

Manuale di Conservazione dei Documenti Informatici di Salerno Solidale S.p.A.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
<i>Redazione</i>	<i>08/04/2021</i>	Ester Amato	Responsabile Conservazione
<i>Verifica</i>	<i>08/04/2021</i>	Ester Amato	Responsabile Conservazione
<i>Approvazione</i>	<i>08/04/2021</i>	Filomena Arcieri	Amministratore Unico

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Ver 1.0	08/04/2021	Prima emissione	
Ver 2.0	31/08/2022	Seconda emissione	
Ver 3.0	22/06/2026	Terza emissione – Revisione Periodica Aggiornamento normativo a seguito dell'entrata in vigore delle Linee Guida AgID (Det. 407/2020 e 371/2021, in vigore dal 1° gennaio 2022) e del Regolamento sui criteri per la fornitura dei servizi di conservazione (Det. AgID 455/2021): aggiornati i riferimenti al regime dei Conservatori (cap. 1.1), al file IPdA e ai pacchetti (cap. 5), alla normativa sulla firma per il registro di protocollo, allo standard PDF/A (cap. 7-8), designato il Pubblico Ufficiale (cap. 2.7).	

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	<u>INTRODUZIONE.....</u>	4
1.1	SCOPO E AMBITO DEL DOCUMENTO	4
1.2	PRINCIPI DI REDAZIONE	5
1.3	RIMANDI AL MANUALE DELLA CONSERVAZIONE REDATTO DA INFOCERT S.P.A.	5
1.4	RIMANDI AL MANUALE DELLA CONSERVAZIONE REDATTO DA AGENZIA DELLE ENTRATE.....	5
1.5	NORMATIVA DI RIFERIMENTO	5
2	<u>MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE: RUOLI E RESPONSABILITÀ</u>	7
2.1	SISTEMA E ATTORI	7
2.2	PRODUTTORE	7
2.3	CONSERVATORI	8
2.4	UTENTE.....	8
2.5	RESPONSABILE DELLA CONSERVAZIONE	8
2.6	ORGANISMI DI TUTELA E VIGILANZA.....	9
2.7	PUBBLICO UFFICIALE.....	10
3	<u>STRUTTURA ORGANIZZATIVA PER IL SISTEMA DI CONSERVAZIONE</u>	11
3.1	ORGANIGRAMMA.....	11
3.2	STRUTTURE ORGANIZZATIVE	11
3.3	COMPITI DI INFOCERT	11
3.3.1.1	Compiti Organizzativi.....	11
3.3.1.2	Compiti di Manutenzione e Controllo	12
3.3.1.3	Compiti Operativi	12
3.3.1.4	Compiti per la protezione dei dati e delle procedure informatiche.....	12
3.4	COMPITI DI AGENZIA DELLE ENTRATE	13
3.4.1.1	Compiti Organizzativi.....	13
3.4.1.2	Compiti di Manutenzione e Controllo	13
3.4.1.3	Compiti Operativi	14
3.4.1.4	Compiti per la protezione dei dati e delle procedure informatiche.....	14
3.5	PUBBLICO UFFICIALE	14
4	<u>TIPOLOGIE DEI DOCUMENTI POSTI IN CONSERVAZIONE</u>	15
4.1	PREMESSA	15
4.2	FASI DEL PROCESSO DI CONSERVAZIONE E RESPONSABILITÀ	15
4.3	DOCUMENTI INFORMATICI E AGGREGAZIONI DOCUMENTALI INFORMATICHE.....	16
5	<u>PROCESSO DI CONSERVAZIONE</u>	18
5.1	PREMESSA	18
5.2	DEFINIZIONE DEI PACCHETTI	19
5.3	FASI DEL VERSAMENTO E LOGICHE DI CONSERVAZIONE	19
5.4	PRESA IN CARICO DEI PACCHETTI DI VERSAMENTO	19
5.4.1	DESCRIZIONE DEL PROCESSO DI CONSERVAZIONE	20
5.4.1.1	Indice del pacchetto di archiviazione e rapporto di versamento.....	21
5.4.1.2	Il processo di esibizione di un pacchetto di distribuzione	21

5.4.1.3	Esibizione a norma.....	22
5.4.2	PRODUZIONE COPIE E DUPLICATI.....	22
6	<u>DESCRIZIONE DEL SISTEMA DI CONSERVAZIONE.....</u>	22
7	<u>MONITORAGGIO E CONTROLLI - INFOCERT</u>	22
7.1	PROCEDURE DI MONITORAGGIO	23
7.2	FUNZIONALITÀ PER LA VERIFICA E IL MANTENIMENTO DELL'INTEGRITÀ DEGLI ARCHIVI	23
7.3	PIANIFICAZIONE DELLE VERIFICHE PERIODICHE DA EFFETTUARE.....	24
7.4	MANTENIMENTO DELLA FIRMA PER IL PERIODO DI CONSERVAZIONE.....	24
8	<u>MONITORAGGIO E CONTROLLI – AGENZIA DELLE ENTRATE</u>	24
8.1	PROCEDURE DI MONITORAGGIO	24
8.2	FUNZIONALITÀ PER LA VERIFICA E IL MANTENIMENTO DELL'INTEGRITÀ DEGLI ARCHIVI	25
8.3	PIANIFICAZIONE DELLE VERIFICHE PERIODICHE DA EFFETTUARE.....	26
8.4	MANTENIMENTO DELLA FIRMA PER IL PERIODO DI CONSERVAZIONE.....	26
9	<u>NORMATIVE IN VIGORE NEI LUOGHI DOVE SONO CONSERVATI I DOCUMENTI.....</u>	27
10	<u>TRATTAMENTO DEI DATI PERSONALI</u>	27
10.1	TUTELA E DIRITTI DEGLI INTERESSATI.....	27
10.2	MODALITÀ DEL TRATTAMENTO	27
10.3	FINALITÀ DEL TRATTAMENTO.....	27
10.4	SICUREZZA DEI DATI	28
11	<u>DISPOSIZIONI FINALI.....</u>	28
12	<u>DOCUMENTI DI RIFERIMENTO E ALLEGATI.....</u>	28
	ALLEGATO 1 – NORMATIVA E STANDARD DI RIFERIMENTO (VERSIONE 3.0 AGGIORNATA);	28
	ALLEGATO 2 – DISCIPLINARE TECNICO (VERSIONE 3.0 AGGIORNATA);	28
	ALLEGATO 3 – MANUALE DELLA CONSERVAZIONE DI INFOCERT S.P.A. ;.....	28
	ALLEGATO 4 – MANUALE DELLA CONSERVAZIONE DELLE FATTURE ELETTRONICHE DI AGENZIA DELLE ENTRATE ;	28

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 Solidale 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 qualificato ai sensi del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici adottato da AgID con Determinazione n. 455/2021 del 25 giugno 2021 (come modificata dalla Determinazione n. 629/2021), in vigore dal 1° gennaio 2022, che ha sostituito il previgente meccanismo di accreditamento di cui alla Circolare AgID n. 65/2014, abrogata dalla medesima data, ed alla Agenzia delle Entrate, di seguito indicati come Conservatori.

L'accordo tra **Salerno Solidale 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**.

L'accordo tra **Salerno Solidale S.p.A.** e **Agenzia delle Entrate** per l'affidamento in *outsourcing* del processo di conservazione è stato formalizzato da parte dell'**Ente** mediante sottoscrizione del contratto di adesione allo specifico servizio di conservazione delle fatture elettroniche, così come previsto dall'art. 1 del Dlgs 127/2015.

Il presente Manuale integra, per le parti specifiche di competenza del Produttore e per quanto riguarda i rapporti tra questi ed i Conservatori, il Manuale di Conservazione degli stessi, allegati al presente documento.

L'indice rimanda ai capitoli e ai paragrafi del Manuale dello specifico 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 sia da **InfoCert S.p.a.** sia da **Agenzia delle Entrate**.

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 Rimandi al Manuale della Conservazione redatto da Agenzia delle Entrate

Si rimanda al Manuale della Conservazione di **Agenzia delle Entrate** per i seguenti argomenti:

- *Glossario e termini di riferimento*
- *Ruoli e Responsabilità interne ad **Agenzia delle Entrate** 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.*

1.5 Normativa di riferimento

Vedi documento Allegato 1.

L'Allegato 1 è stato aggiornato (versione 3.0) per recepire l'evoluzione normativa intervenuta dal 2020 ad oggi, incluse le Linee Guida AgID sulla formazione, gestione e conservazione dei



documenti informatici (Det. 407/2020 e 371/2021, in vigore dal 1° gennaio 2022) e il Regolamento sui criteri per la fornitura dei servizi di conservazione (Det. AgID 455/2021).

2 MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE: RUOLI E RESPONSABILITÀ

2.1 Sistema e Attori

Si rimanda al “Manuale del Sistema di conservazione” di InfoCert e di Agenzia delle Entrate per i ruoli:

- **Responsabile del servizio di conservazione di Infocert S.p.A.**
- **Responsabile del servizio di conservazione di Agenzia delle Entrate**
- **Responsabile Sicurezza dei sistemi per la conservazione di Infocert S.p.A.**
- **Responsabile Sicurezza dei sistemi per la conservazione di Agenzia delle Entrate**
- **Responsabile funzione archivistica di conservazione Infocert S.p.A.**
- **Responsabile esterno del trattamento dei dati personali di Infocert S.p.A.**
- **Responsabile sistemi informativi per la conservazione di Infocert S.p.A.**
- **Responsabile sviluppo e manutenzione del sistema di conservazione di Infocert S.p.A.**

Per quanto riguarda il soggetto Produttore:

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Titolare del trattamento dei dati personali	Salerno Solidale S.p.A.		Dalla data del provvedimento d'individuazione del titolare
Responsabile della conservazione del Produttore	Sig.ra Ester Amato	Definizione delle policies di conservazione	A decorrere dalla data del provvedimento di nomina
Responsabile della gestione documentale del Produttore	Sig.ra Ester Amato	Definizione delle policies di organizzazione documentale	A decorrere dalla data del provvedimento di nomina

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 Solidale S.p.A.
Sede Amministrativa	Via Guido Vestuti – 84133 Salerno (SA)
Recapiti	+39 089751438
Sito web	www.salernosolidale.it
PEC	presidenza@pec.salernosolidale.it
Partita IVA	03309030652

2.3 Conservatori

Ai fini dell'esecuzione del Servizio di conservazione dei documenti informatici del Produttore, la società InfoCert S.p.A. e l'Agenzia delle Entrate sono identificate quali fornitori del Servizio di conservazione, qualificati ai sensi del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici (Determinazione AgID n. 455/2021), in vigore dal 1° gennaio 2022.

Per ulteriori informazioni si rimanda al "Manuale del Sistema di Conservazione" di **InfoCert S.p.A. e di Agenzia delle Entrate in allegato.**

2.4 Utente

In base alla definizione del glossario allegato alle vigenti **Linee Guida** 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* e tra **Agenzia delle Entrate** ed il *Produttore*.

Si identificano gli utenti del Sistema di conservazione nelle seguenti persone:

- [Sig.ra Ester Amato](#), responsabile della conservazione del Produttore.

Nel seguito del documento detto utente è referenziato nel ruolo "**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 dalla vigente normativa in materia di protezione dei dati personali.

2.5 Responsabile della conservazione

Il ruolo di responsabile della conservazione del *Produttore* è in capo alla sig.ra **Ester Amato**.

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**, ed in **Agenzia delle Entrate**.

Gli obiettivi sia di **InfoCert S.p.A.** sia di **Agenzia delle Entrate**, ciascuna per le specifiche competenze e per gli specifici ambiti di intervento, 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 sia **InfoCert S.p.A.** sia **Agenzia delle Entrate** si impegnano alla *conservazione* dei documenti trasferiti e ne assumono 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 svolgendo, tramite la propria struttura organizzativa e di responsabilità, l'insieme delle attività elencate nel Capitolo 4 delle vigenti **Linee Guida**.

In particolare si faccia riferimento a quanto riportato:

- **Cap. 4 "Manuale del Sistema di Conservazione" di InfoCert.**
- **Cap. 4 "Manuale del Sistema di Conservazione" di Agenzia delle Entrate.**

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 Linee Guida i sistemi di conservazione delle pubbliche amministrazioni ed i sistemi di conservazione dei conservatori sono soggetti alla vigilanza dell'AGID, e per tale fine sia il Sistema di conservazione di InfoCert S.p.A. sia il Sistema di conservazione di Agenzia delle Entrate prevedono la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede del Produttore.

2.7 Pubblico Ufficiale

Nei casi previsti dalla normativa, il ruolo di pubblico ufficiale è svolto dal Responsabile della Conservazione in qualità di soggetto responsabile della conservazione dei documenti, individuato nella sig.ra Ester Amato, già designata quale Responsabile della Conservazione del Produttore (cfr. par. 2.5), 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.

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 dal ruolo "Responsabile della conservazione" del sistema di gestione documentale, all'interno del quale 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 26.01.2021**.

Il servizio di conservazione delle fatture elettroniche del *Produttore* è attivato sulla base dell'accordo stipulato con **Agenzia delle Entrate** mediante sottoscrizione del contratto di adesione al servizio di conservazione previsto dall'art. 1 del Dlgs 127/2015 **in data 08.01.2019**.

Il *Produttore* invia i pacchetti di versamento al sistema di conservazione utilizzando il ruolo '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 Compiti di Agenzia delle Entrate

3.4.1.1 Compiti Organizzativi

Agenzia delle Entrate 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 di Adesione al Servizio di Conservazione delle Fatture Elettroniche** ed attuati adottando procedure di tracciabilità tali da garantire la corretta conservazione, l'accessibilità a ogni singolo documento e la sua esibizione.

Agenzia delle Entrate 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.*

3.4.1.2 Compiti di Manutenzione e Controllo

Agenzia delle Entrate 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.*

3.4.1.3 Compiti Operativi

Agenzia delle Entrate 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;*

3.4.1.4 Compiti per la protezione dei dati e delle procedure informatiche

Agenzia delle Entrate 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.

3.5 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;**
- **Fatture Elettroniche in formato FatturaPA.**

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 **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** e all'**Agenzia delle Entrate**, che espleteranno le attività per le quali hanno ricevuto formale delega, nei limiti della stessa e per le quali operano in modo autonomo e ne sono responsabili.

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 abbiano evidenziato delle anomalie		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 o di Agenzia delle Entrate 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*.

Il *Sistema di conservazione* gestito da Agenzia delle Entrate (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 Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici (Determinazione n. 407/2020, modificata dalla Determinazione n. 371/2021, in vigore dal 1° gennaio 2022);**
- **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 alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, Determinazione n. 407/2020 e successiva Determinazione n. 371/2021, in vigore dal 1° gennaio 2022 – riferimento già aggiornato rispetto al previgente Allegato 5 del DPCM 3 dicembre 2013, abrogato dalla medesima data), 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 delle vigenti Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici (Determinazione n. 407/2020 e 371/2021) – già corrispondente, per continuità di struttura tecnica, a quanto previsto dal previgente Allegato 4 del DPCM 3 dicembre 2013, abrogato dal 1° gennaio 2022.

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 – successivamente confluiti, per la parte relativa alla formazione e conservazione, nelle vigenti Linee Guida AgID (Determinazione n. 407/2020 e 371/2021), in vigore dal 1° gennaio 2022, fermo restando il Decreto MEF 17 giugno 2014 per la parte relativa agli obblighi fiscali –, 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 immutabilità 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 .

Per il formato delle Fatture Elettroniche conservabili nel sistema di conservazione si rinvia al “Manuale del Sistema di conservazione” di Agenzia delle Entrate.

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.

Relativamente alla funzioni di:

- a) Invio al sistema di conservazione del pacchetto di versamento delle fatture elettroniche**
- b) Validazione del pacchetto di versamento delle fatture elettroniche**
- c) Descrizione del rapporto di versamento delle fatture elettroniche**

si rimanda al “Manuale del Sistema di conservazione” di Agenzia delle Entrate.

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, disposizione confluita, dal 1° gennaio 2022, nella corrispondente previsione delle vigenti Linee Guida AgID (Determinazione n. 407/2020 e 371/2021).

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 e di Agenzia delle Entrate.**

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 (disposizione confluita, dal 1° gennaio 2022, nella corrispondente previsione delle vigenti Linee Guida AgID, Determinazione n. 407/2020 e 371/2021) 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 e di Agenzia delle Entrate 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 e di Agenzia delle Entrate.

6 DESCRIZIONE DEL SISTEMA DI CONSERVAZIONE

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

Riferimento Cap. 8 "Manuale del Sistema di Conservazione" di Agenzia delle Entrate.

7 MONITORAGGIO E CONTROLLI - INFOCERT

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***

7.1 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 tracciate 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.

7.2 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). Si segnala che lo standard PDF/A comprende, oltre al livello base ISO 19005-1:2005 (PDF/A-1) qui richiamato, anche i livelli successivi ISO 19005-2:2011 (PDF/A-2) e ISO 19005-3:2012 (PDF/A-3), quest'ultimo idoneo all'incorporamento di allegati; il livello effettivamente generato dal sistema di conservazione di InfoCert è specificato nel relativo Manuale del Sistema di Conservazione.

7.3 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.

7.4 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.

8 MONITORAGGIO E CONTROLLI – AGENZIA DELLE ENTRATE

Le funzionalità di controllo del buon funzionamento del sistema di conservazione adottate da Agenzia delle Entrate 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

Agenzia delle Entrate 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 tracciatore 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

Agenzia delle Entrate 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). Si segnala che lo standard PDF/A comprende, oltre al livello base ISO 19005-1:2005 (PDF/A-1) qui richiamato, anche i livelli successivi ISO 19005-2:2011 (PDF/A-2) e ISO 19005-3:2012 (PDF/A-3), quest'ultimo idoneo all'incorporamento di

allegati; il livello effettivamente generato dal sistema di conservazione di Agenzia delle Entrate è specificato nel relativo Manuale del Sistema di Conservazione.

8.3 Pianificazione delle verifiche periodiche da effettuare

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

8.4 Mantenimento della firma per il periodo di conservazione

Il sistema di conservazione di Agenzia delle Entrate 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 sia al sistema di conservazione di **InfoCert** sia al sistema di conservazione di **Agenzia delle Entrate** 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 sia InfoCert sia Agenzia delle Entrate garantiscono la tutela degli interessati in ottemperanza a quanto disposto del D.Lgs. 196/2003 così come rinnovato dal D.Lgs. 101/2018 e dalle successive modifiche intervenute (tra cui il D.L. 139/2021, conv. L. 205/2021, e il D.Lgs. 104/2022) 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 e nel “Manuale del Sistema di Conservazione” di Agenzia delle Entrate e nel Contratto di adesione al servizio di conservazione delle fatture elettroniche, 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 sia del *Contratto LegalDoc* sia del *Contratto per il servizio di conservazione delle fatture Elettroniche* e per l'attivazione del Servizio di conservazione digitale dei documenti informatici. Sia InfoCert sia Agenzia delle Entrate utilizzeranno i dati raccolti per lo svolgimento dell'attività connesse e/o derivante dal Servizio di conservazione 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 e ad Agenzia delle Entrate 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, sia InfoCert sia Agenzia delle Entrate adottano 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 e da Agenzia delle Entrate 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 nei manuali di conservazione di InfoCert e di Agenzia delle Entrate.

12 DOCUMENTI DI RIFERIMENTO E ALLEGATI

Allegato 1 – Normativa e Standard di Riferimento (Versione 3.0 aggiornata);

Allegato 2 – Disciplinare Tecnico (Versione 3.0 aggiornata);

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

Allegato 4 – Manuale della Conservazione delle Fatture Elettroniche di Agenzia delle Entrate ;

Manuale di Conservazione dei Documenti Informatici di

Salerno Solidale S.p.A.

Allegato 1 Normativa e Standard di Riferimento

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
<i>Redazione</i>	<i>08/04/2021</i>	Ester Amato	Responsabile Conservazione
<i>Verifica</i>	<i>08/04/2021</i>	Ester Amato	Responsabile Conservazione
<i>Approvazione</i>	<i>08/04/2021</i>	Filomena Arcieri	Amministratore Unico

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Ver 1.0	08/04/2021	Prima emissione	
Ver 2.0	31/08/2022	Seconda emissione	
Ver.3.0	22/06/2026	Terza 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

1	Introduzione	3
2	Normativa.....	4
2.1	Normativa europea	4
2.2	Normativa nazionale italiana	4
2.3	Linee Guida e Regolamenti AgID (2020-2026)	6
3	Standard di riferimento	7
4	Documentazione di riferimento ai fini della Gestione della Sicurezza delle Informazioni	9
4.1	Standard	9
4.2	Agenzia per la Cybersicurezza Nazionale (ACN) – Normativa e Linee Guida.....	9
4.3	Provvedimenti e Linee Guida Garante Privacy.....	10
4.4	Normativa Specifica per la conservazione delle fatture elettroniche.....	11
4.5	Altre linee guida e raccomandazioni.....	13
5	Siti Istituzionali di Riferimento per il monitoraggio normativo	14

1 Introduzione

Il presente allegato riporta la principale normativa di riferimento per l'attività di conservazione in vigore nei luoghi dove sono conservati i documenti.

