce la certezza della successione temporale degli avvenimenti nel sistema. La sincronizzazione delle macchine

infatti, genera dei file di log temporalmente omogenei tra loro, che permettono di ricostruire con certezza l'ordine di accadimento degli eventi intervenuti a tutti i livelli del sistema, e di individuare la sequenza di svolgimento delle varie operazioni.

Torna al sommario

8.4 Procedure di gestione e di evoluzione

Il sistema di conservazione di InfoCert e il processo da questi implementato rispondono interamente alle norme di legge che regolano la materia.

La progettazione e il continuo miglioramento del sistema di conservazione sono il frutto di una intensa opera di confronto tra le professionalità e le competenze delle diverse funzioni aziendali, al fine di giungere all'erogazione di un sistema pienamente conforme alle norme, architetturalmente stabile, affidabile, e che garantisca elevati livelli di servizio all'utente in condizioni di assoluta sicurezza, certezza degli accessi e tracciabilità delle operazioni.

Punto fondante del processo di progettazione è l'attenta disamina delle norme, al fine di definire puntualmente i requisiti legali che il sistema deve possedere per assicurare la corretta implementazione della conservazione.

Il rispetto dei requisiti di legge è la condizione imprescindibile per l'erogazione del servizio. Oltre a questi sono definiti ulteriori requisiti funzionali, di architettura e di connettività e interoperabilità. I requisiti funzionali, individuati dal gruppo di competenza, rispondono all'obiettivo di offrire al Soggetto Produttore le funzionalità da questi richieste, mentre i requisiti di architettura e di interoperabilità rispondono alla necessità di sviluppare e mantenere un sistema stabile, in linea con le evoluzioni tecnologiche e capace di interfacciarsi con gli altri sistemi sviluppati dall'azienda, sfruttando le economie di scala e di conoscenza.

I Responsabili InfoCert, infatti, sono costantemente impegnati nell'attività di 'technology watch' attraverso la partecipazione a gruppi di lavoro nazionali e internazionali, forum e associazioni di settore con lo scopo di monitorare e prevenire l'obsolescenza tecnologica sia logica che fisica.

Torna al sommario

8.4.1 Criteri di organizzazione del contenuto

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi in cui i documenti sono corredati da tutta una serie di metadati. I documenti inviati al sistema di conservazione, infatti, vengono aggregati secondo criteri di omogeneità secondo le informazioni di configurazione definite in fase contrattuale. In particolare, vengono concordati i parametri fondamentali (bucket, policy, classi documentali) con i quali sono organizzati i documenti presi in carico, per consentire la maggiore interoperabilità possibile tra i sistemi di conservazione.

Se le tipologie documentali conservate sono di tipo sanitario (es. referti, immagini diagnostiche, ecc..) si provvede alla conservazione in ambienti separati e cripatati, in ottemperanza della normativa sulla privacy e sulla data protection.

Torna al sommario

8.4.2 Organizzazione dei supporti

Come atto conclusivo della procedura di conservazione, i documenti vengono memorizzati nel sistema di storage, contenenti tutti i documenti inviati in conservazione e i relativi file IPdA in conformità alle Regole AgID, OAIS e UNI SInCRO.

Torna al sommario

8.4.3 Archivio dei viewer consegnati dal Soggetto Produttore

InfoCert ha stabilito dei formati standard per i documenti da inviare in conservazione, dettagliati nei ‘Dati Tecnici di attivazione’ a disposizione del Soggetto Produttore e nel DPCM del 3 dicembre 2013, per i quali l'azienda definisce e mette a disposizione dei Soggetti Produttori i relativi viewer, mantenendoli aggiornati. Al momento dell'attivazione del servizio, il Soggetto Produttore verifica che i documenti inviati siano nel formato standard e siano leggibili con il software definito da InfoCert.

