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 condetermina 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, cosi come modificato dal D.Lgs 101/2018 e dal Regolamento UE 2016/679 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 del sistema 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 da rispettare 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,***
- ***Registro giornaliero di protocollo.***

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

		abbiano evidenziato delle anomalie		
	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 alla 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 con cui 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 garantisce gli 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 e controllo 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**– Codice in materia di protezione dei dati personali; cosi come modificato dalla normativa italiana di adeguamento al GDPR il D. Lgs 101/2018;
- **Regolamento UE 2016/679 sulla 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.

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,
- Registro giornaliero di protocollo.

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 la conservazione del registro giornaliero di protocollo.

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

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.

SALERNO PULITA S.p.A.
06 MAG 2025
Prot. N. AU 10955

«*SALERNO PULITA S.p.A.*»

DETERMINAZIONE DELL'AMMINISTRATORE UNICO

n.86 del 06.05.2025

"Manuali di gestione e conservazione del protocollo informatico – Approvazione Aggiornamento";

L'AMMINISTRATORE UNICO

Premesso che:

a- Con determina n.118 prot. AU10639 del 01/08/2023 è stato approvato la revisione 2 dei manuali di "gestione" e "conservazione" del protocollo informatico;

b- Con la nota SAP-0003936 del 23/04/2025 la signora Carmela Fabiano, Responsabile dell'ufficio Amministrazione, e nella qualità di Responsabile del "Protocollo Informatico Enterprise", ha trasmesso, il manuale di "gestione documentale" del protocollo informatico con gli aggiornamenti previsti dalla normativa vigente;

c- Il manuale è adottato in esecuzione delle regole tecniche per il protocollo informatico ai sensi delle Linee guida AgId, adottate con Determinazione n. 371/2021 del 17 Maggio 2021;

d- La necessità di approvazione del manuale nasce dal Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 – Regole tecniche per il protocollo informatico;

DISPONE / DETERMINA:

1) Di approvare il manuale di "gestione documentale" del protocollo informatico allegato alla nota SAP-0003936 del 23/04/2025 trasmesso dalla sig.ra Carmela Fabiano;

2) **che** al personale interessato dell'Azienda sarà fornita la più adeguata informazione tramite gli uffici preposti e la pubblicazione sul portale aziendale sezione Amministrazione Trasparente – sottosezione Atti Generali;

3) Che la sig.ra Carmela Fabiano, Responsabile della gestione documentale e della conservazione del protocollo informatico, provveda alla tempestiva informazione del manuale in favore del personale interessato.

4)

«*Salerno Pulita S.p.A.*»
L'Amministratore Unico
Dott. Vincenzo Bennet