Pertanto, viene riportata la normativa europea e nazionale italiana, in particolare in relazione alla gestione della sicurezza delle informazioni del sistema di conservazione.

Sono riportati inoltre gli standard a cui l'attività di conservazione si riferisce e che sono in qualche modo richiamati nel Manuale di Conservazione.

Per la normativa e gli standard di riferimento dopo l'entrata in vigore delle **Linee Guida sulla formazione, gestione e conservazione dei documenti informatici** adottate da AgID con Determinazione del Direttore Generale n. 407/2020 del 9 settembre 2020 si fa riferimento anche alla normativa citata al paragrafo 1.5 delle citate **Linee Guida** e agli standard indicati nell'Allegato 4 delle citate **Linee Guida**, in particolare quelli indicati ai punti 2.2, 2.3, 2.4 rispettivamente per la conservazione digitale, per l'affidabilità.

Anche per gli standard sono specificamente individuati quelli relativi in particolare alla sicurezza delle informazioni e del sistema di conservazione.

Sulla sicurezza delle informazioni vengono riportati alcuni riferimenti di linee guida e provvedimenti del Garante Privacy e altre linee guida e raccomandazioni da siti di riferimento, in particolare dell'ENISA di AGID e di CERT-PA.

Viene periodicamente aggiornato in base agli eventuali aggiornamenti della normativa e degli standard di riferimento.

2 Normativa

2.1 Normativa europea

- **Regolamento (UE) n. 910/2014 del 23 luglio 2014 (eIDAS) – modificato dal Regolamento (UE) 2024/1183**
Regolamento del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS – electronic IDentification, Authentication and trust Services). Il regolamento originario è stato significativamente modificato dal Regolamento (UE) 2024/1183 dell'11 aprile 2024 (c.d. eIDAS 2), entrato in vigore il 20 maggio 2024, che ha istituito il quadro europeo per un'identità digitale e introdotto il Portafoglio Europeo di Identità Digitale (EUDI Wallet), nonché nuovi servizi fiduciari e requisiti aggiornati per i fornitori di servizi fiduciari qualificati (QTSP). La piena operatività delle nuove disposizioni è prevista entro settembre 2026.
- **Regolamento (UE) 2024/1183 dell'11 aprile 2024 (eIDAS 2) – in vigore dal 20 maggio 2024**
Regolamento del Parlamento europeo e del Consiglio che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro relativo a un'identità digitale europea. Introduce il Portafoglio Europeo di Identità Digitale (EUDI Wallet), nuovi servizi fiduciari qualificati (attestati elettronici degli attributi, archivio elettronico qualificato, gestione dispositivi per la creazione di firme/sigilli a distanza) e requisiti di sicurezza armonizzati, inclusi per i servizi fiduciari non qualificati (FEA). Essendo regolamento UE, si applica direttamente senza necessità di recepimento da parte degli Stati membri.
- **Regolamento (UE) n. 679/2016 del 27 aprile 2016 (GDPR)**
Regolamento del Parlamento europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Tuttora vigente e pienamente applicabile.
- **Regolamento (UE) 2022/2554 del 14 dicembre 2022 (DORA – Digital Operational Resilience Act) – applicabile dal 17 gennaio 2025**
Regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario. Rilevante per soggetti che operano in contesti finanziari e per i fornitori di servizi ICT critici, inclusi i conservatori che operano con enti del settore finanziario.

2.2 Normativa nazionale italiana

- **Codice Civile – art. 2215-bis (Documentazione informatica)**
Libro V, Titolo II, Capo III, Sez. III – Disposizioni particolari per le imprese commerciali, § 2 Delle scritture contabili. Tuttora vigente.
- **Legge 7 agosto 1990, n. 241 e s.m.i.**
Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.**
Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- **Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. (Codice Privacy)**

Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. 10 agosto 2018, n. 101 (adeguamento al GDPR), dal D.L. 8 ottobre 2021, n. 139 convertito con L. 3 dicembre 2021, n. 205, e dal D.Lgs. 27 giugno 2022, n. 104 (modifiche relative alla NIS). Testo consolidato aggiornato disponibile sul sito del Garante per la protezione dei dati personali.

➤ **Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio**

Rilevante per le autorizzazioni della Soprintendenza Archivistica in caso di affidamento in outsourcing dell'archivio (art. 21).

➤ **Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i. – Codice dell'Amministrazione Digitale (CAD)**

Codice dell'amministrazione digitale, già modificato dal D.Lgs. 179/2016 e D.Lgs. 217/2017. Ulteriori modifiche rilevanti per la conservazione sono state apportate dal: D.L. 16 luglio 2020, n. 76 (Decreto Semplificazioni) convertito con L. 11 settembre 2020, n. 120 – ha introdotto il nuovo art. 34, comma 1-bis, che disciplina il servizio di conservazione in outsourcing e il relativo regolamento AgID sui criteri di fornitura, sostituendo il precedente meccanismo di accreditamento ex Circolare AgID n. 65/2014; D.L. 30 aprile 2022, n. 36 (Decreto PNRR 2) convertito con L. 29 giugno 2022, n. 79 – modifiche a numerosi articoli del CAD; D.L. 2 marzo 2024, n. 19 (Decreto PNRR 4) convertito con L. 29 aprile 2024, n. 56 – ulteriori aggiornamenti al quadro digitale. Il testo consolidato più aggiornato del CAD (aggiornato alla L. 19 gennaio 2026, n. 11 e al D.L. 19 febbraio 2026, n. 19) è disponibile su Altalex e sul sito AgID.

➤ **Decreto Legislativo 4 settembre 2024, n. 138 – Recepimento Direttiva NIS 2 (Direttiva UE 2022/2555)**

Decreto di recepimento della Direttiva (UE) 2022/2555 (NIS 2) relativa a misure per un livello comune elevato di cybersicurezza nell'Unione. Introduce obblighi di sicurezza delle reti e dei sistemi informativi per soggetti essenziali e importanti, inclusi potenzialmente i conservatori. In vigore dal 16 ottobre 2024.

➤ **DPCM 3 dicembre 2013 – Regole tecniche in materia di sistema di conservazione [ABROGATO]**

Abrogato a decorrere dal 1° gennaio 2022 per effetto dell'entrata in vigore delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici (Determinazione n. 407/2020, come modificata dalla Determinazione n. 371/2021). Mantenuto come riferimento storico per la comprensione della struttura preesistente.

➤ **DPCM 13 novembre 2014 – Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici [ABROGATO]**

Abrogato a decorrere dal 1° gennaio 2022 per effetto dell'entrata in vigore delle Linee Guida AgID (Determinazione n. 407/2020). Mantenuto come riferimento storico.

➤ **DPCM 22 febbraio 2013 – Regole tecniche in materia di firme elettroniche avanzate, qualificate e digitali [PARZIALMENTE SUPERATO]**

Le disposizioni di questo DPCM relative alla firma elettronica avanzata (FEA) sono state in larga misura superate dall'applicazione diretta del Regolamento eIDAS (UE 910/2014) e ulteriormente ridefinite da eIDAS 2 (UE 2024/1183). Rimane un riferimento tecnico per alcune specificità nazionali.

➤ **Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici**

Ancora vigente per la parte relativa agli obblighi fiscali (art. 21, comma 5, D.Lgs. 82/2005). Da leggere in combinato con la normativa sulle fatture elettroniche.

2.3 Linee Guida e Regolamenti AgID (2020-2026)

- **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;
- **Linee Guida sulla formazione, gestione e conservazione dei documenti informatici – AgID, Determinazione n. 407/2020 del 9 settembre 2020, modificata dalla Determinazione n. 371/2021 del 17 maggio 2021 – in vigore dal 1° gennaio 2022**

Costituiscono il principale riferimento normativo tecnico in materia di conservazione dei documenti informatici, sostituendo i DPCM del 2013 e 2014. In vigore dal 1° gennaio 2022 (proroga da giugno 2021). Composte dal testo principale e da 6 allegati: All. 1 – Glossario dei termini e degli acronimi; All. 2 – Formati di file e riversamento; All. 3 – Manuale di gestione documentale; All. 4 – Standard e specifiche tecniche; All. 5 – Metadati (versione aggiornata maggio 2021); All. 6 – Comunicazione tra AOO di documenti amministrativi protocollati (versione aggiornata maggio 2021). Disponibili su: <https://www.agid.gov.it/it/linee-guida>
- **Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici – AgID, Determinazione n. 455/2021 del 25 giugno 2021, modificata dalla Determinazione n. 629/2021 del 17 dicembre 2021 – in vigore dal 1° gennaio 2022**

Adottato ai sensi dell'art. 34, comma 1-bis, lett. b) del CAD (come modificato dal D.L. 76/2020). Definisce i criteri per la fornitura del servizio di conservazione in outsourcing per le PA, sostituendo il meccanismo di accreditamento ex Circolare AgID n. 65/2014. Fissa i requisiti generali, di qualità, di sicurezza e organizzativi per i conservatori (Allegato A) e le indicazioni per il piano di cessazione del servizio (Allegato B). Contestualmente è attivo il marketplace AgID per la qualificazione dei conservatori. Disponibile su: <https://www.agid.gov.it/it/piattaforme/conservazione>
- **Vademecum per l'implementazione delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici – AgID, 2022**

Documento di supporto operativo per l'implementazione pratica delle Linee Guida da parte delle pubbliche amministrazioni. Non ha valore normativo vincolante ma fornisce indicazioni applicative utili. Disponibile su: <https://www.agid.gov.it/it/linee-guida>
- **Circolare AgID n. 2 del 18 aprile 2017 – Misure minime di sicurezza ICT per le pubbliche amministrazioni**

Già citata nella versione precedente; confermata. Sostituisce la Circolare n. 1/2017. GU n. 103 del 05-05-2017.

3 Standard di riferimento

- **ICA – ISAD(G): General International Standard Archival Description, Second Edition (1999)**
Standard dell'ICA (International Council on Archives) per l'elaborazione di descrizioni archivistiche. Tuttora valido.
- **ISO 9001:2015 – Quality management systems – Requirements**
Definisce i requisiti di un sistema di gestione per la qualità.
- **ISO 14721:2012 – Open Archival Information System (OAIS) – Reference model**
Definisce concetti, modelli e funzionalità per la conservazione permanente o a lungo termine di informazioni digitali (CCSDS 650.0-M-2). È allo studio la nuova versione; verificare eventuali aggiornamenti.
- **ISO 16363:2012 – Audit and certification of trustworthy digital repositories**
CCSDS 652.0-M-1. Tuttora valido come riferimento per la certificazione dei repository digitali affidabili.
- **ISO 15836:2009 – Dublin Core metadata element set**
Sistema di metadati del Dublin Core. Verificare disponibilità di aggiornamenti.
- **ISO 23081-1:2006 e ISO/TS 23081-2:2007 / ISO 23081-2:2009 – Records management metadata**
Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale.
- **UNI 11386:2020 (SInCRO) – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali**
La versione 2020 sostituisce la precedente UNI 11386:2010. Definisce lo Schema XML per la struttura dell'indice di conservazione (IPdA/SIP). Il riferimento aggiornato è UNI 11386:2020. Le Linee Guida AgID 2022 rinviano a questo standard aggiornato.
- **UNI ISO 15489-1:2006 e UNI ISO 15489-2:2007 – Informazione e documentazione – Gestione dei documenti di archivio**
Principi generali e linee guida sul record management. Verificare eventuale emissione di versioni aggiornate.
- **LTO6 (Linear Tape Open)**
Standard open per lo storage su nastro. Versione 6 definita alla fine del 2012. Verificare versioni più recenti (LTO-8, LTO-9, LTO-10) per aggiornamento della politica di storage.
- **SQL – Structured Query Language**
Linguaggio standardizzato per database relazionali (RDBMS).
- **UNI ISO 30300:2023 – Information and documentation – Records management – Core concepts and vocabulary**
Versione aggiornata dello standard ISO per il records management (sostituisce la versione 2011). Fornisce il vocabolario e i concetti fondamentali per la gestione documentale.
- **UNI ISO 30301:2019 – Information and documentation – Records management systems – Requirements**

Versione aggiornata (sostituisce la 2011). Requisiti per i sistemi di gestione documentale.

➤ **Modello di interoperabilità tra sistemi di conservazione – AgID, 2022**

Documento tecnico AgID per l'interoperabilità tra sistemi di conservazione digitale, pubblicato nel 2022 come complemento alle Linee Guida. Disponibile su: <https://www.agid.gov.it/it/piattaforme/conservazione>

4 Documentazione di riferimento ai fini della Gestione della Sicurezza delle Informazioni

4.1 Standard

- **ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements**
Versione 2022 (aggiornata rispetto alla precedente 2013). Definisce i requisiti per un ISMS. La versione 2022 ha introdotto una struttura aggiornata e nuovi controlli. I conservatori accreditati AgID devono allinearsi alla versione vigente.
- **ISO/IEC 27017:2015 – Code of practice for information security controls for cloud services**
Codice di condotta per i controlli di sicurezza delle informazioni per i servizi in cloud.
- **ISO/IEC 27018:2019 – Protection of personally identifiable information (PII) in public clouds**
Versione 2019 (sostituisce la 2014). Codice di condotta per la protezione delle PII in cloud pubblici.
- **ISO 22301:2019 – Business continuity management systems – Requirements**
Versione 2019 (sostituisce la 2012). Requisiti per i sistemi di gestione della business continuity.
- **ETSI TS 101 533-1 v1.3.1 (2012-04) e ETSI TR 101 533-2 v1.3.1 (2012-04)**
Standard ETSI per la sicurezza dei sistemi di preservazione delle informazioni (Data/Information Preservation Systems Security). Verificare eventuali aggiornamenti ETSI.
- **SAML – Security Assertion Markup Language**
Standard per lo scambio di dati di autenticazione e autorizzazione. Tuttora valido.
- **NIST SP 800-53 Rev. 5 (2020) – Security and Privacy Controls for Information Systems and Organizations**
Aggiornamento del framework NIST per i controlli di sicurezza e privacy. Riferimento internazionale complementare agli standard ISO/IEC.
- **Framework Nazionale per la Cybersecurity e la Data Protection – CINI, versione 2.0 (2019) / aggiornamenti ACN**
Framework italiano per la cybersecurity, sviluppato dal CINI (Consorzio Interuniversitario Nazionale per l'Informatica) su mandato del DPCM 17 febbraio 2017. Recepisce il NIST CSF. Aggiornamenti successivi sono gestiti dall'Agenzia per la Cybersicurezza Nazionale (ACN), istituita con D.L. 82/2021 convertito con L. 109/2021.

4.2 Agenzia per la Cybersicurezza Nazionale (ACN) – Normativa e Linee Guida

- **Decreto Legislativo 1° agosto 2003, n. 259 e s.m.i. (Codice delle Comunicazioni Elettroniche) – modificato da D.Lgs. 8 novembre 2021, n. 207**
Recepimento della Direttiva UE 2018/1972. Rilevante per i servizi di comunicazione elettronica.

- **Decreto Legge 14 giugno 2021, n. 82 convertito con L. 4 agosto 2021, n. 109 – Istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN)**
Istituisce l'ACN quale autorità nazionale in materia di cybersicurezza. L'ACN ha assunto le funzioni di vigilanza AgID in materia di sicurezza informatica e pubblica linee guida, misure minime e raccomandazioni di sicurezza. Disponibili su: <https://www.acn.gov.it>
- **Misure minime di sicurezza ICT per le Pubbliche Amministrazioni – ACN (aggiornamento 2022)**
L'ACN ha aggiornato le misure minime di sicurezza ICT per le PA già previste dalla Circolare AgID n. 2/2017. Verificare le versioni più recenti pubblicate su: <https://www.acn.gov.it/portale/misure-minime-di-sicurezza-ict-pa>
- **Decreto Legislativo 4 settembre 2024, n. 138 – Recepimento NIS 2 (Direttiva UE 2022/2555)**
Come già indicato nella sezione normativa nazionale. I soggetti essenziali e importanti (inclusi potenzialmente i conservatori in outsourcing per settori critici) devono adottare misure adeguate di gestione del rischio cyber e notificare gli incidenti significativi all'ACN.

4.3 Provvedimenti e Linee Guida Garante Privacy

- **Diritto di accesso - Informazioni personali conservate con tecniche di cifratura - 21 novembre 2001 [39773]**
- **Trattamento dei dati sensibili nella pubblica amministrazione - 30 giugno 2005 [1144445]** (*G.U. n. 170 del 23 luglio 2005*)
- **Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali - 19 aprile 2007, G.U. n. 120 del 25 maggio 2007**
- **"Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" - 14 giugno 2007** (*G.U. 13 luglio 2007, n. 161*)
- **Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema** Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (*G.U. n. 300 del 24 dicembre 2008*) (*così modificato in base al provvedimento del [25 giugno 2009](#)*) (*G.U. n. 149 del 30 giugno 2009*) [*doc. web n. 157749*]
- **Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario e prescrizioni in tema di Fascicolo sanitario elettronico (Fse) - 16 luglio 2009 [1634116]** (*G.U. n. 178 del 3 agosto 2009*)
- **Linee guida in tema di referti on-line - 19 novembre 2009 [1679033], *G.U. n. 288 del 11 dicembre 2009***
- **Dematerializzazione della documentazione clinica -26 novembre 2009** [*doc. web n. 1688961*]
- **Protocollo informatico e protezione dei dati personali dei lavoratori - 11 ottobre 2012,**
- **Registro dei provvedimenti n. 280 dell'11 ottobre del 2012** [*doc. web n. 2097560**]
- **Dossier sanitario e trattamento dei dati personali dei pazienti - 10 gennaio 2013 [2284708], Registro dei provvedimenti n. 3 del 10 gennaio 2013**
- **Trattamento di dati personali sensibili di un dipendente attraverso il**

- protocollo informatico aziendale - 12 giugno 2014 [3318492]** Registro dei provvedimenti n. 298 del 12 giugno 2014,
- **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** (*Pubblicato sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014*)
 - **Linee guida in materia di Dossier sanitario** 4 giugno 2015 [doc. web n. 4084632]
 - **Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015 [4129029],** *Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015*
 - **Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018**
 - **(Pubblicato sulla Gazzetta Ufficiale n. 12 del 15 gennaio 2019)**
 - **Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951]** Registro dei provvedimenti n. 157 del 30 luglio 2019,
 - **Parere del Garante su istanza di accesso civico- 18 dicembre 2019 [9232553] in tema di abusi edilizi** Registro dei provvedimenti n. 220 del 18 dicembre 2019,
 - **Provvedimento del Garante del 9 giugno 2022 – Linee guida cookie e altri strumenti di tracciamento**
Rilevante per i sistemi informativi accessibili via web. Pubblicato su: <https://www.garanteprivacy.it>
 - **Provvedimento del Garante del 23 novembre 2023 n. 533 – Linee guida sull'intelligenza artificiale**
Rilevante per sistemi di conservazione che integrano componenti AI. Il Garante ha avviato una serie di provvedimenti e consultazioni in materia di AI e trattamento dati personali.
 - **Regolamento (UE) 2024/1689 del 13 giugno 2024 – AI Act (Regolamento sull'intelligenza artificiale)**
Regolamento europeo sull'intelligenza artificiale, in vigore dal 1° agosto 2024 con applicazione graduale fino al 2027. Rilevante per i sistemi di conservazione/gestione documentale che integrano componenti di AI classificabili come ad alto rischio o sistemi di IA vietati.

4.4 Normativa Specifica per la conservazione delle fatture elettroniche

- **Decreto Legislativo 5 agosto 2015, n. 127 – Trasmissione telematica delle operazioni IVA e di liquidazioni periodiche**
Art. 1, comma 1: l'Agenzia delle Entrate mette a disposizione gratuitamente il servizio di conservazione delle fatture elettroniche. Tuttora vigente.
- **Decreto Legislativo 5 novembre 2021, n. 173 – Recepimento Direttiva UE 2020/285 (franchigia IVA) e Direttiva UE 2016/1065 (buoni-corrispettivo) – modifiche al DPR 633/72**
Modifica alcune disposizioni del DPR IVA rilevanti per la fatturazione elettronica.
- **Decreto Legge 21 giugno 2022, n. 73 (Decreto Semplificazioni fiscali) convertito con L. 4 agosto 2022, n. 122 – Obbligo di fatturazione elettronica esteso ai forfettari**

Ha esteso progressivamente l'obbligo di fatturazione elettronica a tutte le categorie di contribuenti, anche forfettari, con decorrenza 1° luglio 2022 (forfettari sopra soglia) e 1° gennaio 2024 (tutti i forfettari). Rilevante per la copertura totale della conservazione FatturePA.

➤ **Circolare Agenzia delle Entrate n. 26/E del 13 luglio 2022 – Fatturazione elettronica obbligatoria per tutti i contribuenti**

Chiarimenti interpretativi sull'estensione dell'obbligo di fatturazione elettronica.