Se un Soggetto Produttore ha l'esigenza di inviare in conservazione documenti in formati differenti da quelli definiti standard, provvede a fornire ad InfoCert, tramite apposita funzionalità dell'applicativo dell’interfaccia di LegalDoc, il relativo software di visualizzazione.

Se il Soggetto Produttore invia documenti in formato non standard senza depositare il relativo visualizzatore, oppure nel caso di invio di documenti in modalità cifrata, è sua cura la conservazione degli strumenti necessari per la decifratura e/o la visualizzazione di quanto conservato.

Il Responsabile del servizio della Conservazione mantiene i programmi consegnati in un apposito database sottoposto a un periodico processo di back-up; in questo processo, il Responsabile è supportato dalle apposite procedure automatiche del sistema.

Torna al sommario

8.4.4 Archivio dell'hardware e del software obsoleto

La tenuta di un archivio dell'hardware e dei sistemi operativi ormai obsoleti ma necessari alla visualizzazione dei documenti conservati non è esplicitamente prevista dalla norma, ma è un'attività che si desume dall'obbligo di tenuta dell'archivio dei software nelle eventuali diverse versioni, e a questo direttamente correlata e fa parte delle misure per combattere l'obsolescenza dei formati, citate all'art. 7 comma 1 lettera g) dal Decreto 2013.

Il progresso tecnologico dei sistemi, tuttavia, può portare all'impossibilità di utilizzare i viewer definiti dal Soggetto Produttore, se divenuti obsoleti, sulle macchine di ultima generazione, rendendo di fatto impossibile la presa di conoscenza del contenuto del documento e inficiandone così la validità legale nel tempo. Per far fronte a questo rischio, il Responsabile del servizio della Conservazione mantiene un archivio di tutte le componenti hardware e software non più compatibili con i programmi di visualizzazione garantiti e/o depositati dal Soggetto Produttore, nel caso questi siano i soli strumenti che consentono di rendere leggibile i documenti conservati associati a tale viewer.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

InfoCert possiede un sistema di gestione integrato che risponde attualmente ai requisiti delle norme ISO 9001, 27001, 20000 e 14001.

È inoltre un Qualified Trust Service Provider (ETSI EN 319 401) per i servizi di certificazione qualificata di: firme elettroniche, sigilli elettronici, validazione temporale e autenticazione siti web.

Particolare attenzione viene quindi posta nel mantenimento di livelli di servizio. attraverso l'dozione di un modello di Service Management System conforme alla citata norma ISO/IEC 20000 ha permesso infatti di:

- mappare ed integrare i Livelli di Servizio (SLA) garantiti ai clienti in relazione ai Livelli di servizio operativi garantiti internamente e quelli contrattuali garantiti dai fornitori;
- strutturare e governare la catena di composizione del valore dei servizi;
- ottimizzare la gestione dei processi aziendali integrando processi produttivi con processi di business fornendo un modello per la gestione sui servizi erogati;
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti;
- garantire un controllo dei fornitori che concorrono alla erogazione dei nostri servizi;
- migliorare la qualità dei servizi di business erogati.

Di seguito lo schema rappresentativo del Modello adottato da InfoCert:

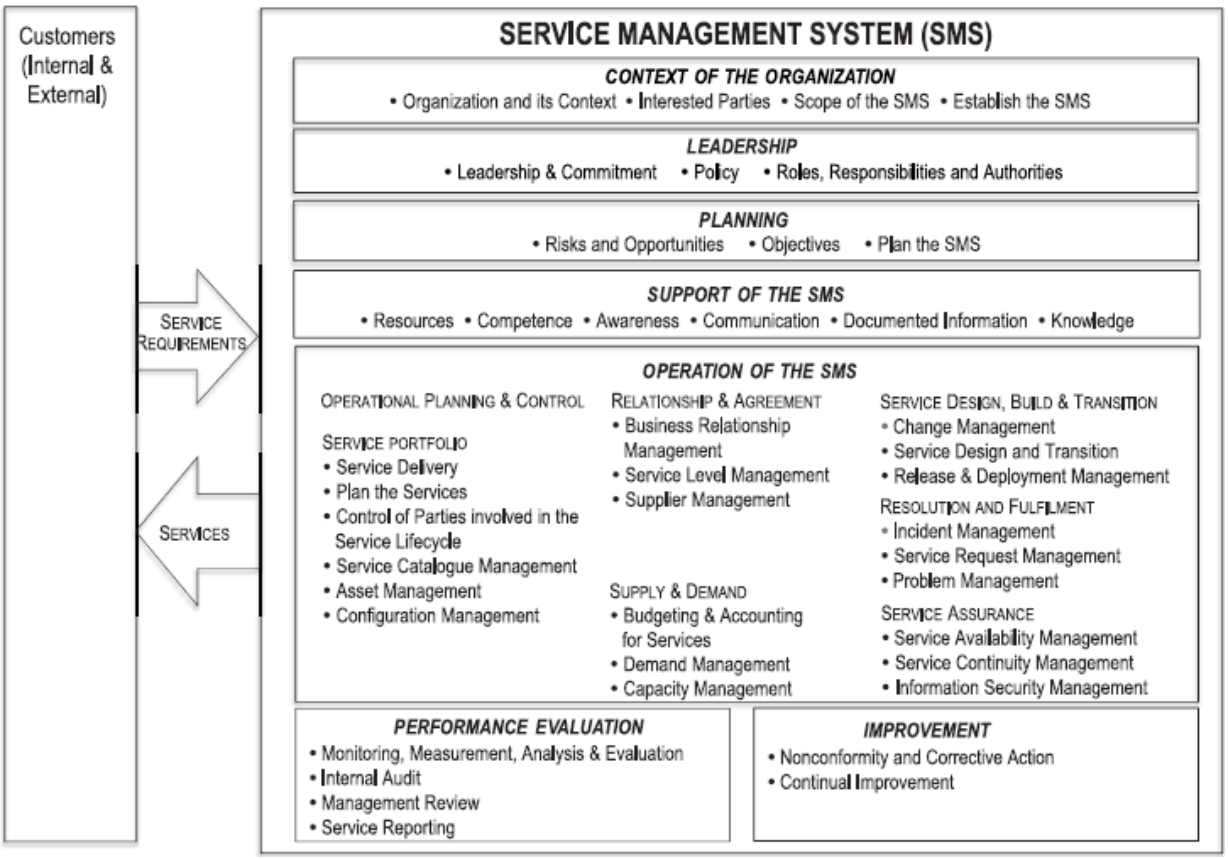

Figura 2 Rappresentazione grafica processi della norma ISO/IEC 20000:11

Le attività di istituzione, attuazione, monitoraggio e sviluppo del Service Management System-SMS seguono il modello ciclico PDCA che si sviluppa nelle seguenti fasi:

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche e i requisiti per la gestione dei servizi inerenti il campo di applicazione; si stabiliscono gli obiettivi di gestione del servizio a tutti i livelli pertinenti.
- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement continuo dei servizi sulla base di quanto definito nel

service management plan, con particolare attenzione al controllo delle modifiche al SMS valutando e limitando I rischi.

- azioni di monitoraggio e revisione del sistema-SMS (Check);
- attuazione di misure a miglioramento del sistema-SMS (Act) ove sono pianificate e attuate idonee azioni correttive sulla base dei risultati della fase precedente.

Il processo di gestione dei Livelli di Servizio [Service Level Management] è considerato un processo cardine del Service Management System in quanto ha effetto sui tre obiettivi principali quali:

- allineare i servizi di business con i bisogni correnti e futuri del cliente
- coordinare i requisiti del mercato sui servizi offerti con gli obbiettivi aziendali
- migliorare la qualità dei servizi di business erogati
- fornire attraverso gli SLA una base per la determinazione del valore del servizio.

Nello specifico InfoCert ha definito degli SLA baseline di riferimento in relazione ai seguenti KPI (Key Performance Indicator):

- Orario di servizio
- Disponibilità di servizio.