4.5 Altre linee guida e raccomandazioni

- **DRAMBORA (Digital Repository Audit Method Based on Risk Assessment)**, Digital Curation Centre (DCC) and Digital Preservation Europe (DPE), versione 1.0 28 febbraio 2007
(<http://www.dcc.ac.uk/resources/repository-audit-and-assessment/drambora>)
- **Misure minime di sicurezza ICT per le pubbliche amministrazioni** (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015), AGID 26 aprile 2016
(<https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict>)
- **2016 Italian Cybersecurity Report Controlli Essenziali di Cybersecurity**, CIS Sapienza, versione 1.0 Marzo 2017 (<http://www.cybersecurityframework.it/>)
- **Linee guida di sicurezza nello sviluppo delle applicazioni**, AGID , 21 novembre 2017, con aggiornamento del maggio 2020 con la pubblicazione di 4 allegati tecnici per lo sviluppo del software sicuro (<https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro>)
- **Conformity assessment of Trust Service Providers - Technical guidelines on trust services; Guidelines on Supervision of Qualified Trust Services - Technical guidelines on trust services; Guidelines on Initiation of Qualified Trust Services - Technical guidelines on trust services Security framework for Trust Service Providers - Technical guidelines on trust services; ENISA, 19 dicembre 2017**
(<https://www.enisa.europa.eu/publications/>)
- **Improving recognition of ICT security standards**, ENISA, 1 febbraio 2018 (<https://www.enisa.europa.eu/publications/>)
- **Annual Report Trust Services Security Incidents 2017**, ENISA, 8 ottobre 2018 (<https://www.enisa.europa.eu/publications/>)
- **Annual Report Trust Services Security Incidents 2018**, ENISA, 15 luglio 2019 (<https://www.enisa.europa.eu/news/enisa-news/annual-report-trust-services-security-incidents-2018> - <https://www.enisa.europa.eu/publications/>)
- **Annual Report Trust Services Security Incidents 2019**, ENISA, 10 luglio 2020 (<https://www.enisa.europa.eu/news/enisa-news/annual-report-on-trust-services-security-incidents-in-2019> - <https://www.enisa.europa.eu/publications/>)

5 Siti Istituzionali di Riferimento per il monitoraggio normativo

- *AgID – Linee Guida e Regolamenti: <https://www.agid.gov.it/it/linee-guida>*
- *AgID – Piattaforma Conservazione: <https://www.agid.gov.it/it/piattaforme/conservazione>*
- *ACN – Agenzia per la Cybersicurezza Nazionale: <https://www.acn.gov.it>*
- *Garante Privacy: <https://www.garanteprivacy.it>*
- *EUR-Lex (normativa UE): <https://eur-lex.europa.eu>*
- *Normattiva (normativa nazionale): <https://www.normattiva.it>*

Manuale di Conservazione dei Documenti Informatici di Salerno Solidale S.p.A.

Allegato 2 Disciplinare Tecnico

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
<i>Redazione</i>	<i>08/04/2021</i>	Ester Amato	Responsabile Conservazione
<i>Verifica</i>	<i>08/04/2021</i>	Ester Amato	Responsabile Conservazione
<i>Approvazione</i>	<i>08/04/2021</i>	Filomena Arcieri	Amministratore Unico

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Ver 1.0	08/04/2021	Prima emissione	
Ver 2.0	31/08/2022	Aggiornamento normativo a seguito dell'entrata in vigore delle Linee Guida AgID (Det. 407/2020 e 371/2021) e del Regolamento conservatori (Det. 455/2021): aggiornati i riferimenti al Registro di Protocollo (cap. 4.1), ai rapporti con i Conservatori (cap. 1), allo standard PDF/A (cap. 2.2), ai metadati (cap. 5.4-5.6), allo standard UNI 11386:2020 (cap. 3) e verifica decorrenza FatturePA (cap. 4.3).	
Ver 3.0	22/06/2026	Revisione Periodica	

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.....	3
2	Formati Gestiti.....	4
2.1	Caratteristiche generali dei formati	4
2.2	Formati per la Conservazione	5
3	La tipologia dei pacchetti informativi gestiti.....	6
3.1	Specifiche del Pacchetto di Versamento	6
3.2	Specifiche del Rapporto di Versamento	7
4	Tipologie dei documenti posti in conservazione.....	8
4.1	Conservazione del Registro Giornaliero di Protocollo	8
4.2	Conservazione dei Documenti Protocollati	9
4.3	Conservazione delle FatturePA.....	9
5	Metadati da associare alle diverse tipologie di documenti	11
5.1	Metadati Minimi da associare a qualsiasi documento informatico	11
5.2	Metadati Minimi del documento informatico amministrativo	11
5.3	Metadati Minimi del documento informatico avente rilevanza tributaria	12
5.4	Metadati Minimi Registro Giornaliero di Protocollo.....	12
5.5	Metadati Minimi Documento Protocollato	13
5.6	Metadati Minimi FatturaPA	13

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;
- 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 Agenzia delle Entrate;
- La tipologia dei pacchetti informativi (Versamento, Archiviazione, Distribuzione) gestiti dal Sistema di Conservazione di InfoCert;
- La tipologia dei pacchetti informativi (Versamento, Archiviazione, Distribuzione) gestiti dal Sistema di Conservazione di Agenzia delle Entrate;
- L'elenco delle *classi documentali* e definizione dei metadati gestiti dal Sistema di Conservazione di InfoCert;
- L'elenco delle *classi documentali* e definizione dei metadati gestiti dal Sistema di Conservazione di Agenzia delle Entrate.

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

A decorrere dal 1° gennaio 2022 i rapporti con i Conservatori (InfoCert S.p.A. e Agenzia delle Entrate) sono regolati, oltre che dai rispettivi accordi/contratti di servizio, dal "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici" adottato da AgID con Determinazione n. 455/2021 del 25 giugno 2021 (come modificata dalla Determinazione n. 629/2021), che ha sostituito il precedente meccanismo di accreditamento di cui alla Circolare AgID n. 65/2014, abrogata dalla medesima data. L'Ente verifica periodicamente che i Conservatori mantengano i requisiti di qualità, sicurezza e organizzazione previsti dal predetto Regolamento (Allegato A).

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 informatici, 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 (PDF/A-1, ver. PDF 1.4). Si segnala che lo standard PDF/A comprende inoltre i livelli successivi ISO 19005-2:2011 (PDF/A-2) e ISO 19005-3:2012 (PDF/A-3), quest'ultimo idoneo all'incorporamento di allegati (rilevante in particolare per le FatturePA con allegati, cfr. cap. 4.3). Il livello PDF/A effettivamente generato dai Sistemi di Conservazione di InfoCert e Agenzia delle Entrate è specificato nei rispettivi Manuali del Sistema di Conservazione.
	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 possono 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 documento 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.

Riferimento paragrafo 6.2 "Manuale del Sistema di Conservazione" di Agenzia delle Entrate.

La struttura dell'indice del pacchetto di versamento/archiviazione (IPdA) è coerente con lo standard UNI 11386:2020 "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI SInCRO)", richiamato dalle Linee Guida AgID vigenti, che sostituisce la precedente versione UNI 11386:2010.

3.2 Specifiche del Rapporto di Versamento

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

Riferimento paragrafo 7.9.1 "Manuale del Sistema di Conservazione" di Agenzia delle Entrate.

4 Tipologie dei documenti posti in conservazione

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

- Registro di protocollo informatico;
- Documento Protocollato;
- Fatture Elettroniche in formato FatturaPA

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 AgID sulla formazione, gestione e conservazione dei documenti informatici (Determinazione n. 407/2020 del 9 settembre 2020, come modificata dalla Determinazione n. 371/2021 del 17 maggio 2021, in vigore dal 1° gennaio 2022), e in particolare al relativo Allegato 6 "Comunicazione tra AOO di documenti amministrativi protocollati", 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 normativa (giornaliera) e inviato in conservazione dai Servizi competenti sui relativi procedimenti. L'unico registro
Salerno Solidale S.p.A. Manuale di Conservazione Allegato 2 – Disciplinare Tecnico Pagina 8 di 13	

	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	Documento 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 normativa (giornaliera) e inviato in conservazione dai Servizi competenti sui relativi procedimenti. Con ordine di servizio saranno individuati gli operatori preposti all'operazione

4.3 Conservazione delle FatturePA

Tipologia di documento	Fatture elettroniche nel formato FatturaPA		
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) corredato da eventuali allegati.		
Modalità di invio	La gestione delle fatture elettroniche è effettuata mediante lo specifico servizio messo a disposizione da Agenzia delle Entrate. 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.		
Data di decorrenza del processo di conservazione	08/01/2019. Si segnala che il D.L. 21 giugno 2022, n. 73 (convertito con L. 4 agosto 2022, n. 122) ha esteso progressivamente l'obbligo di fatturazione elettronica anche ai soggetti in regime forfettario (dal 1° luglio 2022 per i soggetti sopra soglia, dal 1° gennaio 2024 per tutti). Da verificare ed eventualmente confermare che il flusso di conservazione copra anche le fatture emesse/ricevute da/verso tali soggetti a partire dalle rispettive decorrenze.		
Descrizione del flusso	La funzione automatica per la generazione del pacchetto di versamento sarà successivamente concordata anche in vista di		
Salerno Solidale S.p.A.		Manuale di Conservazione Allegato 2 – Disciplinare Tecnico	Pagina 9 di 13

	eventuali chiarimenti che la vigente normativa proporrà. La procedura estrae i dati secondo le specifiche definite nel manuale di gestione del Conservatore. Successivamente è possibile il trasferimento automatico in conservazione oppure la generazione del file e l'esecuzione manuale dell'operazione di upload nel portale del Conservatore.
--	---

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 immutabile, 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.**

5.4 Metadati Minimi Registro Giornaliero di Protocollo

Si rimanda in merito a quanto previsto dalle linee guida AgID, in particolare alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici (Determinazione n. 407/2020, mod. Determinazione n. 371/2021), Allegato 5 "Metadati" (versione aggiornata maggio 2021), che individua il set minimo di metadati applicabile al Registro Giornaliero di

Protocollo, in coerenza con quanto definito dal connettore di interscambio con il Protocollo Informatico fornito da Datagraf Servizi S.r.l.

5.5 Metadati Minimi Documento Protocollato

Si rimanda in merito a quanto previsto dalla normativa vigente, in particolare alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici (Determinazione n. 407/2020, mod. Determinazione n. 371/2021), Allegato 5 "Metadati" (versione aggiornata maggio 2021), e al set minimo effettivamente applicato dal connettore di interscambio con il Protocollo Informatico fornito da Datagraf Servizi S.r.l.

5.6 Metadati Minimi FatturaPA

Si rimanda in merito a quanto previsto dalla normativa vigente, in particolare alle specifiche tecniche del formato FatturaPA vigenti (Provvedimento dell'Agenzia delle Entrate e relativo Allegato tecnico) e al Manuale del Sistema di Conservazione di Agenzia delle Entrate, versione corrente, che individuano il set minimo di metadati associato alle fatture elettroniche conservate.

tinexta
infocert

Manuale della Conservazione

Sommario

MANUALE DELLA CONSERVAZIONE.....	1
REGISTRO DELLE VERSIONI.....	4
SCOPO E AMBITO DEL DOCUMENTO	6
TERMINOLOGIA.....	7
NORMATIVA E STANDARD DI RIFERIMENTO	13
RUOLI E RESPONSABILITÀ	16
PROFILO DI TINEXTA INFOCERT	16
RESPONSABILI TINEXTA INFOCERT	19
OGGETTI SOTTOPOSTI A CONSERVAZIONE	22
FORMATI.....	23
METADATI	23
IL PROCESSO DI CONSERVAZIONE	27
CONTROLLI DI VERSAMENTO	28
PRODUZIONE DI COPIE O DUPLICATI	29
VERIFICHE DI INTEGRITÀ E LEGGIBILITÀ.....	29
SCARTO DEI PACCHETTI DI ARCHIVIAZIONE	30
HANDOVER E INTEROPERABILITÀ	31
RICERCA ED ESIBIZIONE DEI DOCUMENTI CONSERVATI.....	31
I SISTEMI DI CONSERVAZIONE	32
SIGILLO DEI PACCHETTI DI ARCHIVIAZIONE	33
MARCA TEMPORALE DEI PACCHETTI DI ARCHIVIAZIONE	33

STORAGE	34
SICUREZZA E PROTEZIONE DEI DATI	34
PROCEDURE DI GESTIONE E MONITORAGGIO	35
CONTROLLI PERIODICI E AUDIT	38
SPECIFICITÀ DEL CONTRATTO	40

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 e introduzione Linee Guida AgID
11	Aprile 2022	Semplificazione nella descrizione dei processi Introduzione del servizio SAFE LTA Aggiornamento procedure di monitoraggio
12	Maggio 2023	Nuovo logo Aggiornamento TSS per la marca temporale
13	Agosto 2024	Semplificazione e aggiornamento Responsabili, Profilo Tinexta Infocert (indirizzi e qualificazione ACN), Sistema SAFE LTA e Specificità del contratto
14	Aprile 2025	Nuovo logo Cambio Responsabile del servizio
15	Dicembre 2025	Cambio ragione sociale

tinexta
infocert

SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il **manuale della conservazione di Tinexta Infocert**, ai sensi delle **Linee Guida AgID**, Agenzia per l'Italia Digitale, su formazione, gestione e conservazione dei documenti informatici di maggio 2021, richiamate dal **Codice dell'Amministrazione Digitale** - decreto legislativo n. 82 del 2005.

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.

Ogni soggetto produttore, cliente dei servizi di conservazione di Tinexta Infocert e titolare dei documenti conservati, può liberamente far riferimento al presente documento nel proprio manuale della conservazione.

Il presente manuale è firmato digitalmente a riprova del fatto che il management aziendale ha approvato i contenuti.

TERMINOLOGIA

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.
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.
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

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.
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 <i>bit</i> 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.
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 <i>wrapping</i>), 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.

FUNZIONE DI HASH CRITTOGRAFICA	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o <i>digest</i> (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 " <i>digest</i> " (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 <i>hash</i> 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.
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.
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 (<i>FILE PACKAGE</i>)	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.
<i>PATH</i>	Percorso (<i>vedi</i>).
<i>PATHNAME</i>	Concatenazione ordinata del percorso di un file e del suo nome.
<i>PERCORSO</i>	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
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.
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
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.
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

<i>TIMELINE</i>	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di <i>timeline</i> 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.
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.

NORMATIVA E STANDARD DI RIFERIMENTO

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

- eIDAS (electronic IDentification Authentication and Signature) Reg. 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, così come modificato dal Reg. (UE) 2024/1183 of the European Parliament and of the Council of April 2024.
- 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.
- 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) e ss.mm.ii.;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 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 [parzialmente abrogate dalle Linee Guida AgID a partire da gennaio 2022];
- 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;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici pubblicate a settembre 2020, aggiornate nel maggio 2021 e pienamente applicabili dal gennaio 2022.

- Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici di dicembre 2021 (marketplace).

Si riportano di seguito gli standard di riferimento:

- UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- ISO/TR 18492 - Long-term preservation of electronic document-based information;
- ISO 20652 - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard;
- ISO 20104 - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS);
- ISO/CD TR 26102 - Requirements for long-term preservation of electronic records;
- SIARD Software Independent Archiving of Relational Databases 2.0;
- ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de données pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018;
- METS - Metadata Encoding and Transmission Standard;
- PREMIS – PREservation Metadata: Implementation Strategies;
- EAD (3)/ISAD (G);
- EAC (CPF)/ISAAR (CPF)/NIERA (CPF);
- SCONS2/EAG/ISDIAH;
- ISO 16363 - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories;
- ISO/IEC 27001 - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018 - Information technology -- Security techniques -- Code of practice for

protection of personally identifiable information (PII) in public clouds acting as PII processors;

- ETSI TS 101 533-1 V1.2.1 - 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 V1.2.1 - 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.

Inoltre, si segnalano due procedure aziendali interne connesse al servizio:

- **Procedura di handover e scarto**, che descrive le modalità di richiesta ed esecuzione delle attività di versamento da/a un altro Conservatore e delle attività di cancellazione fisica e logica dei documenti, nel rispetto delle Linee Guida AgID e del GDPR.
- **Piano di cessazione**, che descrive le attività di Tinexta Infocert in caso di cessazione dei servizi di conservazione, in modo da fornire a utenti e clienti il supporto necessario alla migrazione verso altri Conservatori.

RUOLI E RESPONSABILITÀ

Nel processo di conservazione digitale intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità.

I ruoli individuati dalle Linee Guida AgID sono:

- a) **TITOLARE DELL'OGGETTO DELLA CONSERVAZIONE** (soggetto produttore degli oggetti di conservazione);
- b) **PRODUTTORE DEI PACCHETTI DI VERSAMENTO** (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, anche attraverso l'utilizzo di piattaforme o sistemi Tinexta Infocert);
- c) **UTENTE ABILITATO** (persona, ente o sistema che interagisce con i servizi di conservazione, al fine di fruire delle informazioni di interesse, cioè per le attività di ricerca ed esibizione a norma);
- d) **RESPONSABILE DELLA CONSERVAZIONE** (interno al cliente/produttore, che sceglie di affidare il servizio a Tinexta InfoCert);
- e) **CONSERVATORE** (Tinexta Infocert).

I primi quattro ruoli sono tipicamente individuati all'interno dell'organigramma di quello che per Tinexta Infocert è il cliente/produttore.

Quest'ultimo affida in *full outsourcing* il servizio di conservazione a Tinexta Infocert S.p.A., in accordo con quanto previsto dai documenti contrattuali descritti al capitolo 'Specificità del Contratto' e dalle Linee Guida AgID. In particolar modo, nell'Atto di affidamento sono elencate funzioni e ambiti oggetto della delega.

All'interno dell'organigramma di Tinexta Infocert, sono, invece, individuati un **Responsabile del servizio di conservazione**, un **Responsabile della funzione archivistica** (come previsto dal Regolamento AgID) e gli altri ruoli qui di seguito riportati.

PROFILO DI TINEXTA INFOCERT

Tinexta Infocert si pone sul mercato europeo come **Trust Service Provider** qualificato ai sensi del Regolamento eIDAS, leader del mercato 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.

Tinexta Infocert dal 2014 è stata 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.

Da febbraio 2022, è iscritta al Marketplace dei servizi di conservazione di AgID come conservatore qualificato - <https://conservatoriqualeificati.agid.gov.it/>

Inoltre, Tinexta Infocert è tra i fornitori presenti nel Catalogo delle Infrastrutture digitali e dei Servizi Cloud di ACN (Agenzia per la Cybersicurezza Nazionale), requisito normativo necessario per offrire alla Pubblica Amministrazione, le proprie soluzioni di conservazione digitale a norma: SAFE LTA (SaaS - ID Scheda in ACN: SA-3452) e LegalDoc (SaaS - ID Scheda: SA-779),

<https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud>

denominazione sociale	Tinexta Infocert S.p.A.
sede legale:	Piazzale Flaminio 1/b, 00196 Roma
sedi operative:	Piazza da Porto, 3, 35131 - Padova Via Fernanda Wittgens, 6, 20123 – Milano Via Gian Domenico Romagnosi 4, 00196 Roma
telefono:	049.7849350
sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
codice fiscale / partita IVA	07945211006
numero REA	RM – 1064345

Oggi il servizio di conservazione di Tinexta Infocert si declina in due prodotti:

- **LegalDoc**, storico servizio, sviluppato sulla base delle Regole Tecniche del 2013, pensato per il mercato italiano e accreditato AgID dal 2014.
- **SAFE LTA (Long-Term-Archiving)**, sviluppato nel 2021, sulla base delle specifiche *eArchiving building block* del *Connecting Europe Facility* (CEF), in ottica internazionale.

La **comunità di riferimento** del servizio di Conservazione digitale di Tinexta 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) e delle varie geografie internazionali.



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).

Tinexta 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.

Tinexta Infocert, inoltre, nello svolgimento delle proprie attività, ha conseguito le seguenti certificazioni: <https://www.infocert.it/certificazioni>

RESPONSABILI TINEXTA INFOCERT

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	Lucia Bortoletto	- 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 (in collaborazione con Ufficio Legale e Product Marketing Manager), 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.	da marzo 2025
Responsabile funzione archivistica di conservazione	Marta Gaia Castellan	- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il	da settembre 2015

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		Ministero dei beni e delle attività culturali per quanto di competenza; controlli periodici a campione sulla leggibilità dei documenti conservati.	

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

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile del servizio	Nicola Maccà	Da luglio 2018 a marzo 2025
Responsabile sviluppo e manutenzione del sistema di conservazione	Lucia Bortoletto	da luglio 2018 a gennaio 2022 (data in cui il Regolamento AgID ha ristretto le figure di responsabilità alle due nella precedente tabella)
Responsabile trattamento dati personali	Ilenia Gentilezza	da marzo 2020 a luglio 2023
Responsabile Sicurezza dei sistemi per la conservazione	Giovanni Belluzzo	da luglio 2018 a gennaio 2022
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
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

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
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

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).

I pacchetti 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 o in una singola chiamata. Le modalità di versamento sono diverse: dal caricamento manuale attraverso portale web, all'utilizzo di chiamate applicative. Il sistema ritorna una Ricevuta di versamento.

Per "**PACCHETTO DI ARCHIVIAZIONE**" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center Tinexta Infocert e associato a un file XML, detto Indice del Pacchetto di Archiviazione (IPdA o indice di conservazione UNI SInCRO) sigillato e marcato temporalmente dal Responsabile del servizio di Tinexta Infocert. In LegalDoc coincide con il Rapporto di versamento.