Torna al sommario

9.1 Procedure di monitoraggio

La soluzione di monitoraggio, nel seguito denominata TMS, è fornita dal Gruppo Sintesi che si occupa della completa gestione di tutta la piattaforma.

TMS si occupa di monitorare e misurare tutto lo stack tecnologico usato per erogare i servizi InfoCert, infatti non è solo in grado di dire se un servizio o un particolare componente hardware stanno funzionando correttamente, ma è anche in grado di misurarne le risorse utilizzate e le performance.

La piattaforma è costruita a partire da una versione customizzata del noto software open source Nagios e per rilevare i dati dai diversi componenti utilizza diverse tecnologie (SNMP, NRPE, Sahi, ecc.), inoltre, è stata sviluppata l'integrazione con la piattaforma di controllo *Cloudwatch*, tool nativo di AWS consente di avere il pieno controllo e la gestione delle metriche di tutte le componenti presenti in cloud I monitoraggi possono essere eseguiti in modalità attiva (quindi la piattaforma interroga puntualmente le diverse componenti) oppure in modalità passiva (ovvero sono le singole componenti che inviano dati alla piattaforma, senza il bisogno di venire interrogate da essa).

L'infrastruttura di monitoraggio, ad oggi, è composta da:

- due apparati fisici (denominati probe) posizionati all'interno del Data Center,
- una probe posizionata all'interno dei locali della CA,
- un'altra probe posizionata nel sito di DR.

Alle quattro probe fisiche si aggiunge un pool di macchine virtuali posizionate nella server farm di *Clouditalia* e la piattaforma *Cloudwatch* posizionata in AWS Le probe fisiche si occupano di effettuare i monitoraggi sull'infrastruttura ed i servizi ospitati nei locali nei quali sono installate mentre le macchine virtuali si occupano di effettuare le navigazioni dei servizi sia da rete interna che tramite internet, *Cloudwatch* invece gestisce i monitoraggi di tutte le metriche infrastrutturali presenti in AWS. Tutti i dati raccolti vengono infine centralizzati su una piattaforma resa disponibile online per una veloce e facile consultazione degli stessi.

Oltre alle misurazioni effettuate sull'infrastruttura e la verifica del traffico dati tra il cloud e il DC, il sistema di monitoraggio è in grado di misurare anche le performance dei servizi, infatti tramite le navigazioni effettuate dalle macchine virtuali si riesce a capire se un servizio è disponibile e anche quanto tempo impiega per effettuare una certa elaborazione.

Con tutti i dati raccolti si popola una base di dati in ottica di Business Intelligence che risulta di fondamentale importanza per la redazione della reportistica riguardante gli SLA dei vari servizi ma anche, e soprattutto, per supportare i processi di decisione aziendale.

La soluzione di monitoraggio fin qui descritta risulta indispensabile per individuare tempestivamente eventuali anomalie sui servizi erogati da InfoCert, ma soprattutto è in grado di segnalarci su quale dei molti componenti che compongono un servizio andare a concentrare l'azione correttiva per una rapida risoluzione degli incident.

Torna al sommario

9.1.1 Processi di monitoraggio del sistema di conservazione

Il monitoraggio del sistema di conservazione si esplica su due diversi livelli operativi:

- sistema di monitoring della disponibilità del sistema
- sistema di monitoring dell'integrità degli archivi.

Torna al sommario

9.1.2 Monitoring della disponibilità del sistema

Tale operazione viene svolta coerentemente con le procedure di monitoring generali di InfoCert. In particolare, tutte le componenti costituenti il sistema di conservazione, ovvero i servizi applicativi, i processi di elaborazione batch e le interfacce per l'utente finale sono monitorate con i tool definiti nella piattaforma di monitoraggio TMS precedentemente descritta.

A fronte di anomalie rilevate lo strumento invia delle segnalazioni al Service Desk InfoCert che le gestisce in conformità ai processi di Incident Management e, se necessario, Problem Management. Tali processi sono descritti nelle procedure che definiscono il Sistema di gestione integrato InfoCert.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Il sistema di memorizzazione utilizzato, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architetturale e alle procedure di memorizzazione permanente dei dati, garantisce l'immodificabilità, l'integrità, la leggibilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione.

Il sistema mantiene traccia di tutte le operazioni effettuate sui documenti in appositi file di log.

Inoltre, è garantita la tracciatura di tutti i documenti richiamati dal Soggetto Produttore mediante interrogazione al sistema e conseguentemente esibiti, che rappresenta un'ulteriore prova di leggibilità, effettuata direttamente dal Soggetto Produttore.

In aggiunta, come descritto dall'art. 7 comma 1 lettera g) del DPCM del 3 dicembre 2013, "al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati", InfoCert, per rispondere a tali richieste, ha attivato sottosistemi di controllo automatico dedicati alla simulazione della navigazione nel sistema e delle operazioni che effettua l'utente, svolgendo controlli di coerenza dei dati e attività di ripristino da situazioni di errore.

In ogni occasione in cui il file viene copiato o spostato di posizione, funzionalità automatiche verificano che le sue dimensioni non siano mutate durante lo spostamento e che non siano intervenute alterazioni, che possano inficiarne la visualizzazione.

Il Responsabile del servizio della Conservazione, come descritto nell'art. 7 comma 1 lettera f) "assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità" dei documenti conservati con procedure automatiche e manuali, al fine di prevenire il rischio che i documenti non possano essere visualizzabili, inficiando il mantenimento della loro validità legale nel tempo.

L'apposita procedura, detta verificatore, esegue il test di leggibilità binaria mediante il continuo calcolo delle impronte dei documenti conservati, con successivo confronto con l'hash del documento contenuto nel file delle direttive della conservazione inviato dal Soggetto Produttore. Se la procedura non registra differenze tra i due hash, il documento è inalterato rispetto a quanto trasmesso dal Produttore.

Vengono eseguiti i seguenti passi operativi:

- verifica della validità della firma digitale e della marcatura temporale apposte all'atto della conservazione dal Responsabile del servizio della Conservazione sul file IPdA e, se presenti, verifica della firma digitale e della marcatura temporale del documento;
- calcolo dell'impronta del documento e confronto con quella contenuta all'interno del file IPdA;

- generazione di un report che viene automaticamente sottoposto alla conservazione nell'area dedicata al Responsabile del servizio della Conservazione (quindi a sua volta firmato e marcato temporalmente dal Responsabile del servizio della Conservazione stesso).

La procedura appena descritta viene applicata sia sul supporto primario sia su quello secondario.

In caso di anomalie, se il documento risulta corrotto in uno dei due repository, il sistema tenta il ripristino automatico con il dato presente nel repository integro. Se invece ambedue le copie sono alterate, viene inviato un alert al Responsabile del servizio della Conservazione, che tenterà il ripristino manuale partendo da un'altra sorgente (per esempio le copie di backup). Se nessuna sorgente è disponibile viene redatto un verbale di incidente, sottoscritto e conservato dal Responsabile del servizio della Conservazione per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.

Periodicamente, il sistema produce dei report di sintesi dell'attività di verifica svolta.

In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio della Conservazione e i suoi Responsabili incaricati sono dotati di apposita strumentazione (detta CORE, Console del Responsabile), con credenziali dedicate, con la quale procedono manualmente e periodicamente ad una verifica campionaria di leggibilità dell'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.

Viene poi redatto automaticamente un verbale che attesta l'elenco dei documenti visualizzati, successivamente sottoscritto e conservato dal Responsabile del servizio della Conservazione nell'area appositamente creata nel sistema di conservazione.

9.3 Controlli

Oltre ai monitoraggi appena descritti, il sistema di conservazione implementa numerosi sotto-processi dediti al controllo del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al Soggetto Produttore o al personale incaricato dell'amministratore del sistema.