Questo indice di conservazione, secondo lo standard **UNI 11386 SInCRO 2020**, contiene: una sezione di SelfDescription (con i riferimenti dell'applicativo e del Conservatore), una sezione di PVolume (con lo schema xsd), una sezione MoreInfo per LegalDoc (con token, bucket, policy, operation, target), una sezione FileGroup (con token, hash e SHA dei vari file del pacchetto), una sezione Process (con i riferimenti al manuale, al Responsabile del servizio e al riferimento temporale).

Ogni documento da conservare viene identificato in modo univoco attraverso un token (es. per LegalDoc TB853E72B7552EBB8D0AF3FE9EE1EAB3D97519959346B83DD5E539).

Per "**PACCHETTO DI DISTRIBUZIONE**" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente, in risposta a una sua ricerca e richiesta di esibizione. Il suo contenuto coincide con il "pacchetto di archiviazione".

Eventuali specificità sono concordate con il Soggetto produttore e descritte nelle 'Specificità del Contratto' - Specifiche tecniche per l'integrazione – Allegato Tecnico al Contratto LegalDoc o SAFE LTA. Un pacchetto di archiviazione in LegalDoc è composto da:

- L'Indice di Conservazione UNI SInCRO, altrimenti detto Indice del Pacchetto di Archiviazione o Indice di Conservazione (sigillato e marcato dal Responsabile del servizio di Tinexta Infocert)
- File di parametri (contenente le informazioni per la leggibilità nel tempo)
- File di indici (contenente i metadati del documento conservato)
- File di dati (documento conservato)

Un pacchetto di archiviazione in SAFE LTA è composto da:

- L'Indice di Conservazione UNI SInCRO, altrimenti detto Indice del Pacchetto di Archiviazione o Indice di Conservazione (sigillato e marcato da Tinexta Infocert)
- Metadata Descriptive (file XML di metadattazione)
- Metadata Preservation (file XML di metadattazione secondo lo standard PREMIS)
- Schemas (file XSD di metadattazione)

- Representation (documento conservato)

FORMATI

Tipologie documentali e formati sono sempre concordati con il soggetto produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione'.

In LegalDoc i visualizzatori di alcuni formati (definiti in Tinexta Infocert come 'standard' perché maggiormente richiesti) sono automaticamente assegnati all'atto dell'attivazione del proprio ambiente di conservazione e sono forniti da Tinexta Infocert al soggetto produttore all'atto di attivazione del servizio.

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	

Tutti i documenti inviati in conservazione sono associati al visualizzatore configurato per il particolare formato.

Conservare documenti in altri formati (jpeg, Open Document Format, eml, DICOM, ecc..), in conformità con l'**Allegato 2 delle Linee Guida AgID**, è sempre possibile. Qualora un soggetto produttore necessiti di formati aggiuntivi rispetto a quelli standard, può segnalarlo nei 'Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA (compresi nelle 'Specificità del Contratto') o configurarli autonomamente utilizzando l'apposita funzionalità ed eventualmente conservare gli appositi visualizzatori all'interno del sistema. Un'apposita sezione dell'ambiente di conservazione, infatti, è dedicata alla conservazione dei visualizzatori dei formati (*viewer*), che può essere arricchita a seconda delle esigenze.

METADATI

I metadati sono dati associati ai documenti da conservare in fase di formazione, per identificarli, descrivendone il contesto, il contenuto e la struttura, così da permetterne la gestione del tempo. Nei sistemi di conservazione sono anche utilizzati come chiavi di ricerca.

Le Linee Guida di AgID su formazione gestione e conservazione dei documenti informatici, all'**Allegato 5**, prevedono un set di metadati obbligatori per il documento informatico (maggiormente diffuso), il documento amministrativo informatico (pensato per le pubbliche amministrazioni) e per le aggregazioni documentali (come per esempio i fascicoli).

In breve:

Identificativo del Documento

Un set di metadati serve a identificare il documento da conservare. Si indica il numero utilizzato nel sistema di gestione documentale dove il documento viene formato e gestito, per es. documentID, o identificativo Sdl per le fatture o ID SAP o DossierID. Si indica anche l'impronta di hash e l'algoritmo utilizzato (si suggerisce SHA-256).

Modalità di Formazione

Questo metadato serve a dichiarare come il documento da conservare è stato formato. Le possibilità sono:

- per 'creazione tramite l'utilizzo di strumenti software' (es. documenti scritti al pc)
- per 'acquisizione per via telematica o della copia per immagine' (es. documenti scansionati)
- per 'transazioni o processi informatici o moduli o formulari resi disponibili all'utente' (es. documenti compilati come form online)
- per 'generazione da registrazioni o banca dati' (es. estrazioni da database).

Tipologia Documentale

Metadato che può essere compilato con un valore fisso (default) per determinati processi e che indica per es. contratti, libri sociali, libri e registri contabili, fatture, determine, nota spese, ecc.

Dati di Registrazione

Questo set di metadati descrive un'eventuale registrazione del documento su un registro o repertorio prima del suo versamento in conservazione.

Il flusso può essere:

- in uscita se il documento viene spedito all'esterno dell'azienda/amministrazione
- in entrata se il documento è stato ricevuto dall'esterno
- interno se il documento resta all'interno dell'azienda/amministrazione che lo ha formato.

Il tipo di registro può essere:

- Nessuno
- Protocollo Ordinario/ Protocollo Emergenza
- Repertorio/Registro.

È necessario anche indicare la data e ora di registrazione e il numero attribuito al documento (es. numero del contratto, numero della nota spese, o nel caso dei libri sociali potrebbe coincidere con il progressivo del verbale di assemblea o nel caso di libri fiscali il numero potrebbe essere un progressivo formato da mese e anno).

Oggetto

In questo campo si indica l'oggetto del documento, con particolare attenzione alle parole chiave con cui verrà ricercato in futuro.

Soggetti e Ruoli

Questo set di metadati indica i soggetti vari che sono coinvolti nella formazione e gestione del documento prima del suo versamento in conservazione.

I valori ammessi da AgID sono:

- assegnatario
- autore
- mittente
- destinatario
- operatore
- produttore
- RGD= Responsabile della Gestione Documentale
- RSP= Responsabile del Servizio di Protocollo
- Soggetto che effettua la registrazione
- Altro
- Amministrazione che effettua la registrazione
- RUP= Responsabile Unico del Procedimento

Almeno un soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla) e un autore o un mittente vanno indicati obbligatoriamente.

Questi set di metadati possono essere ripetibili.

Per es. possiamo indicare il mittente e il destinatario di una fattura, l'autore e il soggetto che effettua la registrazione di un libro sociale o fiscale, o di una nota spese, l'autore di un contratto.

Per ciascun ruolo è necessario poi specificare anche il tipo di soggetto, tra:

- AS per Assegnatario
- PF per persona fisica
- PG per organizzazione
- PAI per amministrazione pubblica italiana
- PAE per le Amministrazioni Pubbliche estere
- SW per i documenti prodotti automaticamente (Se Ruolo = Produttore)
- RUP per Responsabile Unico del Procedimento.

E per ciascuno si specificano poi rispettivamente nome, cognome (se PF) o denominazione (se PG), ed eventualmente anche il codice fiscale e gli indirizzi mail.

Allegati

Questo set di metadati serve a indicare se il documento da conservare ha allegati, quanti sono (valori ammessi: 0, 1, 2, 3...) e quali sono, legando il documento padre e i suoi allegati con un reciproco rimando, basato sul numero identificativo di ciascun documento.

Classificazione e Fascicolazione

Questo set di metadati, tipicamente utilizzato dalle pubbliche amministrazioni, indica il riferimento al titolo e alla classe del titolare/piano di classificazione, con la possibilità di inserirne la codifica, la descrizione e l'URI per un rimando puntuale.

È possibile indicare anche l'identificativo dell'aggregazione documentale (es. del fascicolo o della serie) a cui il documento da conservare fa riferimento.

Booleani

Alcuni metadati, definiti come 'booleani' vengono popolati solo con 'vero' o 'falso', indicando se il documento conservato è o non è riservato, è o non è firmato digitalmente, è o non è marcato temporalmente, è o non è sigillato, è o non è accompagnato da una certificazione di processo (se scansionato).

Formato

Un set di metadati indica il formato del documento da conservare (es. PDF, XML, ecc.), specificando opzionalmente anche il prodotto software, la versione e il produttore.

Nome File e Versione

Tra i metadati si indicano anche il nome file del documento da conservare e la sua versione (es. 1, 2, 3).

Se la versione è maggiore di 1, cioè si sta versando in conservazione un documento che è una rettifica o un'annotazione o integrazione di un documento già conservato, questa modifica va tracciata con un set di metadati che indica il tipo di modifica, l'identificativo della versione precedente, chi l'ha fatta e quando.

Tempo di Conservazione

Opzionalmente è possibile inserire tra i metadati anche il riferimento alle tempistiche di conservazione, per facilitare le attività di selezione e scarto.

Nei servizi erogati in ambito internazionale, i metadati sono concordati con il produttore, in base alla normativa locale e specifica.

Tipologie documentali e metadati sono sempre concordati con il soggetto produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA, che contengono anche delle note operative per una corretta metadattazione, secondo le Linee Guida AgID e nel 'file di configurazione', che descrive nel dettaglio l'ambiente di conservazione (bucket o Company).

Tuttavia, il produttore può in autonomia aggiungere ulteriori metadati ad ogni versamento.

IL PROCESSO DI CONSERVAZIONE

I sistemi di conservazione sono erogati in modalità **SaaS** (*Software as a Service*) secondo uno schema di *Business Process Outsourcing* (BPO).

I servizi hanno l'obiettivo di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di tutti i documenti informatici conservati, nel rispetto della normativa vigente.

Il processo può essere così schematizzato:

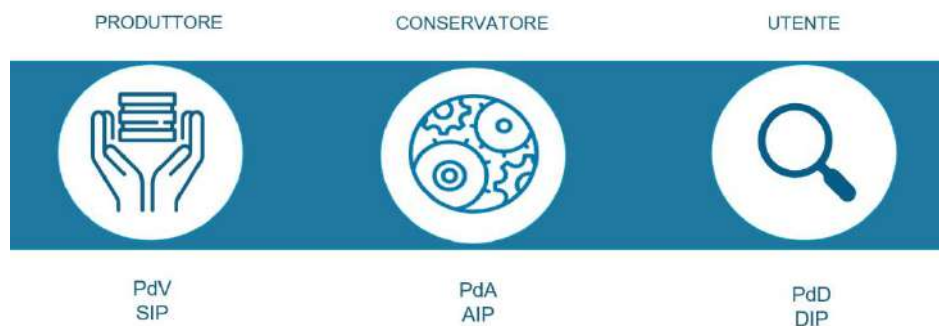


Figura 1 disegno di processo

1. il produttore invia i documenti in conservazione con un pacchetto di versamento, contenente anche i metadati necessari;
2. il pacchetto viene preso in carico dal sistema se rispetta la configurazione concordata (formati, metadati, parametri, policy...) e se l'impronta di hash calcolata coincide con quella contenuta nel pacchetto;

in SAFE LTA, il sistema restituisce al produttore il link per potere reperire il rapporto di versamento;

3. il sistema crea i pacchetti di archiviazione; il Responsabile del servizio sigilla e marca temporalmente l'indice di conservazione UNI SInCRO di ogni singolo pacchetto di archiviazione, a garanzia di integrità, immutabilità e autenticità;

in LegalDoc, il sistema restituisce al produttore l'indice di conservazione come ricevuta (rapporto di versamento);

4. il database del sistema viene aggiornato, il pacchetto di archiviazione viene indicizzato, memorizzato e ridonato più volte;
5. il documento conservato può essere ricercato attraverso i metadati, su richiesta dell'utente in possesso delle apposite credenziali, in qualsiasi momento, ed esibito mediante un pacchetto di distribuzione, che contiene tutte le evidenze del processo.

I sistemi consentono, quindi, le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati dal produttore;
- **conservazione del pacchetto di archiviazione**, a norma di legge e per tutta la durata prevista dal contratto;
- **rettifica del pacchetto di archiviazione**, modifica logica, nel pieno rispetto del principio di tracciabilità;
- **ricerca** tra i documenti conservati, utilizzando uno o più metadati popolati in fase di versamento;
- **esibizione del pacchetto di distribuzione**, contenente sia il documento conservato che gli altri documenti a corredo della corretta conservazione, che possono essere scaricati in autonomia, in qualsiasi momento;
- **scarto**, su richiesta formale del Responsabile della conservazione del produttore, cioè cancellazione fisica e logica dei pacchetti di archiviazione e di ogni loro duplicato.

I sistemi di conservazione, quindi, integrano il sistema di gestione documentale del soggetto produttore, sia esso un'azienda o un ente, e ne estendono i servizi con funzionalità di archivio di deposito.

Le fasi di formazione e gestione dei documenti sono organizzate liberamente dal cliente/produttore all'interno del proprio sistema di gestione documentale, in quanto i servizi qui descritti intervengono solamente nella fase di conservazione e solamente per i documenti che il soggetto produttore sceglie di conservare.

CONTROLLI DI VERSAMENTO

In fase di versamento vengono automaticamente eseguiti dei controlli sui pacchetti:

- formato dichiarato del documento da conservare (mime type),
- correttezza della struttura dei pacchetti di versamento,
- controlli formali di coerenza rispetto alla configurazione,
- validazione dei tracciati dei file di indice (metadati),
- abilitazione utenza all'attività di versamento,
- validità sessione in uso.

secondo regole e policy concordate in fase di attivazione 'Specificità del Contratto – Scheda Dati Tecnici per LegalDoc o *Submission Agreement* per SAFE LTA di attivazione e File di configurazione'.

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

La documentazione tecnica per integrare SAFE LTA con altri sistemi via API è disponibile su <https://developers.infocert.digital/>

Al terzo rifiuto del pacchetto, sarà necessario contattare il servizio di assistenza tecnica di Tinexta Infocert per tentare una soluzione del problema.

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

PRODUZIONE DI COPIE O DUPLICATI

All'attivazione del servizio vengono concordate con il soggetto produttore le modalità di ricerca ed esibizione dei documenti conservati ('Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA) e vengono create apposite credenziali (user/password).

Gli utenti abilitati possono in qualsiasi momento ricercare e scaricare pacchetti di distribuzione, attraverso interfaccia web o chiamate applicative.

Ogni documento informatico così scaricato in locale è da considerarsi un duplicato, ovvero il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario (CAD art. 1 - i quinquies).

Laddove richiesto dalla natura delle attività, il Responsabile della Conservazione può in autonomia formare copie su diversi supporti dei documenti ottenuti dai pacchetti di distribuzione, anche con l'intervento di un pubblico ufficiale, a garanzia della loro conformità all'originale.

Anche il Responsabile del servizio può valutare il coinvolgimento di un pubblico ufficiale, in relazione all'evolversi dei formati e del contesto tecnologico dei sistemi.

VERIFICHE DI INTEGRITÀ E LEGGIBILITÀ

I sistemi di memorizzazione utilizzati, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architettuale e alle procedure di memorizzazione permanente dei dati, garantiscono l'immodificabilità, l'integrità, la leggibilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione.

I sistemi mantengono traccia di tutte le operazioni effettuate sui documenti in appositi file di log.

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

In aggiunta, Tinexta Infocert 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.

I servizi assicurano la **verifica periodica**, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi con procedure automatiche e manuali.

L'apposita procedura, detta **verificatore binario**, esegue il test di integrità 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:

- calcolo dell'impronta del documento;
- 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 sigillato e marcato temporalmente dal Responsabile del servizio della conservazione stesso).

In caso di anomalie, 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 per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.

In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio 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 'umana' dell'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.

Anche in questo caso viene poi redatto automaticamente un verbale con gli identificativi dei documenti visualizzati, successivamente sottoscritto e conservato dal Responsabile del servizio.

SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

I servizi di conservazione di Tinexta Infocert consentono lo scarto archivistico, cioè la **cancellazione di un pacchetto di archiviazione** e di qualsiasi suo duplicato prodotto durante le attività di conservazione, sia dal punto di vista logico che dal punto di vista fisico, su richiesta formale del Responsabile della conservazione interno al soggetto produttore/titolare del documento.

La procedura può essere attivata per varie ragioni, sia alla chiusura del contratto, sia in continuità di servizio (in itinere), per il venir meno della rilevanza amministrativa, legale o storica dei documenti conservati per il suo produttore, anche in relazione alla *retention period policy* configurata in fase di attivazione del servizio.

Il così detto **scarto in itinere** si può, quindi, richiedere al Customer Care di Tinexta Infocert tramite apposito **modulo**, oppure può essere attivato tramite **chiamate applicative**. In entrambi i casi è richiesta una lista di token firmata digitalmente dal Responsabile della Conservazione interno al produttore/titolare.

Per gli enti pubblici e per gli archivi privati dichiarati di notevole interesse storico, le richieste di scarto sono sottoposte a nulla osta delle soprintendenze archivistiche o delle commissioni di sorveglianza di competenza., verifica che deve essere effettuata dal Responsabile della Conservazione dell'ente.

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 handover tra conservatori e scarto'.

HANDOVER E INTEROPERABILITÀ

Gli archivi di conservazione generati dai sistemi Tinexta Infocert sono conformi allo standard di interoperabilità **UNI SInCRO**. L'adozione di tale standard permette l'interoperabilità e la trasferibilità dei dati in modo semplificato.

Nel caso il soggetto produttore decida di rescindere, chiudere o interrompere il contratto di affidamento del servizio di conservazione, in qualsiasi momento può effettuare il **download** dei propri **pacchetti di distribuzione** in autonomia, attraverso la procedura di esibizione, o, in alternativa, richiedendo il **servizio di restituzione** (su supporto da concordare in base a volume ed esigenze) tramite apposito **modulo**.

Al termine della procedura di handover verso il nuovo Conservatore, i pacchetti verranno cancellati. Seguendo i dettami dello standard OAIS, il versamento in Tinexta Infocert di pacchetti di distribuzione (PdD) provenienti da un altro Conservatore dovrà riguardare sempre **interi pacchetti**, qualsiasi sia il 'modo' con cui vengono formati e le tipologie di metadati o indici che hanno, e non dovrà mai riguardare il singolo documento. È fondamentale in questa procedura di versamento conservare in Tinexta Infocert quante più informazioni possibili sul processo di conservazione precedente e sul Conservatore di provenienza.

Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di handover e scarto'.

RICERCA ED ESIBIZIONE DEI DOCUMENTI CONSERVATI

La ricerca e l'esibizione a norma dei documenti conservati può avvenire tramite chiamate applicative o tramite portale WEB.

Le chiavi di ricerca sono i metadati popolati in fase di versamento.

I sistemi restituiscono un pacchetto di distribuzione, contenente sia il documento conservato che tutti i report e le evidenze di conservazione.

La guida al portale LegalDoc WEB è disponibile qui:

<https://knowledgecenter.infocert.digital/Home/Guida/manuale-utente-legaldoc-web?lang=it>

La guida al portale SAFE LTA WEB è disponibile qui:

<https://knowledgecenter.infocert.digital/Home/Guida/manuale-utente-safe-lta>

I SISTEMI DI CONSERVAZIONE

I sistemi sono organizzati su più siti nel territorio italiano (Region AWS Milano), con applicazioni software in architettura distribuita, utilizzano servizi AWS in modalità SaaS, e una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, firme digitali e sigilli, supporti di conservazione).

Per ragioni di sicurezza, i sistemi sono protetti da firewall configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile. Gli interi sistemi sono interessati periodicamente da processi di back-up completi dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria.

I servizi di conservazione sono accessibili online, tramite portale o chiamate applicative e sono erogati anch'essi in modalità SaaS.

Dal punto di vista architetturale **LegalDoc** è realizzato utilizzando la tecnologia dei Web Services, secondo architettura REST su protocollo HTTPS. Solo per un ristretto numero di Clienti viene utilizzato uno storage presente nel DataCenter di Milano. Ha quindi un'architettura HYBRID Cloud.

Dal punto di vista architetturale **SAFE LTA** si basa su architettura a microservizi, espone api REST-ful e aderisce allo standard OAuth2 / OIDC per quanto riguarda gli scenari di autenticazione / autorizzazione. L'autenticazione utilizza Kong e Keycloak.

Rispetta lo standard ISO 14721 recante il reference model OAIS (*Open Archival Information System*) utilizzato a livello internazionale per la conservazione di risorse digitali e lo standard PREMIS per la metadattazione.

SAFE LTA è interamente erogato su cloud AWS, ha quindi un'architettura PUBLIC Cloud.

I servizi generalizzati usati da servizi di conservazione sono:

- Identity Provider Tinexta Infocert, in quanto Provider ed erogatore di servizi riferiti alla identità digitale,
- SignAPI Tinexta Infocert, in quanto Provider ed erogatore di servizi legati alla Certification Authority.

Sia le applicazioni WEB di interfaccia sia le API REST sono adoperabili solo previa autenticazione: per LegalDoc

- In entrambi i casi l'autenticazione è una basic authentication

per SAFE LTA

- l'autenticazione da interfaccia web è governata attraverso flusso di *authorization-code-flow*, così come previsto da standard,
- l'autenticazione da agenti software che integrano le API REST è governata da flusso di *client-credential-flow*, così come previsto da standard.

Le funzionalità fruibili sono:

- Invio in conservazione dei pacchetti di versamento
- Attività di ricerca avanzata
- Recupero di documenti e metadati
- Download di pacchetti di distribuzione.

Inoltre, per SAFE LTA sono previste le seguenti funzionalità

- Provisioning
- Gestione utenti, gruppi e autorizzazioni

I servizi di conservazione non solo effettuano la validazione di pacchetti di versamento, ma si occupano anche di effettuare una verifica formale dei formati.

Tutte le interazioni tra gli utenti e l'archivio sono registrate in appositi log per ragioni di sicurezza e trasparenza.

La configurazione degli ambienti di conservazione di Legaldoc prevede le seguenti definizioni:

- **Bucket:** è l'area di conservazione dei documenti
- **Policy;** descrive le regole che devono essere seguite durante il processo di conservazione (mime type si possono usare, durata del retention period, etc)
- **Classe documentale:** identifica una tipologia documentale con i suoi metadati. Ad esempio: fatture attive, contratti, libri e registri contabili, ecc.

La configurazione degli ambienti di conservazione di SAFE LTA prevede le seguenti definizioni:

- **Company Group:** identifica un contenitore logico dal quale possono dipendere una o più Company, cioè aree di conservazione. Ogni Company Group è ad uso esclusivo di un solo cliente/titolare.
- **Company:** area di conservazione dei documenti, che può essere usata, ad esempio, per raggruppare i documenti delle diverse società/aziende di un gruppo (Company Group), denominando ogni Company con il nome della singola azienda facente parte del Gruppo.
- **Country:** identifica gli standard normativi adottati dal sistema per la conservazione rispetto alle varie geografie, ed è configurabile a livello di Company.
- **Document Class:** identifica una tipologia documentale con i suoi metadati. Ad esempio: fatture attive, contratti, libri e registri contabili, ecc.

La documentazione tecnica di dettaglio è disponibile su <https://developers.infocert.digital/>

SIGILLO DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, su ogni pacchetto di archiviazione il Responsabile del servizio della conservazione di Tinexta Infocert appone:

- **in Legaldoc una firma digitale qualificata con certificato intestato al Responsabile del servizio di conservazione di Tinexta Infocert**
- **in SafeLTA un sigillo qualificato a nome di Tinexta Infocert.**

Il servizio utilizza un sistema automatico erogato dalla CA - Certification Authority – Tinexta Infocert.

MARCA TEMPORALE DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, viene apposta anche una marca temporale su ogni pacchetto di archiviazione. La marca temporale viene richiesta al TSS - *Time Stamping Service* - Tinexta Infocert, che la restituisce firmata con un certificato emesso dalla TSA - *Time Stamping Authority* - Tinexta Infocert. Il TSS è sincronizzato tramite i segnali forniti dai sistemi satellitari GPS, Galileo e

GLONASS ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

STORAGE

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.

Il sistema di conservazione di Tinexta Infocert e dei suoi partner tecnologici supporta la memorizzazione dei file sia su storage magnetici ad alte performance che su sistema Object Storage. 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 di tutti i documenti.

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

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

Per entrambi i servizi cloud è stata scelta AWS Europe (*Region Milan*), quindi, tutti i dati risiedono in **territorio italiano**.

SICUREZZA E PROTEZIONE DEI DATI

Tinexta Infocert si impegna a mantenere i più alti livelli di qualità e sicurezza, assegna un'importanza strategica alla gestione sicura delle informazioni e riconosce la necessità di sviluppare, mantenere, controllare e migliorare costantemente un **sistema di gestione della sicurezza delle informazioni (ISMS)** in conformità alla **norma UNI CEI EN ISO/IEC 27001: 2017**. Nella policy di sicurezza di Tinexta Infocert per ciascun capitolo della norma ISO vengono fornite le indicazioni da seguire nello svolgimento di tutte le attività. In particolar modo:

- *Management direction for information security,*
- *Organization of information security,*
- *Human resource security,*
- *Asset management,*
- *Access control, Cryptography,*
- *Physical and environmental security,*
- *Operations security,*
- *Communications security,*
- *System acquisition, development, and maintenance,*
- *Supplier relationships,*
- *Information security incident management,*
- *Information security aspects of business continuity management,*
- *Compliance with legal and contractual requirements.*

Tinexta Infocert ha anche ottenuto il **Report SOC 2 Tipo II**, su sicurezza, disponibilità, integrità del trattamento, riservatezza e privacy dei servizi, in conformità all'International **Standard on Assurance Engagements (ISAE) 3000**.

I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio. L'azienda ha mappato tutti i flussi di dati interni e di quelli da e per l'esterno. Sono implementati controlli automatici per evitare l'interconnessione con server esterni non autorizzati. L'accesso alla rete e ai sistemi è consentito esclusivamente agli utenti autorizzati, seguendo quanto prescritto dalla policy aziendale relativa agli Amministratori di Sistema e alla gestione degli accessi logici. Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono priorizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione. Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity e al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti.

A supporto di tali censimenti è stato implementato un CMDB (*Configuration Management Data Base*). Viene effettuata una valutazione di impatto sulla protezione dei dati personali. Il ciclo di vita dei dati è definito e documentato.

Tutti gli accessi (fisici e logici) sono regolati da policy apposite. I diritti di accesso sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.

L'integrità di rete è protetta. Le reti di comunicazione e controllo sono protette.

I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili.

Sono attivi ed amministrati piani di *Incident Response* e di *Business Continuity, Incident Recovery, Disaster Recovery e Vulnerability Management*.

I sistemi informativi, il personale e gli asset sono costantemente monitorati per identificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione. Sono implementati meccanismi che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse. È attiva una policy di gestione dei log, inclusiva della conservazione dei log di sicurezza dei sistemi.

L'organizzazione ha implementato un processo formalizzato di *Incident Management* che include i criteri per documentare l'incidente ai fini del *problem management*, delle comunicazioni istituzionali e delle comunicazioni verso gli stakeholder.

Tutti gli utenti sono informati e addestrati.

Ai sensi del Regolamento UE n. 679/2016 GDPR, Tinexta Infocert assume il ruolo di Responsabile del trattamento dei dati personali. La nomina è inserita all'interno delle "Specificità del Contratto – Atto di Affidamento".

Il trattamento dei dati è effettuato:

- ai soli fini dell'erogazione del servizio,
- con l'adozione delle misure di sicurezza ex art. 32 del Regolamento,
- nel rispetto degli obblighi posti in carico al Responsabile del trattamento dall'art. 28 del Regolamento.

PROCEDURE DI GESTIONE E MONITORAGGIO

I sistemi di conservazione di Tinexta Infocert e i processi da questi implementati rispondono interamente alle norme di legge che regolano la materia. La loro progettazione e il loro continuo miglioramento 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 servizi architetturealmente stabili, affidabili, e che

garantiscono 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 e degli standard, al fine di definire puntualmente i requisiti di *compliance*. Oltre a questi sono definiti ulteriori requisiti funzionali, di architettura e di connettività e interoperabilità, anche in relazione con le evoluzioni tecnologiche, sfruttando le economie di scala e di conoscenza. I Responsabili Tinexta 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.

Inoltre, Tinexta Infocert ha deciso di adottare un sistema di gestione dei servizi IT (SMS) conforme a **ISO IEC 20000** (standard internazionale di gestione dei servizi IT) al fine di mantenere e migliorare la qualità dei servizi aziendali che fornisce. Questi hanno un'attenzione particolare alle esigenze dei clienti, sostenuti da un ciclo continuo di monitoraggio, reporting e revisione degli SLA concordati.

Inoltre, Tinexta Infocert ha adottato un sistema di gestione dei servizi IT (SMS) certificato per la norma **ISO/IEC 20000-1:2018** (standard internazionale di gestione dei servizi IT) al fine di mantenere e migliorare la qualità dei servizi aziendali che fornisce. Questi hanno un'attenzione particolare alle esigenze dei clienti, sostenuti da un ciclo continuo di monitoraggio, reporting e revisione degli **SLA concordati**.

Tale modello di *Service Management System* ha permesso 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 Tinexta 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.

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

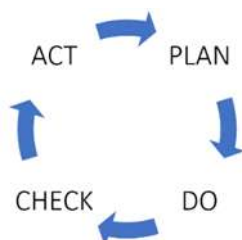


Figura 2 Rappresentazione del modello PDCA SMS

- 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 obiettivi aziendali
- migliorare la qualità dei servizi di business erogati
- fornire attraverso gli SLA una base per la determinazione del valore del servizio.

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

- orario di servizio
- disponibilità di servizio.

Inoltre, Tinexta Infocert si è dotata di una soluzione di monitoraggio open source denominata Grafana LGTM (Loki Grafana Tempo Mimir), un'architettura autogestita in-house nella Region "Milano" del fornitore AWS, che permette la completa gestione dei dati di osservabilità ai Team DEVOPS.

Questa piattaforma di osservabilità abilita i Team DEVOPS di identificare e analizzare problemi di tipo infrastrutturale e applicativo.

Utilizzando un evoluto sistema di gestione e raccolta dati effettua un monitoring full-stack, fornisce gli strumenti per l'ottimizzazione dei servizi, oltre ad un'efficiente gestione di segnalazione degli incident.

Inoltre, è stata abilitata l'integrazione con le piattaforme di controllo Cloudwatch, tool nativi di AWS, che consente di avere il pieno controllo e la gestione delle metriche e log di tutte le "componenti gestite" presenti in cloud.

Il tool è composto dai seguenti elementi fondamentali:

- AGENT: risiedono sui server e collezionano i segnali di telemetria inviando (con connessione unidirezionale) i dati alla piattaforma centrale posta in cloud attraverso protocollo TLS. Gli agent effettuano un controllo sia di tipo infrastrutturale che di performance, consentendo anche la costruzione di schemi architetturali tra i servizi;
- GRAFANA SERVER: è il cuore dello strumento, dove i segnali sono accessibili tramite linguaggi di query dedicati consentendo di gestire, aggregare ed elaborare i dati, definendo la modalità di visualizzazione e gestione di eventuali alert;
- SONDE: possono essere di tipo "black box" oppure script di navigazione complessi, eseguiti da location privata o pubblica; grazie a questa diversa collocazione è possibile verificare il corretto funzionamento di un servizio sia della rete interna che da rete Internet.

Con le metriche raccolte 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 e prevenire tempestivamente anomalie sui servizi erogati da Tinexta Infocert, segnalando in modo puntuale le componenti impattate.

Il monitoring della disponibilità del servizio viene svolto coerentemente con le procedure generali di Tinexta 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 precedentemente descritta.

A fronte di anomalie rilevate, lo strumento, grazie all'integrazione nativa, invia delle segnalazioni ad OPSGENIE, tool di gestione delle notifiche in conformità ai processi di Incident Management aziendali. Tali processi sono descritti nelle procedure che definiscono il Sistema di gestione integrato Tinexta Infocert.

CONTROLLI PERIODICI E AUDIT

In Tinexta 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, ed effettua la raccolta dei dati relativi al funzionamento dei servizi. Il gruppo si riunisce periodicamente, 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.

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.).

Inoltre, il programma di audit aziendale è attuato secondo le procedure del Sistema Integrato di Gestione, con il fine di determinare se i processi aziendali sono:

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

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

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.

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

SPECIFICITÀ DEL CONTRATTO

Le **Condizioni Generali di Contratto** o **Accordo Quadro** regolano la vendita in generale di tutti i servizi Tinexta Infocert.

A questi tipicamente si aggiungono i seguenti allegati:

- Allegato A – Offerta Commerciale,**
- Allegato B – DPA - Data Processing Agreement,**
- Allegato C – Allegato Tecnico,**
- Allegato D – Misure di Sicurezza,**
- Allegato E – Manuale Operativo**, cioè il presente manuale.

Nell'**Allegato C – Allegato Tecnico** sono descritte le condizioni particolari di LegalDoc e SAFE LTA ed è inserito l'**Atto di Affidamento**, che rappresenta la formalizzazione della delega ad Tinexta Infocert del servizio di conservazione e stabilisce espressamente quali attività di fatto vengano assunte da Tinexta Infocert e quali, al contrario, rimangano a carico dell'affidatario, soggetto produttore, come stabilito dalle Linee Guida AgID.

Qui è maggiormente dettagliata anche l'infrastruttura tecnica e l'architettura di ciascun servizio.

Sono richiamati anche la **Scheda dati tecnici d'attivazione** per LegalDoc e il **Submission Agreement** per SAFE LTA, con cui il soggetto produttore/cliente/titolare fornisce tutte le informazioni necessarie su tipologie documentali, metadati, formati e utenze di accesso, per la configurazione degli ambienti di conservazione.

tinexta
infocert

think next,
trust now

MANUALE DEL SERVIZIO DI CONSERVAZIONE DELLE FATTURE ELETTRONICHE

*(Servizio di Conservazione previsto dall'art. 1, comma, 1 del
D.Lgs. 127/2015)*

Versione 3.0

del 29/07/2025

Allegato 2

INDICE DEL DOCUMENTO

1. REGISTRO DELLE VERSIONI	4
2. SCOPO E AMBITO DEL DOCUMENTO	6
3. TERMINOLOGIA (GLOSSARIO, ACRONIMI)	7
4. NORMATIVA E STANDARD DI RIFERIMENTO	13
4.1 NORMATIVA DI RIFERIMENTO DEL SISTEMA DI CONSERVAZIONE.....	13
4.2 NORMATIVA DI RIFERIMENTO DELLE FATTURE ELETTRONICHE.....	13
4.3 STANDARD DI RIFERIMENTO	14
5. RUOLI E RESPONSABILITÀ.....	14
6. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	17
6.1 ORGANIZZAZIONE DEL SERVIZIO	17
6.2 STRUTTURA ORGANIZZATIVA DELL'AGENZIA DELLE ENTRATE.....	18
7. OGGETTI DEL PROCESSO DI CONSERVAZIONE.....	18
7.1 OGGETTI CONSERVATI	18
7.2 PACCHETTO DI VERSAMENTO	19
7.3 PACCHETTO DI ARCHIVIAZIONE	20
7.4 PACCHETTO DI DISTRIBUZIONE.....	22
8. IL PROCESSO DI CONSERVAZIONE.....	23
8.1 MODALITÀ DI ACQUISIZIONE E CONTROLLO DELLE FATTURE ELETTRONICHE AI FINI DELLA CONSERVAZIONE	25
8.2 MONITORAGGIO DELLE RICHIESTE DI CONSERVAZIONE E DEI DOCUMENTI CONSERVATI	26
8.3 PREPARAZIONE E GESTIONE DEL PACCHETTO DI VERSAMENTO	26
8.4 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE	29
8.5 PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE	30
8.6 PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESPORTAZIONE	32
8.7 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE	32
8.8 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE	33
8.9 ESORTAZIONE DAL SISTEMA DI CONSERVAZIONE	33
8.10 LE RICEVUTE DEL SISTEMA DI CONSERVAZIONE	34
9. IL SISTEMA DI CONSERVAZIONE	37
9.1 COMPONENTI LOGICHE	37
9.2 RIVERSAMENTO DIGITALE	38
10. MONITORAGGIO E CONTROLLI.....	39
10.1 PROCEDURE DI MONITORAGGIO.....	39
10.2 VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI	39
10.3 ACCESSO AI DATI E INTEGRITÀ.....	40
10.4 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE	41
11. SPECIFICITÀ DEL SERVIZIO	41

11.1 SERVIZIO DI CONSERVAZIONE - MODALITÀ E TEMPI DI EROGAZIONE	41
11.2 DURATA DELLA CONSERVAZIONE.....	43
11.3 SCHEDA RIEPILOGATIVA DEL SERVIZIO.....	43

1. REGISTRO DELLE VERSIONI

Versione	Data validità	Modifiche apportate	Osservazioni
1.0	01/07/2016	Prima versione	
1.1	10/07/2017	Modifica dei criteri di assemblaggio dei PdA Modifica delle modalità e dei tempi di erogazione del servizio di esibizione	
1.2	19/02/2018	Nomina del nuovo Responsabile del servizio di conservazione Nomina del nuovo Responsabile Sicurezza dei sistemi per la conservazione	
1.3	01/07/2018	Adeguamenti alle modifiche apportate dalla LEGGE 27 dicembre 2017, n. 205 al D.lgs. del 5 agosto 2015, n.127	
1.4	01/12/2018	Nomina del nuovo Responsabile del servizio di conservazione	
1.5	01/01/2019	Nomina del nuovo Responsabile del servizio di conservazione pag. 43 – precisazioni sulla data di disponibilità dei pacchetti di distribuzione	
1.6	01/06/2019	Nomina del nuovo Responsabile del servizio di conservazione	
1.7	21/05/2020	Aggiornamento dati anagrafici dell'Agenzia (cambio indirizzo)	
1.8	04/06/2021	Aggiornamento a seguito della nuova versione dell'accordo di servizio	
1.9	01/12/2022	Aggiornamento a seguito delle nuove linee guida AgID del 10 settembre 2020 e s.m.i. e del relativo adeguamento dei sistemi	
2.0	31/01/2023	Aggiornamento a seguito del nuovo accordo di servizio con l'introduzione del ruolo di Richiedente	

2.1	30/11/2023	Rivisitazione del formato grafico del documento	
2.2	01/04/2024	Nomina del nuovo Responsabile del servizio di conservazione	
3.0	29/07/2025	Aggiornamento del manuale a seguito dell'introduzione delle funzioni di esportazione delle fatture conservate e miglioramento della descrizione del processo di conservazione	

Tabella 1 - Registro delle versioni

2. SCOPO E AMBITO DEL DOCUMENTO

La conservazione a norma dei documenti digitali è un processo che garantisce nel tempo la validità legale di un documento informatico versato nel sistema di conservazione; tale processo garantisce autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti.

Il presente *manuale del servizio di conservazione delle fatture elettroniche* (di seguito "*Manuale*") è relativo al servizio di conservazione delle fatture elettroniche, messo a disposizione dei contribuenti dall'Agenzia delle Entrate, come previsto dall'art 1 del Decreto legislativo 5 agosto 2015, n. 127 (Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni effettuate attraverso distributori automatici, in attuazione dell'articolo 9, comma 1, lettere d) e g), della legge 11 marzo 2014, n. 23). L'Agenzia delle Entrate si avvale del sistema di conservazione messo a disposizione dalla società Sogei S.p.A., nella sua qualità di società *in house*, in virtù degli specifici accordi contrattuali in essere con l'Agenzia stessa, rimanendo estranea Sogei S.p.A. nei rapporti con i contribuenti.

Il servizio di conservazione è conforme alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (di seguito "*Linee guida*") emanate ai sensi dell'art. 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 e s.m.i.

Scopo del documento è descrivere:

- l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi nel processo di conservazione;
- il modello di funzionamento e la descrizione del processo di conservazione;
- l'architettura, 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.

L'adesione del Richiedente all'Accordo di servizio per la conservazione delle fatture elettroniche di cui all' art. 1, comma 1, del D.lgs. 127/2015 (di seguito "accordo di servizio") comporta tra le altre cose:

- l'accettazione del ruolo di **Responsabile della Conservazione delle fatture elettroniche** per le quali viene richiesta la conservazione all'Agenzia delle Entrate secondo quanto previsto dall'art. 1 del decreto legislativo 127/2015;
- l'affidamento, attraverso delega parziale, ai sensi di quanto previsto al paragrafo 4.5 delle Linee guida, della conservazione delle fatture elettroniche prodotte, all'Agenzia delle Entrate, che offre idonee garanzie organizzative, tecnologiche e di protezione di dati personali. La stessa Agenzia, come espressamente specificato nell'accordo di servizio, definisce ed attua le politiche complessive del sistema di conservazione e ne governa la gestione;
- l'accettazione integrale del presente Manuale predisposto dall'Agenzia delle Entrate;

- la responsabilità legale dell'autenticità e del contenuto del documento; tale responsabilità rimane in capo al contribuente, produttore Titolare *dell'oggetto della conservazione*.

L'accordo di servizio è archiviato nel sistema di gestione documentale dell'Agenzia delle Entrate.

3. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Di seguito un glossario dei termini usati (contrassegnati con asterisco i termini del glossario presenti nelle linee guida AgID).

- **Archiviazione elettronica:** processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione.
- **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.
- **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.

Documento: rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica.

- **Documento analogico originale:** documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
- **Documento informatico*:** la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Nel presente contesto è la fattura elettronica.