I controlli effettuati si distinguono nelle tre tipologie: controlli di versamento, controlli di

processo e controlli periodici.

Torna al sommario

9.3.1 Controlli di versamento

In fase di versamento dei pacchetti in LegalDoc vengono automaticamente eseguiti dei controlli, preventivamente concordati con il soggetto Produttore nelle 'Specificità del contratto' all'attivazione del servizio e che riguardano:

- abilitazione utenza al versamento;
- validità sessione in uso (di default della durata di un'ora tra login e logout);
- struttura del file di Parametri (contenente le informazioni per la leggibilità nel tempo del documento da conservare);
- struttura del file di Indici (contente i metadati del documento da conservare, alcuni dei quali obbligatori, in coerenza con i 'Dati Tecnici di attivazione');
- mime type dichiarato in coerenza con i 'Dati Tecnici di attivazione';
- dimensione massima del documento da conservare (di default 256 megabyte, variabile su richiesta);
- presenza nello stesso path dello stesso nome-file (su richiesta);
- validità del certificato qualificato di firma digitale con cui è sottoscritto il documento da conservare (su richiesta).

InfoCert non effettua controlli sull'eventuale presenza di virus nei pacchetti di versamento, che sono conservati in LegalDoc alla stregua di tutti gli altri file.

Torna al sommario

9.3.2 Controlli di processo di progettazione e sviluppo dei servizi

L'organizzazione garantisce che non vengano rilasciati prodotti/servizi per i quali non siano state completate le attività di controllo della qualità citate nelle relative procedure di rilascio.

Per maggiori dettagli si rimanda a "PR/235 Progettare e sviluppare un servizio informatico InfoCert", "PR/225- Change Management InfoCert", "Service Management System-SMS".

Torna al sommario

9.3.3 Monitoraggio e registrazioni durante il ciclo produttivo

Lungo l'intero ciclo produttivo si effettuano i controlli al fine di verificare la conformità del prodotto e del processo a quanto previsto dalle procedure applicabili.

Nelle procedure “PR/235 Progettare e sviluppare un servizio informatico InfoCert” e “PR/225- Change Management InfoCert” sono indicate le fasi specifiche per i controlli, i test e le misurazioni del prodotto/servizio in termini di ciclo di vita, tecniche, metriche del SW, gestione dei controlli, dello “sforzo/effort”, tenuta in controllo dei costi e dei tempi di realizzazione, la definizione dei mezzi e delle risorse necessarie.

Il prodotto/servizio è oggetto di un processo progressivo di accettazione: le registrazioni documentano la conformità del prodotto ai criteri di accettazione e indicano la persona che autorizza il rilascio.

Il prodotto/servizio è predisposto per la consegna al cliente ad esito positivo delle prove, controlli e collaudi. I prodotti che non superano le prove, i controlli e i collaudi sono sottoposti alla procedura per il trattamento dei prodotti non conformi.

Torna al sommario

9.3.4 Monitoraggio e registrazioni per collaudo finale

Il prodotto/servizio corrispondente ai requisiti contrattuali è oggetto di un processo progressivo di accettazione che viene attivato in occasione di ogni consegna ufficiale al Produttore, o di una accettazione globale fatta alla fine del processo produttivo secondo quanto previsto dalla procedura.

Torna al sommario

9.3.5 Controlli periodici

In InfoCert è attiva una struttura appositamente preposta alla supervisione e controllo della gestione dei problemi e del rispetto dei livelli del sistema per tutte le applicazioni.

La struttura si avvale di un gruppo di lavoro trasversale all'azienda ed effettua la raccolta dei dati relativi al funzionamento dei servizi.

Il gruppo si riunisce con una periodicità mensile al fine di individuare le cause dei malfunzionamenti registrati nel periodo, analizzare le soluzioni contingenti adottate per il superamento del problema e sviluppare eventuali proposte per rimedi strutturali.