- **Documento archiviato:** documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica.
- **Documento conservato:** documento sottoposto al processo di conservazione.
- **Documenti in formato XML:** XML (sigla di eXtensible Markup Language) è un linguaggio di markup, ovvero un linguaggio marcatore basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo. Un XSD definisce il tipo di un documento XML in termini di elementi e attributi che possono apparire, in quale relazione reciproca, quale tipo di dati può contenere, ed altro. Può essere usata anche con un programma di validazione, al fine di accertare a quale tipo appartiene un determinato documento XML. XSLT (eXtensible Stylesheet Language Transformations) è il linguaggio di trasformazione dell'XML. Ha lo scopo di rendere possibile la trasformazione di un documento XML in un altro documento tramite un foglio di stile XSL, che fornisce la semantica per la trasformazione.
- **Esibizione*:** operazione che consente di visualizzare un documento conservato.
- **Evento di conservazione:** evento a partire dal quale sono portati in conservazione i documenti presi in carico. Tale evento si verifica sulla base della frequenza di assemblaggio.
- **Evidenza informatica*:** sequenza finita di bit che può essere elaborata da una procedura informatica.
- **Firma digitale:** un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1, comma 1, lettera s) del Codice dell'Amministrazione Digitale.
- **Formato del documento informatico*:** modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
- **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.
- **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.

- **Immodificabilità:** caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
- **Impronta 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 del servizio 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.
- **Marca Temporale:** una marca temporale (timestamp) è una sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento.
- **Memorizzazione:** processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
- **Metadati*:** dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
- **Pacchetto di archiviazione (PdA)*:** pacchetto informativo generato dal sistema di conservazione dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel Manuale.
- **Pacchetto di distribuzione (PdD)*:** pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.

- **Pacchetto di versamento (PdV)*:** pacchetto informativo inviato 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.
- **Presa in carico del Pacchetto di Versamento:** accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal Manuale.
- **Processo di conservazione:** insieme delle attività finalizzate alla conservazione dei documenti informatici.
- **Produttore dei Pacchetti di versamento*:** 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.
- **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.
- **Registrazione informatica:** insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente.
- **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.
- **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. Ai fini del presente documento, il titolare dell'oggetto della conservazione o, in caso di persona giuridica, il suo rappresentante legale coincide con il responsabile della conservazione.
- **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 del servizio di conservazione:** l'Agenzia delle Entrate, alla quale il Responsabile della Conservazione ha affidato la conservazione delle fatture elettroniche che viene effettuata tramite il sistema di conservazione realizzato e gestito dalla società Sogei S.p.A., individua nella propria organizzazione il Responsabile del

servizio di conservazione che, su delega del Responsabile della conservazione, definisce ed attua le politiche complessive del sistema di conservazione e ne governa la gestione, in relazione al modello organizzativo descritto nel presente Manuale.

- **Responsabile del sistema di memorizzazione:** soggetto che ha il compito di gestire, monitorare e garantire il corretto funzionamento del sistema di memorizzazione e assicurare che i dati siano trattati in modo sicuro, siano accessibili solo a chi autorizzato, e siano gestiti in modo efficiente, proteggendo sia l'organizzazione che i diritti degli utenti.
- **Responsabile del trattamento dei dati:** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
- **Responsabile della sicurezza:** soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
- **Richiedente:** è il sottoscrittore dell'accordo di servizio in proprio o in ragione di incarico o delega da parte del titolare dell'oggetto della conservazione; ai fini dell'accordo il titolare dell'oggetto della conservazione coincide con il responsabile della conservazione.
- **Riferimento temporale*:** insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
- **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.
- **Sistema di memorizzazione:** insieme di tecnologie, infrastrutture e procedure utilizzate per gestire e recuperare i dati in formato digitale all'interno di un'organizzazione, garantendo l'accessibilità, la durabilità e la protezione nel tempo.
- **Titolare dell'oggetto della conservazione*:** soggetto che produce o riceve il documento informatico da versare in conservazione e ne assume la responsabilità nell'ambito del processo di conservazione.
- **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.

- **W.O.R.M.** (Write Once Read Many): l'acronimo indica la caratteristica di alcuni tipi di supporti (ottici o magnetici) che rende i dati registrati su di essi non modificabili e non cancellabili, ma solo accessibili in lettura ed in copia.

4. NORMATIVA E STANDARD DI RIFERIMENTO

4.1 NORMATIVA DI RIFERIMENTO DEL SISTEMA DI CONSERVAZIONE

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo A)” - Capo IV
- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell’amministrazione digitale” e s.m.i.
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
- Decreto 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. 82/2005”
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR)
- Linee guida AgID sulla formazione gestione e conservazione dei documenti informatici del 9 settembre 2020 e pubblicato il 10 settembre 2020 e s.m.i.

4.2 NORMATIVA DI RIFERIMENTO DELLE FATTURE ELETTRONICHE

- Decreto del Presidente della Repubblica numero 633 del 26 ottobre 1972
- Legge n. 244 del 24 dicembre 2007
- Decreto del Ministro dell’Economia e delle finanze del 7 marzo 2008
- Decreto-legge 29 novembre 2008, n. 185 “Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale” convertito con modificazioni dalla L. 28 gennaio 2009, n. 2 (art. 16, comma 12-bis)
- Decreto interministeriale n. 55 del 3 aprile 2013
- Decreto legislativo 5 agosto 2015, n. 127 “Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni effettuate attraverso distributori automatici, in attuazione dell’articolo 9, comma 1, lettere d) e g), della legge 11 marzo 2014, n. 23”
- Decreto-legge del 16 ottobre 2017, n. 148 (in G.U. 16/10/2017, n.242), convertito con modificazioni dalla L. 4 dicembre 2017, n. 172 (in G.U. 05/12/2017, n. 284).
- Legge del 27 dicembre 2017, n. 205 (in SO n.62, relativo alla G.U. 29/12/2017, n.302)

- Decreto MEF 24 agosto 2020, n. 132 Regolamento recante individuazione delle cause che possono consentire il rifiuto delle fatture elettroniche da parte delle amministrazioni pubbliche. (GU n.262 del 22-10-2020)

4.3 STANDARD DI RIFERIMENTO

Si riportano di seguito i riferimenti dei principali standard elencati nell'allegato 4 "Standard e specifiche tecniche" delle Linee guida relativamente alla conservazione digitale e sicurezza informatica:

- UNI 11386 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali
- ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione
- ISO 15836 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core
- ISO/TR 18492 - Long-term preservation of electronic document-based information
- ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System)
- ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ETSI TS 101 533-1 V1.2.1 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 V1.2.1 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

5. RUOLI E RESPONSABILITÀ

Il Responsabile della Conservazione delega all'Agenzia delle Entrate le seguenti funzioni:

- a) la definizione e l'attuazione delle politiche di conservazione e dei requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare;

- b) la gestione del processo di conservazione di cui garantisce nel tempo la conformità alla normativa vigente;
- c) la generazione e la sottoscrizione del rapporto di versamento, secondo le modalità previste dal Manuale;
- d) la generazione e la sottoscrizione del pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale;
- e) il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi dei file fattura trasmessi e della leggibilità dei file fattura per come trasmessi all'Agenzia escludendo dalla delega la leggibilità degli eventuali allegati codificati all'interno degli stessi file fattura che il Responsabile della conservazione deve garantire mantenendo validi e funzionanti nel tempo gli strumenti software utilizzati per la loro formazione o visualizzazione;
- g) l'adozione di misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, nonché di analoghe misure con riguardo all'obsolescenza del formato dei file fattura, escludendo dalla delega le misure riguardanti l'obsolescenza dei formati degli eventuali allegati codificati all'interno degli stessi file fattura che il Responsabile della conservazione deve garantire mantenendo validi e funzionanti nel tempo gli strumenti software utilizzati per la loro formazione o visualizzazione;
- h) la duplicazione o la copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale;
- i) l'adozione delle misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- j) l'assistenza agli organismi competenti previsti dalle norme vigenti e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza, relativamente al solo sistema di conservazione.

Di seguito sono indicati ruoli e attività dei soggetti che partecipano al processo di conservazione delle fatture elettroniche nel sistema dell'Agenzia delle Entrate.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali affidamenti
Responsabile del servizio di conservazione e Produttore dei PdV	Agenzia delle Entrate Margherita Arcieri	Tutte le attività delegate dal Responsabile della Conservazione (Richiedente) Produzione dei pacchetti di versamento e trasferimento al sistema di conservazione	Dal 1° aprile 2024	Si avvale del sistema di conservazione e dei servizi ICT messi a disposizione dalla società Sogei S.p.A. regolato da specifico contratto.
Responsabile Sicurezza dei sistemi per la conservazione	Agenzia delle Entrate Giuseppe Buono	Definizione e attuazione delle policy di sicurezza	Dal 19 febbraio 2018	Si avvale del sistema di conservazione messo a disposizione dalla società Sogei S.p.A. regolato da specifico contratto

Tabella 2 – Ruoli e responsabilità

6. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

6.1 ORGANIZZAZIONE DEL SERVIZIO

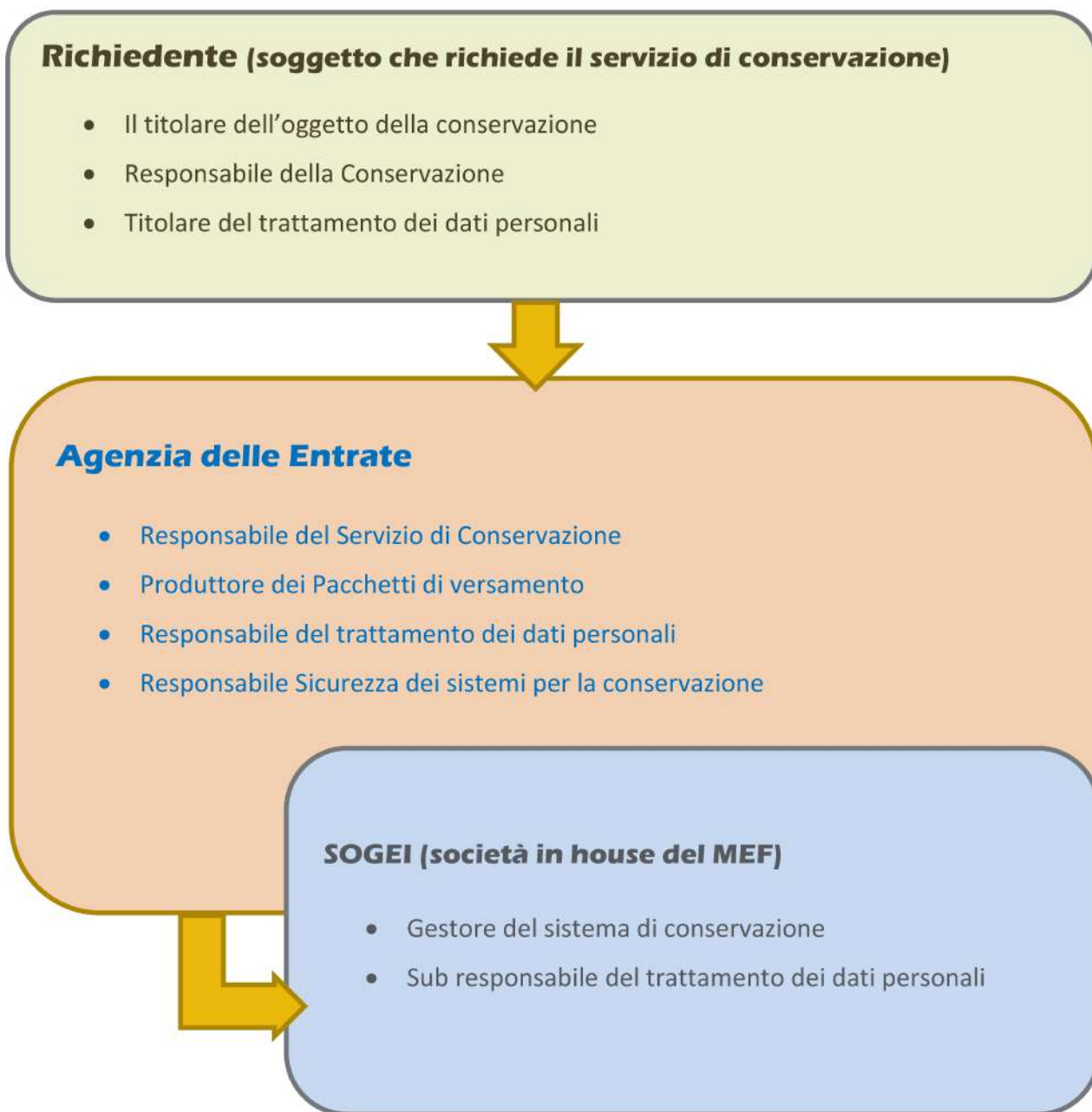


Figura 1 - Organizzazione del Servizio di conservazione

6.2 STRUTTURA ORGANIZZATIVA DELL'AGENZIA DELLE ENTRATE

Responsabile del Servizio di Conservazione

L'Agenzia delle Entrate, alla quale il Responsabile della Conservazione ha affidato la conservazione delle fatture elettroniche, individua nella propria organizzazione il Responsabile del servizio di conservazione che definisce ed attua le politiche complessive del sistema di conservazione e ne governa la gestione, in relazione al modello organizzativo descritto nel presente Manuale. L'Ufficio Reingegnerizzazione dei processi fornisce supporto al Responsabile del servizio di Conservazione nelle attività di governo, gestione e monitoraggio del sistema.

Responsabile della Sicurezza dei sistemi per la conservazione

Soggetto, persona fisica, dipendente dell'Agenzia, che assicura la definizione e l'attuazione delle policy, delle regole e delle procedure di sicurezza che devono essere implementate dalle strutture di competenza per la corretta conservazione, coerentemente con i requisiti stabiliti, avvalendosi di Sogei S.p.A in virtù dei rapporti contrattuali in essere.

Responsabile del trattamento dei dati personali

L'Agenzia delle Entrate assume il ruolo di Responsabile del trattamento dei dati personali necessario per lo svolgimento del servizio affidatogli tramite l'accordo di servizio, nel rispetto di tutte le norme previste dal Regolamento generale sulla protezione dei dati delle persone fisiche con riguardo al trattamento dei dati personali (Regolamento Europeo 2016/679 e D.Lgs 196/2003). L'Agenzia è autorizzata ad avvalersi di Sogei S.p.A in virtù dei rapporti contrattuali in essere quale proprio partner tecnologico.

7. OGGETTI DEL PROCESSO DI CONSERVAZIONE

7.1 OGGETTI CONSERVATI

Nell'ambito del servizio è applicato il procedimento di conservazione per i seguenti tipi di documenti:

- Fattura elettronica ordinaria (FatturaB2B o FatturaPA)
- Fattura elettronica semplificata (FatturaB2BS)

Di tali documenti sono previste le seguenti specificità:

- firmati digitalmente con certificato di firma elettronica qualificata rilasciato da un certificatore accreditato nelle modalità:

- CAdES-BES;
- XAdES-BES;
- firmati in formato CAdES con certificato di firma elettronica rilasciato dall'Agenzia delle Entrate;
- privi di firma.

I file fattura elettronica sono di formato XML con schema XSD pubblicato sul sito <https://www.fatturapa.gov.it/> "Fatturazione elettronica verso la Pubblica amministrazione".

Si precisa che la firma digitale è obbligatoria solo per le fatture elettroniche ordinarie verso la Pubblica Amministrazione, mentre per le altre la firma è opzionale.

I documenti eventualmente allegati alla fattura sono contenuti nell'apposito elemento previsto dalle specifiche tecniche incluso nello schema XML, codificati in formato base64Binary (RFC 2045): `<xs:element name="Attachment" type="xs:base64Binary" />`.

Il sistema di conservazione non controlla i formati originali di tali documenti codificati all'interno dei file fattura e non ne assicura la trasformazione in forme leggibili, ma garantisce l'integrità e l'immodificabilità dei dati così come codificati all'interno dei file fattura.

È il Responsabile della conservazione che deve garantire la leggibilità di tali allegati mantenendo validi e funzionanti nel tempo gli strumenti software utilizzati per la loro formazione o visualizzazione.

7.2 PACCHETTO DI VERSAMENTO

Il pacchetto di versamento – nel seguito **PdV** – è un pacchetto informativo organizzato secondo un formato predefinito, che contiene i documenti fattura inviati in conservazione dal produttore dei PdV, oltre ai relativi metadati ed all'indice.

Il PdV è generato automaticamente da appositi servizi di versamento, gestiti da SOGEI, che prelevano e organizzano i documenti fattura presenti nei sistemi di memorizzazione delle fatture elettroniche trasmesse e ricevute attraverso il Sistema di Interscambio e di quelle inviate in conservazione dal Responsabile della conservazione in modalità puntuale tramite il portale Fatture e Corrispettivi.

Ogni PdV può contenere esclusivamente documenti della stessa tipologia, ovvero della stessa Classe Documentale. In questo senso l'elenco dei metadati dei singoli documenti è omogeneo.

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

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

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

7.3 PACCHETTO DI ARCHIVIAZIONE

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

Il PdA è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma digitale.

Al fine di fornire data certa, sul pacchetto di archiviazione viene apposta una marcatura temporale contestualmente all'apposizione della firma digitale.

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

La struttura dell'IPdA è quella prevista dallo standard UNI 11386 - SInCRO (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali) di seguito rappresentato.

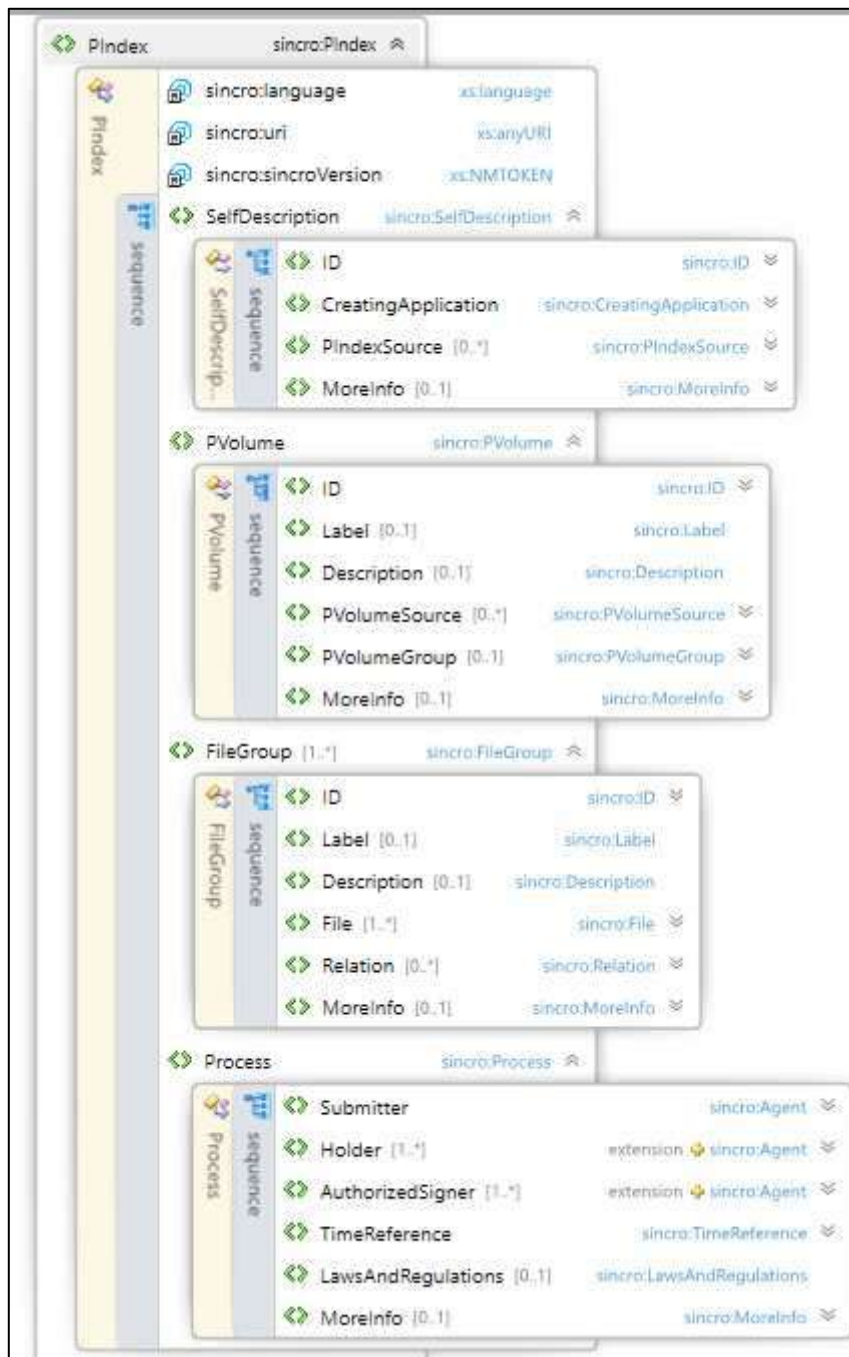


Figura 2 - Schema indice pacchetto di archiviazione

7.4 PACCHETTO DI DISTRIBUZIONE

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

Il PdD è un insieme di metadati e documenti generato dal sistema di conservazione in modo corrispondente alla richiesta di esibizione effettuata dall'utente.

Il PdD è un archivio compresso in formato .zip, firmato digitalmente dal "Gestore del sistema di conservazione", che contiene i seguenti elementi:

- indice del pacchetto di distribuzione – IPdD;
- la copia digitale dei file relativi ai documenti richiesti (in formato originale firmato o meno);
- il foglio di stile relativo allo schema XSD in base alla versione dei documenti richiesti;
- il file firmato relativo al PdA del documento (uno o più in base ai documenti oggetto della richiesta di esibizione);
- il file firmato della delega del Tecnico della conservazione che ha firmato il PdA del documento (uno o più).

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

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

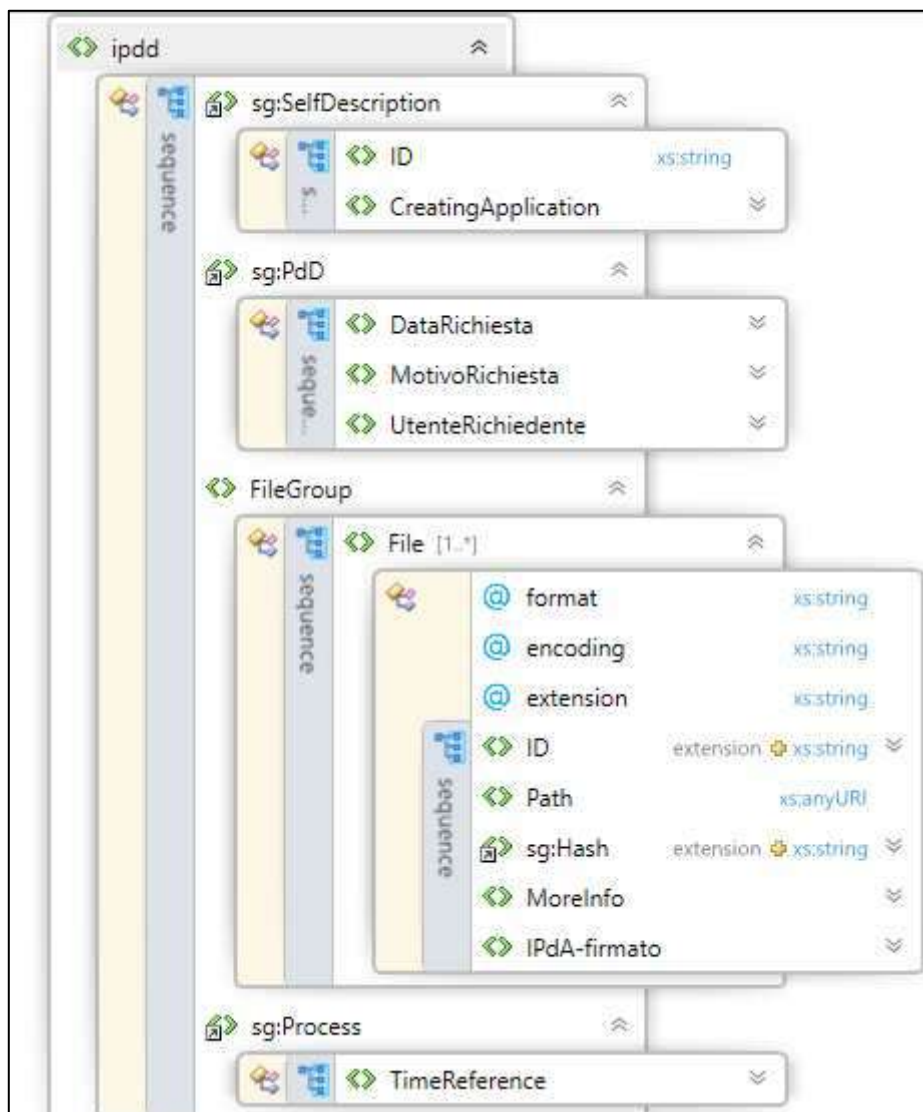


Figura 3 - Schema indice pacchetto di distribuzione

8. IL PROCESSO DI CONSERVAZIONE

La formazione del PdV è effettuata da appositi servizi ICT, gestiti da SOGEI, mediante il prelievo dei documenti dal sistema di memorizzazione e dal portale Fatture e Corrispettivi (inclusi i metadati), sulla base di un elenco di fatture elettroniche per le quali è prevista la conservazione, a seguito di adesione allo specifico accordo da parte di uno o entrambi i

soggetti coinvolti. Ad esito del processo di conservazione è inviato al sistema di memorizzazione un riscontro sulle fatture per le quali la conservazione ha avuto buon esito, per l'aggiornamento dello stato del singolo documento sul sistema di memorizzazione.

Il processo di conservazione si svolge secondo le fasi descritte di seguito:

1. **Ingestion dei documenti:** rappresenta la fase di ricezione del pacchetto di versamento da parte del sistema di conservazione.
2. **Presa in carico del PdV:** rappresenta la fase di presa in carico del pacchetto di versamento da parte del sistema di conservazione. In caso di esito positivo dei controlli formali, il PdV assume lo stato di "preso in carico" nel momento in cui viene prodotto il rapporto di versamento (RdV); in caso di esito negativo di almeno uno dei controlli formali il pacchetto di versamento non è preso in carico.
3. **Validazione del PdV:** rappresenta la fase di elaborazione del pacchetto di versamento da parte del sistema di conservazione per preparare i file per la successiva fase di assemblaggio ed archiviazione.
4. **Generazione del RdV:** rappresenta la fase in cui il sistema di conservazione, per ciascun PdV, genera il rapporto di versamento, in cui per ciascun documento indica l'esito dei controlli e, nel caso di mancato superamento, la motivazione del rifiuto.
5. **Assemblaggio dei PdA:** rappresenta la fase di assemblaggio dei documenti in pacchetti di archiviazione secondo le regole di archiviazione definite nel presente manuale.
6. **Firma digitale e marcatura temporale dei PdA:** rappresenta la fase di firma digitale e marcatura temporale dei pacchetti di archiviazione per attestare il corretto svolgimento del processo di conservazione e certificare la data dell'operazione di firma. La firma digitale e la marca temporale vengono apposte in modalità automatica, tramite un dispositivo HSM, dal "Gestore del sistema di conservazione" in virtù di una specifica delega.
7. **Archiviazione dei PdA:** rappresenta la fase di conservazione dei pacchetti di archiviazione che è l'ultima fase del processo di conservazione.
8. **Generazione del rapporto di conservazione:** rappresenta la fase in cui il sistema di conservazione, genera il rapporto di conservazione (RdC) giornaliero, in cui per ciascun documento viene indicato lo stato conservato e la data di conservazione.

8.1 MODALITÀ DI ACQUISIZIONE E CONTROLLO DELLE FATTURE ELETTRONICHE AI FINI DELLA CONSERVAZIONE

Le fatture elettroniche inviate al sistema di conservazione devono essere conformi alle specifiche tecniche pubblicate nella relativa sezione di “*Fattura elettronica e corrispettivi telematici*” del sito dell’Agenzia delle Entrate.

Sui file fattura vengono effettuati, tra gli altri, controlli relativi:

- al formato, rispetto allo schema XSD di riferimento;
- all’integrità della firma per i file firmati;
- alla dimensione massima consentita dei file.

La richiesta di conservazione delle fatture elettroniche viene effettuata dal Responsabile della conservazione tramite i servizi dell’Agenzia disponibili nella apposita area riservata del portale Fatture e Corrispettivi:

- con modalità implicita e automatica per tutte le fatture riferite al titolare soggetto IVA secondo quanto previsto dall’art.7 dell’accordo di servizio;
- con modalità puntuale, a seguito dell’upload per tutte le fatture riferite al titolare soggetto IVA secondo quanto previsto dall’art.6 dell’accordo di servizio.

Nel primo caso, se il file fattura trasmesso attraverso il Sistema di Interscambio supera i controlli di conformità alle specifiche tecniche, viene prodotta la ricevuta di consegna o di impossibilità di recapito, che, per i soggetti IVA che hanno aderito al servizio di conservazione, assume anche il valore di ricevuta di avvio del processo di conservazione.

Le fatture elettroniche, identificate in modo univoco e persistente, sono consultabili all’interno del portale “Fatture e Corrispettivi”.

Le fatture elettroniche o i loro duplicati informatici possono essere consultati e scaricati accedendo nella apposita area riservata del portale Fatture e Corrispettivi, con le modalità indicate nel provvedimento del Direttore dell’Agenzia delle entrate n. 433608 del 24 novembre 2022.

Nel secondo caso, le richieste di invio in conservazione delle fatture effettuate in modalità puntuale sono trattate secondo la normativa vigente in ambito di istanze alla Pubblica Amministrazione (DPR 445/2000), ovvero sono protocollate nel sistema di gestione documentale dell’Agenzia delle entrate.

Viene generata automaticamente per ciascun file fattura trasmesso tramite *upload* la relativa “*Richiesta di conservazione*” resa disponibile nell’apposita area riservata del portale Fatture e Corrispettivi.

Se il file fattura supera i controlli di conformità alle specifiche tecniche, viene prodotta una *Ricevuta di avvio del processo di conservazione*.

La *Ricevuta di avvio del processo di conservazione* contiene:

- il numero identificativo della *Richiesta di conservazione*;

- gli estremi del soggetto che ha effettuato la *Richiesta di conservazione*;
- l'elenco delle terne (Identificativo fattura, Nome file, Impronta) rappresentative di ciascun file fattura inviato in conservazione;
- la dicitura "*Si ricorda che la conservazione delle fatture in elenco sarà effettuata in occasione del primo evento di conservazione successivo alla data della presente comunicazione*".

La *Ricevuta di avvio del processo di conservazione* è registrata nel Sistema di gestione documentale dell'Agenzia delle entrate.

I documenti trasmessi con modalità puntuale, per i quali tutti i controlli hanno avuto esito positivo, sono depositati in un'area del portale Fatture e Corrispettivi in attesa del completamento del processo di conservazione.

8.2 MONITORAGGIO DELLE RICHIESTE DI CONSERVAZIONE E DEI DOCUMENTI CONSERVATI

Per le fatture inviate in modalità puntuale è disponibile nella apposita sezione all'interno delle interfacce web di fruizione dei servizi per i soggetti passivi IVA, l'elenco delle richieste di conservazione, indicante, per tutte le fatture, lo stato di conservazione (inviato in conservazione, presa in carico o conservato) o l'eventuale segnalazione di errore.

Per le fatture trasmesse attraverso il Sistema di Interscambio che superano i controlli di conformità alle specifiche tecniche, viene prodotta la ricevuta di consegna o di impossibilità di recapito, che, per i soggetti IVA che hanno aderito al servizio di conservazione, assume anche il valore di ricevuta di avvio del processo di conservazione.

8.3 PREPARAZIONE E GESTIONE DEL PACCHETTO DI VERSAMENTO

Il pacchetto di versamento (PdV) rappresenta lo strumento per l'invio dei documenti nel sistema di conservazione. In particolare, l'operazione di versamento consiste nella trasmissione al sistema di conservazione dei documenti da conservare e dei metadati che li identificano utilizzando il PdV.

I sistemi di accoglienza dell'Agenzia (il sistema di memorizzazione delle fatture elettroniche trasmesse attraverso il Sistema di Interscambio e l'interfaccia WEB per l'upload delle fatture elettroniche) consentono, tramite apposite funzionalità automatiche, di individuare i documenti che faranno parte dei pacchetti di versamento (PdV).

Il PdV contiene oltre ai documenti anche i relativi metadati, tramite i quali nelle fasi successive del processo di conservazione è possibile identificare univocamente le fatture permettendo di generare i pacchetti di archiviazione (PdA), in modo omogeneo rispetto al Responsabile della conservazione.

Tra i criteri di formazione del PdV sono presenti anche il tempo e la dimensione, per consentire una gestione ottimizzata del versamento nel sistema di conservazione.

I metadati dei documenti sono quelli specificati nel capitolo 11 "Specificità del servizio".

Nel PdV sono presenti le seguenti sezioni:

- anagrafica del PdV e codice;
- descrizione generale del sistema utilizzato dal produttore dei PdV per la formazione dei PdV;
- sezione dei file che contiene i dati del file, l'impronta (hash) e l'algoritmo di hash, i metadati;
- sezione del processo che contiene il riferimento del soggetto produttore del PdV e il riferimento temporale.

Il PdV è un file XML con schema XSD predefinito contenente:

- Data di disponibilità alla conservazione del documento
- Stato del documento
- Soglia temporale (limite temporale di permanenza dei documenti nell' 'area di attesa')
- Soglia numerica (limite numerico dei file contenuti nel PdV)
- Identificativo del PdV
- Identificativo del documento
- Servizio documentale
- Tipologia del documento
- Metadati del documento associati al servizio di conservazione
- Impronta (hash)
- Codifica impronta (algoritmo di calcolo)
- Formato
- Firma (quando presente)
- Identificativo di archiviazione nell'area di scambio del contenuto del documento
- Dati di descrizione generale del sistema utilizzato dal produttore dei PdV per la formazione del PdV (nome, versione, produttore software)
- Dati generali del soggetto produttore del PdV e del riferimento temporale presenti nella sezione di processo (ruolo, organizzazione, ragione sociale riferimento temporale, ecc.)

L'invio dei PdV al Sistema di conservazione prevede i seguenti passi:

1. Predisposizione dei documenti da conservare.
2. Generazione dell'indice del PdV (iPdV) secondo la struttura predefinita.
3. Richiamo dei servizi di versamento del sistema di conservazione.

Il servizio produttore dei PdV nel momento in cui richiama i servizi di versamento deve comunicare le seguenti informazioni:

- iPdV stringa relativa al file xml secondo la struttura predefinita;
- Impronta dell'iPdV e algoritmo di calcolo.

Il sistema di conservazione per ogni PdV inviato dal servizio produttore effettua i seguenti controlli:

- verifica abilitazione per l'invio del PdV;
- verifica conformità struttura iPdV allo schema di riferimento;
- verifica univocità riferimenti documentali all'interno del pacchetto;
- verifica corrispondenza tra il riferimento documentale dichiarato all'interno del pacchetto e quello presente nella destinazione nota e condivisa.

Se il PdV supera i controlli formali effettuati dal sistema di conservazione, viene accettato dal sistema di conservazione e preso in carico per la fase successiva del processo.

Se il PdV non supera i controlli formali effettuati dal sistema di conservazione, viene prodotto il *Rifiuto da parte del sistema di conservazione* e il processo di conservazione si interrompe. Nel caso di un archivio compresso contenente più file fatture, anche se solo alcuni file fattura non superano i controlli, sarà rifiutato l'intero archivio compresso.

Il *Rifiuto da parte del sistema di conservazione* contiene:

- il numero identificativo della *Richiesta di conservazione o della ricevuta di consegna o di impossibilità di recapito*;
- gli estremi del soggetto che ha effettuato la richiesta di invio in conservazione;
- l'elenco delle quintuple (Identificativo fattura¹, Nome file, Impronta, Motivo rifiuto, Azione) rappresentative di ciascun file fattura per cui è stato richiesto l'invio in conservazione.

I casi di rifiuto da parte del sistema di conservazione sono analizzati dal produttore dei PdV ai fini della risoluzione dei problemi riscontrati e del miglioramento del processo.

¹ L'identificativo univoco della fattura (idSdI) è attribuito dal Sistema di Interscambio in fase di accoglienza del file fattura, indipendentemente dal canale di trasmissione utilizzato per la trasmissione.

8.4 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE

Il sistema di conservazione genera i pacchetti di archiviazione, di seguito PdA, applicando le regole di assemblaggio dei documenti secondo i criteri definiti nel capitolo 11 “Specificità del servizio”.

L'organizzazione dei documenti nei PdA, in generale, può essere diversa dalla organizzazione dei documenti nei PdV poiché i criteri di assemblaggio sono specifici del sistema di conservazione.

Al fine di consentire una gestione ottimizzata dei processi di conservazione, vengono adottati criteri di assemblaggio basati sul tempo (frequenza di assemblaggio) e sulla dimensione (numero massimo di documenti contenuti in un PdA).

L'assemblaggio dei PdA avviene di norma al primo *evento di conservazione* utile; la frequenza di tale evento è indicata nelle caratteristiche specifiche del servizio al capitolo 11. Per i soli documenti trasmessi con modalità puntuale, a fronte di richieste di esibizione riferite a documenti presi in carico dal sistema di conservazione, ma non ancora conservati, viene forzato l'assemblaggio dei documenti e la conservazione per permettere di soddisfare l'operazione di esibizione.

I PdA sono numerati progressivamente nel sistema di conservazione.

I PdA sono sottoposti alla firma digitale da parte del gestore del sistema di conservazione.

La firma digitale del PdA è subordinata alla verifica dei poteri di firma del gestore del sistema di conservazione che possiede una specifica delega alla firma.

Contestualmente alla firma digitale del PdA è apposta automaticamente anche la marca temporale.

Il sistema di conservazione per ogni PdA generato e firmato effettua i seguenti controlli preliminari alla conservazione:

- Verifica integrità del PdA, tramite verifica della firma digitale e verifica validità del certificato alla data di firma.
- Verifica conformità struttura IPdA allo schema di riferimento.
- Verifica correttezza metadati.
- Verifica delle deleghe attive al momento della firma.

I PdA sono memorizzati nel dispositivo W.O.R.M. del sistema di conservazione ed il processo di conservazione è completato.

8.5 PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESIBIZIONE

Il sistema di conservazione prevede la predisposizione e gestione dei pacchetti di distribuzione ai fini dell'*esibizione*. In tal caso il PdD contiene i documenti richiesti, i riferimenti ad essi correlati e i PdA relativi ai documenti richiesti.

A seguito di una *Richiesta di esibizione* il sistema di conservazione fornisce la risposta generando uno o più pacchetti di distribuzione, in base al numero dei documenti richiesti, ovvero una notifica di scarto della richiesta.

Non sono possibili richieste di esibizione di fatture conservate con modalità automatiche (trasmesse o ricevute attraverso il sistema di interscambio SdI) che non si trovano ancora in stato di conservazione.

La richiesta di esibizione può essere effettuata solo dal Responsabile della conservazione o da un suo incaricato e deve essere corredata da una delle seguenti motivazioni:

- Accertamento da autorità preposte (per esempio Gdf, Agenzia delle entrate, INPS, altro Ente);
- Accertamento organi di controllo contabile;
- Richiesta per documentazione procedimenti giudiziari.

Le richieste di esibizione sono trattate secondo la normativa vigente in ambito di istanze alla Pubblica Amministrazione (DPR 445/2000).

L'utente può richiedere l'esibizione delle fatture selezionandole da una lista costruita sulla base di criteri di ricerca finalizzati all'individuazione puntuale dei documenti di interesse. La ricerca delle fatture da esibire può essere effettuata impostando uno o più dei seguenti parametri di ricerca:

- identificativi fiscali del Cedente Prestatore o del Cessionario Committente;
- identificativo SdI (per i file pervenuti dal Sistema di Interscambio laddove presente opportuno accordo di servizio);
- nome del file;
- data di ricezione del file a sistema.

I parametri di ricerca consentono all'utente di ricercare in particolare solo tra i file in cui egli figuri solo come Cedente Prestatore o solo come Cessionario Committente e di operare la ricerca anche sulle Partite Iva collegate, qualora presenti.

La ricerca produce come output una tabella nella quale, per ciascun file conservato o preso in carico che soddisfi i criteri di ricerca, sarà presente una riga contenente:

- informazioni sul tipo di provenienza del file (Sistema di Interscambio o caricamento manuale);
- l'identificativo SdI (nel caso di file provenienti dal Sistema di Interscambio);

- il numero fattura e la data della fattura nel caso di file contenenti una sola fattura;
- in caso di lotto di fatture (file contenenti più fatture) non viene riportato il dettaglio di numero e data fattura ma l'indicazione generica di "lotto fatture";
- la data di caricamento a sistema;
- gli identificativi fiscali, la Denominazione (o Nome e Cognome) del Cedente prestatore e del Cessionario Committente.

Ogni riga della tabella può essere selezionata (massimo 50 fatture) mediante pulsante di selezione e inserita in una lista di file, verificabile dall'utente, a partire dalla quale è possibile generare una richiesta di esibizione previo inserimento obbligatorio della motivazione della richiesta. Le motivazioni possibili sono le seguenti:

- Accertamento da autorità preposte (per esempio Gdf, Agenzia delle entrate, INPS, altro Ente);
- Accertamento organi di controllo contabile;
- Richiesta per documentazione procedimenti giudiziari.

Per ogni richiesta effettuata, è prodotta e messa a disposizione nell'area riservata del portale Fatture e Corrispettivi del Richiedente una ricevuta di presa in carico della richiesta di esibizione, protocollata nel sistema di gestione documentale dell'agenzia delle entrate, contenente almeno:

- identificativo univoco della richiesta;
- identificativo fiscale (codice fiscale/partita IVA) di chi l'ha formulata;
- nome di ciascun file oggetto della richiesta.

La generazione del pacchetto di distribuzione, contenente i documenti richiesti ovvero la notifica di scarto della richiesta, avviene con tempistiche differenti a seconda dei casi descritti nelle specificità del servizio al capitolo 11.

Il PdD può contenere un numero limite di cinque documenti; in base a tale numero, il sistema di conservazione genera uno o più PDD per soddisfare la richiesta.