Torna al sommario

9.4 Soluzioni adottate in caso di anomalie

Ad ogni semestre il Responsabile del servizio della Conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).

Torna al sommario

9.4.1 Auditing generale del sistema

Il Programma di AUDIT aziendale è attuato secondo le procedure del Sistema Integrato di Gestione.

Gli Audit sono condotti, sempre secondo le citate procedure, con il fine di determinare se i processi aziendali:

- sono in accordo con quanto previsto nei documenti di riferimento
- sono compliant alla normativa di riferimento
- sono compliant agli standard adottati dal sistema di conservazione
- sono attuati efficacemente
- sono idonei al conseguimento degli obiettivi della Qualità e miglioramento servizi

In ogni processo aziendale, le modalità di audit sono improntate alle indicazioni dello standard UNI EN ISO 19011 ed hanno per oggetto:

- strutture organizzative
- risorse utilizzate
- procedure
- processi
- prodotti e i risultati dell'attività
- documentazione
- addestramento
- segnalazioni dei clienti e terze parti.

Le attività di audit sono in capo all'Area Management System che le esegue direttamente o le delega a personale esterno qualificato.

Oltre alle verifiche ispettive sopra descritte indirizzate al Sistema Gestione Qualità, sono pianificati e condotti audit su tutti gli altri componenti del Sistema di Gestione Integrato (SGSI-ISO 27001, SMS-ISO 20000, SGA-ISO14001, Verifiche di interoperabilità condotte da AgID, Privacy, Sicurezza Fisica, M231/01 ecc.).

Relativamente al SGA-ISO14001 l'attività di audit comprende anche la verifica di conformità legislativa.

Relativamente al SGA-ISO14001 l'attività di audit comprende anche la verifica di conformità legislativa.

Il processo prevede inoltre la gestione controllata di tutti gli Audit esterni svolti dagli Enti istituzionali, relativi ai Sistemi di Gestione ed ai Prodotti/Servizi certificati.

A fronte di non conformità rilevate in sede di verifica ispettiva, il Responsabile della Struttura Organizzativa valutata definisce un piano di attuazione delle azioni correttive o migliorative richieste.

Il Responsabile delle verifiche e ispezioni (auditing) pianifica e implementa processi di audit che coinvolgono aspetti di processo, organizzazione, tecnologici e logistici. L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto, alla

documentazione generale del sistema, ai principi che ispirano il sistema qualità e al presente Manuale della Conservazione.

L'audit è un processo fondamentale per lo screening del sistema, in quanto consente l'individuazione delle aree critiche d'intervento e la pianificazione dei necessari interventi sul sistema, ragion per cui è svolto periodicamente.

Torna al sommario

9.4.2 Incident management

L'ambito completo del processo si applica alla gestione degli incidenti informatici che possono interessare uno o più servizi tecnologici eventualmente interconnessi ed è formalmente descritto dalla procedura 'PR455-Incident Management InfoCert'. La procedura definisce anche la metodologia di assegnazione della gravità di un incidente e della relativa priorità di gestione in base alla matrice di analisi di impatto/urgenza effettuata utilizzando le informazioni sul servizio di riferimento e sui relativi SLA del servizio o nelle istruzioni /policy specifiche relative alla sicurezza informatica.

Urgenza ⇨ Impatto⇩	ALTA	MEDIA	BASSA
ALTO	Critica	Alta	Media
MEDIO	Alta	Media	Bassa
BASSO	Media	Bassa	Molto bassa

L'impatto è definito in base alla BIA [Business Impact Analisys] del servizio.

L'urgenza è dettata dallo SLA di disponibilità del servizio.

Il processo di gestione degli incidenti, condotto secondo le raccomandazioni delle Best Practice ITIL e in conformità alle norme ISO 27001, si focalizza sulle modalità di gestione e di ripristino tempestivo degli incidenti informatici.

Il modello organizzativo prevede che il supporto specialistico sistemistico sia gestito dall'area di Product Factory che gestisce il ciclo di vita dell'incidente con gli strumenti per la rilevazione e tracciamento degli eventi.

Il processo d'Incident Management, che ha lo scopo di minimizzare impatti e tempi di disservizio, alimenta il processo di Problem Management (PR456), che a sua volta ha lo scopo di prevenire il verificarsi e il ripetersi di tali errori.

A tale scopo il Problem Management cerca di individuare la causa principale degli incidenti e ne attua le opportune azioni preventive, correttive e/o migliorative.

I processi di Incident Management e Problem Management sono soggetti a un miglioramento continuativo.

Il Responsabile del servizio della Conservazione mantiene il verbale degli incidenti e delle contromisure attuate sono inviate al sistema di conservazione.

Torna al sommario

10. SPECIFICITÀ DEL CONTRATTO

I servizi sono regolati dai seguenti documenti contrattuali, che contengono e descrivono tutte le esigenze richieste dai Soggetti Produttori.

La documentazione contrattuale e tecnica elencata è resa disponibile all'atto del perfezionamento dell'accordo di servizio al Produttore.

1. ***Condizioni Generali di Contratto*** che regola la vendita del servizio di conservazione nelle diverse modalità di erogazione;
2. ***Richiesta di attivazione*** che comporta l'adesione al servizio e disciplina le condizioni economiche;
3. ***Dati tecnici per l'attivazione*** con cui il Soggetto Produttore fornisce tutte le informazioni necessarie su tipologie documentali, metadati e credenziali di accesso di cui necessita;
4. ***File di configurazione*** redatto da InfoCert all'attivazione del servizio, contiene i dati di configurazione del soggetto produttore, delle user d'accesso, delle policy associate e delle tipologie documentali, comprensivi di metadati e formati configurati;
5. ***Atto di affidamento*** che rappresenta la formalizzazione dell'affidamento ad InfoCert del processo di conservazione, la nomina del Responsabile del trattamento dei dati personali ai sensi del Regolamento UE n. 679/2016 GDPR, e stabilisce espressamente quali attività di fatto vengano assunte da InfoCert e quali, al contrario, rimangano a carico dell'affidatario, Soggetto Produttore, come stabilito dagli articoli 5 e 6 del DPCM del 3 dicembre 2013;
6. ***Specifiche Tecniche di integrazione (sia per i web services che per LegalDoc Connector)*** che fornisce tutte le informazioni tecniche necessarie ad operare l'integrazione tra i Sistemi di Gestione documentali del Produttore e il sistema di conservazione di InfoCert;
7. ***Impegno alla riservatezza***;
8. ***Allegato Tecnico*** che descrive le modalità di fornitura del servizio e l'infrastruttura tecnico-tecnologica utilizzata per la sua erogazione;

9. ***Manuale Utente*** che risponde alla necessità di documentare operativamente il processo dal punto di vista del Produttore/Utente;
10. ***Descrizione dei codici di errore*** per fornire una casistica esaustiva dei possibili messaggi di errore del servizio di conservazione e delle azioni che è necessario intraprendere per porvi rimedio.

La documentazione relativa alle procedure e/o ai processi interni di InfoCert, invece, è resa disponibile solo su esplicita richiesta del Soggetto Produttore e all'atto del perfezionamento di una specifica NDA (non-disclosure agreement).

Per i Soggetti Produttori con una infrastruttura tecnologica complessa viene redatto un '**Manuale dei processi per la conservazione**', che rimanda al presente Manuale per quanto riguarda le sezioni standard (es. Struttura organizzativa e Ruoli di responsabilità del Conservatore, Dettaglio tecnico del sistema di conservazione e trattazione dei pacchetti di archiviazione, Monitoraggio e controlli del Conservatore), e dettaglia le specificità del singolo Produttore (es. modalità di versamento o esibizione, tipologie documentali, metadati scelti, infrastrutture tecnologiche particolari).

Torna al sommario