Il sistema di conservazione effettua le seguenti attività:

- genera il PdD.
- Sottopone il PDD alla firma digitale da parte del gestore del sistema di conservazione.
- rende disponibile il PdD in un'area condivisa per il recupero dello stesso da parte del Responsabile della conservazione / Richiedente.

Il pacchetto di distribuzione o la notifica di scarto della richiesta rimangono a disposizione in un'apposita area, in attesa del loro prelevamento. Una volta scaricato, il pacchetto di distribuzione non sarà più disponibile per il prelevamento.

Il pacchetto di distribuzione contiene:

- l'indice del pacchetto iPDD;
- i documenti richiesti;
- i pacchetti di archiviazione dei documenti richiesti
- il file con le deleghe alla firma dei pacchetti di archiviazione.

Una descrizione completa del pacchetto di distribuzione è presente nel paragrafo 7.4.

8.6 PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE AI FINI DELL'ESPORTAZIONE

Il sistema di conservazione prevede la predisposizione automatica dei pacchetti di distribuzione ai fini *dell'esportazione a seguito della richiesta del Responsabile della conservazione / Richiedente*.

Nel caso di esportazione il sistema genera il pacchetto di distribuzione coincidente con il "pacchetto di archiviazione" come previsto dalla norma, ciò significa che in ciascun PDD è contenuto il PDA e tutti i suoi documenti, le deleghe e i fogli di stile.

Rispetto al PDD generato a fronte di una richiesta di esibizione, cambiano solo i contenuti, nel primo caso sono presenti solo i documenti richiesti, mentre nel secondo caso sono presenti tutti i documenti del PDA.

Il sistema di conservazione genera automaticamente un PDD per ciascun PDA presente nell'archivio del Responsabile della conservazione / Richiedente.

8.7 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE

Il sistema di conservazione produce i duplicati informatici dei documenti conservati nel momento in cui genera il pacchetto di distribuzione includendoli nello stesso pacchetto.

Tra le informazioni inserite nell'indice del pacchetto di distribuzione è presente l'impronta del file del documento conservato calcolata in fase di ricezione.

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

8.8 SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

Il sistema di conservazione prevede lo scarto dei pacchetti di archiviazione alla scadenza dei termini di conservazione previsti dall'accordo di servizio. L'attività è svolta dal Gestore del sistema di conservazione e dal Responsabile del servizio di conservazione.

Una volta che il pacchetto di archiviazione con le relative fatture elettroniche viene scartato, non è più fisicamente presente nell'archivio di conservazione e non è più possibile richiedere l'esibizione dei documenti.

8.9 ESPORTAZIONE DAL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione rende disponibili le funzionalità di supporto al processo di esportazione per la restituzione al Responsabile della conservazione, di tutti i contenuti conservati, le fatture elettroniche e i relativi PDA.

L'esportazione dal sistema di conservazione può essere richiesta sia in caso di recesso sia in caso di risoluzione dell'accordo di servizio, tramite i servizi disponibili nell'area riservata del portale Fatture e Corrispettivi.

Di seguito sono indicati i passaggi previsti dal processo di esportazione:

- Il Responsabile della conservazione, o un suo incaricato o delegato, effettua la richiesta preliminare di restituzione delle proprie fatture conservate.
- Viene fornito al richiedente la stima delle fatture già in conservazione o da conservare e la loro dimensione, indicando se il download può essere eseguito dal portale Fatture e Corrispettivi o tramite altri sistemi. Viene richiesta la conferma della procedura di esportazione.
- La richiesta di restituzione (a seguito di conferma) viene protocollata nel sistema di gestione documentale dell'Agenzia delle Entrate.
- Il sistema di conservazione, a partire dalle richieste di restituzione protocollate, provvede a:
 - o calcolare la previsione dimensionale rispetto a quanti pacchetti e documenti devono essere esportati e fornire l'informazione all'utente;
 - o selezionare dall'archivio di conservazione i pacchetti di archiviazione della partita IVA di riferimento;
 - o selezionare dall'archivio di conservazione i documenti fatture elettroniche in essi referenziate;
 - o inserire pacchetti di archiviazione e documenti in un'area temporanea del sistema;
 - o generare i pacchetti di distribuzione dei documenti con i contenuti stabiliti (PDD dei PDA) par. 8.6;
 - o apporre la firma digitale sui pacchetti di distribuzione in formato compresso (.zip)
 - o generare il registro di scarico e memorizzarlo nell'archivio recessi;

- trasferire i pacchetti di distribuzione e il registro di scarico nell'area temporanea del sistema.
- Il sistema di conservazione contrassegna i pacchetti di archiviazione ed i relativi documenti per i quali è stata chiesta la restituzione con l'opportuno stato ovvero con la cancellazione fisica dal sistema di conservazione.
- Il Responsabile della conservazione nel periodo di tempo stabilito effettua il download del/dei pacchetti di distribuzione e del registro di scarico dalla apposita sezione della propria area riservata del portale Fatture e Corrispettivi. Nel caso la quantità e le dimensioni delle fatture non siano gestibili dal portale verranno attivati procedure sicure per consentire il download dei dati.
- Il sistema di conservazione sposta in una area di obsolescenza la documentazione così contrassegnata in attesa della definitiva cancellazione dal sistema e aggiorna l'archivio di conservazione in modo da dismettere dal ciclo gestionale tali documenti.
- Il Titolare dell'oggetto di conservazione contestualmente alla conferma di recupero delle fatture, procede a richiedere la cancellazione delle stesse, che viene protocollata.
- In base a tale richiesta il sistema di conservazione provvede ad eliminare logicamente e fisicamente le fatture.

L'esportazione avviene in un formato che garantisce il rispetto dei modelli d'interoperabilità per la successiva eventuale importazione in altro sistema di conservazione a norma.

Durante il processo di esportazione e fino al download delle fatture, è possibile annullare la richiesta di cancellazione fatta, grazie alle funzionalità presenti sul portale Fatture e Corrispettivi. Qualora la richiesta di annullamento avvenga dopo la protocollazione della richiesta di esportazione, la stessa verrà protocollata all'interno del sistema di gestione documentale dell'Agenzia.

8.10 LE RICEVUTE DEL SISTEMA DI CONSERVAZIONE

Nel presente capitolo sono descritte le ricevute prodotte internamente al sistema di conservazione. Tali ricevute sono generate secondo strutture informative predefinite.

Sono generate, sigillate elettronicamente e messe a disposizione del Responsabile della conservazione e/o del produttore dei PdV per un periodo di tempo prestabilito in destinazione nota e condivisa con il sistema di conservazione.

Rapporto di versamento

Il rapporto di versamento – nel seguito RdV - è un pacchetto informativo generato dal sistema di conservazione al termine dei controlli di integrità del file e della verifica del formato effettuati dal sistema di conservazione sui singoli documenti contenuti in un pacchetto di versamento.

Ogni RdV si riferisce ad un pacchetto di versamento e riporta per ogni documento l'esito positivo o negativo delle verifiche effettuate, in questo ultimo caso riportando la motivazione dell'esito di rifiuto.

Il RdV è un'evidenza informatica, ovvero un file, che descrive l'esito delle verifiche effettuate sui documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

Rapporto di conservazione

Il rapporto di conservazione – nel seguito RdC - è un pacchetto informativo generato dal sistema di conservazione al termine della fase di conservazione dei documenti.

Il contenuto del RdC è formato in modo automatico e sottoscritto con firma elettronica dal sistema di conservazione che lo rende disponibile al produttore dei documenti – anche attraverso il produttore dei PdV – in una destinazione nota e condivisa con il sistema di conservazione.

Ogni RdC si riferisce ai pacchetti di archiviazione ed ai documenti conservati in una certa data e riporta per ogni documento la data di conservazione.

Il RdC è un'evidenza informatica, ovvero un file, che descrive l'esito conservazione e comunica le relative date di conservazione dei documenti che ne fanno parte attraverso l'uso di metadati. È in formato XML.

Registro di scarico per scarto ed esportazione

Il registro di scarico è un documento generato dal sistema di conservazione al termine della fase di scarto oppure al termine della fase di esportazione.

Il registro di scarico viene generato in formato PDF/A ed in formato strutturato (JSON) per eventuali utilizzi tecnici.

Il contenuto del registro è un riepilogo delle informazioni dei documenti e dei loro riferimenti nel sistema di conservazione.

Per ogni riga del registro che corrisponde alla singola fattura esportata / scartata dal sistema di conservazione sono riportate le seguenti informazioni:

- Identificativo documento fattura elettronica, così come assegnato dal sistema fatture e corrispettivi in fase di generazione / trasmissione della fattura;
- Nome file originale, nome del file fattura elettronica;
- Hash del documento, impronta del file calcolata dal sistema di conservazione in fase di versamento;
- Algoritmo hash del documento, algoritmo di generazione dell'impronta del file (es. SHA-256);
- Tipo firma documento, tipo firma del documento (es. CADES, XADES);
- Data conservazione, data in cui è stato conservato il documento;
- PDA, identificativo del pacchetto di archiviazione generato dal sistema di conservazione durante il processo di conservazione;
- Hash PDA, impronta del file calcolata dal sistema di conservazione;

- Algoritmo hash del PDA, algoritmo di generazione dell'impronta del file (es. SHA-256);
- Tipo firma PDA, tipo firma del file (es. CADES);
- PDV, identificativo del pacchetto di versamento generato dal sistema fatture e corrispettivi in fase di versamento in conservazione;
- RDV, identificativo del rapporto di versamento generato dal sistema di conservazione al termine dell'acquisizione del documento fattura elettronica;
- RDC, identificativo del rapporto di conservazione generato dal sistema di conservazione al termine del processo di conservazione del documento fattura elettronica.

Solo per i registri di scarico delle richieste di export sono presenti anche le seguenti informazioni:

- Identificativo della richiesta di esportazione;
- iPDD, identificativo del pacchetto di distribuzione generato a seguito della richiesta di esportazione delle fatture dal sistema di conservazione.

9. IL SISTEMA DI CONSERVAZIONE

Di seguito sono descritte le componenti del sistema di conservazione.

9.1 COMPONENTI LOGICHE

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

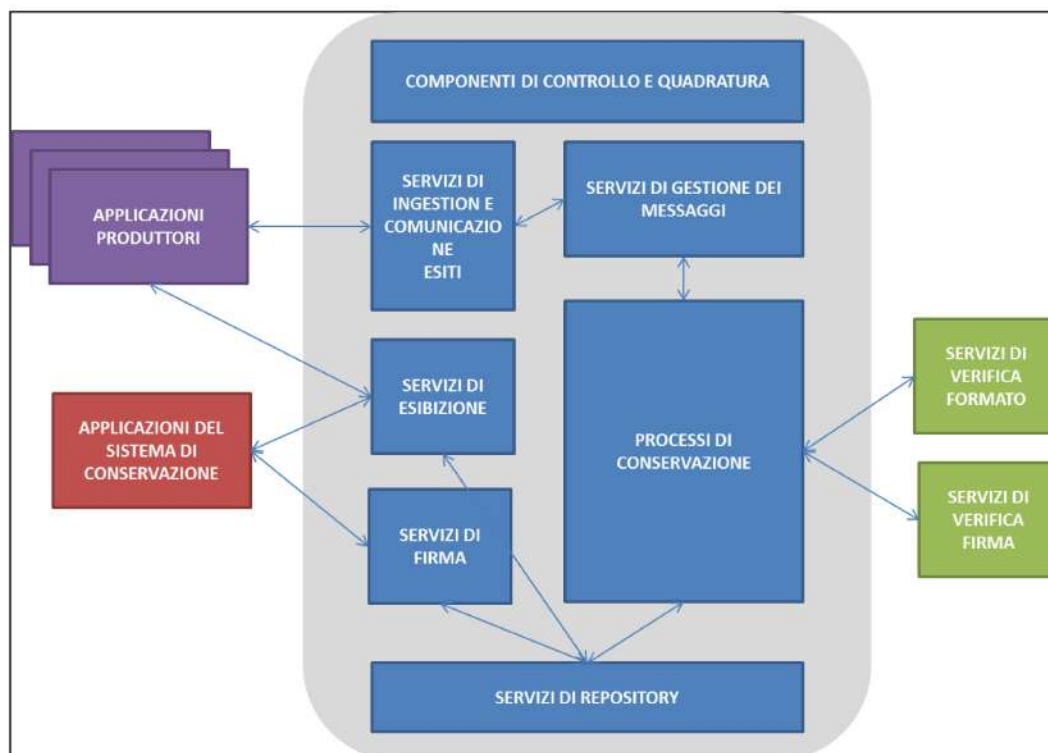


Figura 4 - Schema componenti logiche del Sistema di conservazione

- **Applicazioni produttori:** sono le applicazioni del sistema informativo che producono e inviano in conservazione i documenti.
- **Applicazioni del sistema di conservazione:** sono le applicazioni rese disponibili dal sistema di conservazione che forniscono le funzionalità di ricerca ed esibizione dei documenti conservati rivolte al responsabile della conservazione e relativi delegati.

- **Componenti di controllo e quadratura:** sono i componenti di monitoraggio operativo del sistema, sia automatici sia fruibili dagli utenti che fanno parte dell'infrastruttura organizzativa del Responsabile del servizio di conservazione.
- **Servizi di ingestione e comunicazione esiti:** sono i servizi esposti dal sistema di conservazione per la ricezione dei documenti da conservare e la comunicazione degli esiti da parte dei produttori.
- **Servizi di esibizione:** sono i servizi esposti dal sistema di conservazione per ottenere l'esibizione dei documenti conservati; tali servizi possono essere richiamati da applicazione del sistema informativo se previsto nel Manuale.
- **Servizi di firma:** sono i servizi esposti dal sistema di conservazione per la firma dei pacchetti di archiviazione dei documenti; tali servizi prevedono l'utilizzo di meccanismi automatici massivi per l'apposizione della firma digitale da parte degli utenti autorizzati.
- **Servizi di gestione dei messaggi:** sono i servizi che gestiscono le code di lavoro della fase di ingestione dei documenti.
- **Processi di conservazione:** sono i processi di back-end del sistema di conservazione che realizzano tutte le funzionalità del processo di conservazione. Supportano anche il processo di generazione delle deleghe alla firma dei pacchetti di archiviazione.
- **Servizi di repository:** sono i servizi che realizzano le funzionalità di tipo dati per gli archivi operazionali, temporanei, documentali e W.O.R.M. utilizzati dal sistema di conservazione.
- **Servizi di verifica formato:** sono servizi esterni al sistema di conservazione che permettono la verifica del formato dei documenti da conservare per garantire la coerenza con i formati previsti dalla normativa.
- **Servizi di verifica firma:** sono servizi esterni al sistema di conservazione che permettono la verifica della firma e del certificato di firma dei documenti da conservare per garantire le caratteristiche di integrità ed autenticità.

9.2 RIVERSAMENTO DIGITALE

I documenti conservati su supporti W.O.R.M. idonei a garantire la conformità agli originali vengono riprodotti mediante due tipologie di riversamento, *diretto* e *digitale*.

Il riversamento *diretto* consente il trasferimento di uno o più documenti conservati da un supporto di memorizzazione a un altro, senza modificare la rappresentazione informatica.

Il riversamento *digitale* viceversa prevede il trasferimento di uno o più documenti conservati da un supporto di memorizzazione a un altro, con la modifica della rappresentazione informatica del contenuto. Si tratta, in questo caso, di un aggiornamento tecnologico

dell'archivio informatico, in quanto, ad esempio, non risulta essere più conveniente mantenere nel tempo il formato di rappresentazione digitale dei documenti originariamente conservati.

Il flusso operativo del riversamento *digitale* si conclude con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti, del riferimento temporale e della firma digitale da parte del Responsabile Operativo o di suoi incaricati.

10. MONITORAGGIO E CONTROLLI

10.1 PROCEDURE DI MONITORAGGIO

Di seguito sono descritte le principali tipologie di monitoraggio previste per il sistema di conservazione in termini qualitativi e quantitativi:

- monitoraggio funzionale, per verificare il corretto svolgimento del processo di conservazione in base alle seguenti fasi:
 - o ingestion dei documenti;
 - o acquisizione dei documenti;
 - o firma dei pacchetti di archiviazione;
 - o conservazione dei documenti.
- monitoraggio operativo, che ha l'obiettivo di tenere sotto controllo le fasi di acquisizione, assemblaggio nei pacchetti di archiviazione, apposizione della firma digitale e conservazione dei documenti.

10.2 VERIFICA DELL'INTEGRITÀ DEGLI ARCHIVI

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

- Calcolo dell'impronta e confronto con l'ultima memorizzata.
- Verifica della firma e della marca temporale.
- Verifica del formato.

Ciascuna delle tipologie di verifica è effettuata da un apposito componente di sistema che effettua la verifica secondo i seguenti criteri:

- Il periodo, dalla data _____ alla data _____.
- Il servizio di conservazione.
- Il formato del documento.
- Il tipo documento / classe documentale.

L'esecuzione delle verifiche è registrata nell'archivio degli audit periodici del sistema di conservazione con il relativo esito.

10.3 ACCESSO AI DATI E INTEGRITÀ

Di seguito sono descritte le principali misure di *sicurezza logica* predisposte per il controllo degli accessi alle applicazioni del sistema di conservazione.

In relazione alla funzionalità per la firma dei pacchetti di archiviazione:

- L'autenticazione è svolta dall'infrastruttura di sicurezza del Sistema dell'Agenzia delle entrate e consiste nella verifica delle credenziali.
- L'autorizzazione alla firma dei pacchetti di archiviazione viene effettuata tramite l'identità dell'utente ed applica le ACL attribuite ai pacchetti di archiviazione in fase di firma.
- L'applicazione prevede diversi profili di autorizzazione, gestiti ed assegnati agli utenti.
- L'autorizzazione alla firma digitale dei pacchetti di archiviazione è in carico all'applicazione, che verifica che l'utente sia autorizzato.
- La riservatezza è assicurata dall'uso delle funzionalità di cifratura del canale di comunicazione messe a disposizione dal protocollo TLS/SSL.

In relazione agli applicativi produttori dei PdV:

- L'autenticazione dell'applicazione produttrice dei PdV che richiede la conservazione dei documenti prevede la firma della richiesta SOAP.
- L'autorizzazione all'uso del servizio di ingestion è effettuata applicativamente.
- La riservatezza dei documenti oggetto di acquisizione è assicurata dall'uso delle funzionalità di cifratura del canale di comunicazione messe a disposizione dal protocollo TLS/SSL.
- L'integrità e l'autenticità dei PdV ricevuti sono assicurate dall'uso del meccanismo di firma delle richieste previsto per l'autenticazione.

10.4 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE

Le anomalie che possono manifestarsi nel corso dell'esecuzione del processo di conservazione sono classificabili in macro-tipologie, per ciascuna delle quali sono effettuate azioni specifiche.

Ambito	Anomalia	Azione	Responsabile
Oggetti conservati	Documenti non conservabili	Verifica con il produttore dei PdV ed eventuale rifiuto dal sistema di conservazione	Responsabile del servizio di conservazione
Sistemi / infrastruttura	Indisponibilità / malfunzionamenti di sistema	Verifica interna	Gestore del sistema di conservazione
Software del sistema di conservazione	Errori del software di conservazione / esibizione	Attivazione di correttiva secondo le procedure aziendali	Responsabile del servizio di conservazione
Livelli di servizio	Mancato rispetto dei livelli di servizio definiti	In dipendenza della problematica	Responsabile del servizio di conservazione
Sicurezza logica	Incidente di sicurezza (malware, accesso ai dati non autorizzato, ...)	Gestione dell'incidente, adozione di contromisure e ripristino dei sistemi	Gestore del sistema di conservazione

Tabella 3 - Azioni specifiche in caso di anomalie

11. SPECIFICITÀ DEL SERVIZIO

Il Responsabile della conservazione, può fruire del servizio di conservazione messo a disposizione dall'Agenzia delle entrate, attraverso accesso autenticato all'area riservata del portale Fatture e Corrispettivi anche per tramite di un suo incaricato o delegato.

11.1 SERVIZIO DI CONSERVAZIONE - MODALITÀ E TEMPI DI EROGAZIONE

Di seguito vengono indicati i tempi di risposta per le varie fasi di processo

Fase del processo	Descrizione	Tempi
Presa in carico delle fatture elettroniche inviate in conservazione in modalità puntuale	<i>Restituzione della "Ricevuta di avvio del processo di conservazione" che attesta l'avvenuta presa in carico da parte del sistema di conservazione, ovvero un "Rifiuto da parte del sistema di conservazione" nel caso di mancata presa in carico.</i>	Entro 72 ore - al netto dei giorni festivi - dalla ricezione di una "Richiesta di conservazione" di fatture effettuata manualmente dal Richiedente.
Presa in carico delle fatture elettroniche trasmesse attraverso il Sistema di Interscambio	<i>Restituzione della ricevuta di consegna o di impossibilità di recapito</i>	Entro 5 giorni – al netto dei giorni festivi – dalla trasmissione.
Richiesta di esibizione	<i>Richiesta di esibizione delle fatture elettroniche già conservate</i>	Entro 48 ore - al netto dei giorni festivi - dalla data di ricezione della "Richiesta di esibizione"
	<i>Richiesta di esibizione delle fatture elettroniche inviate in conservazione in modalità puntuale, prese in carico e non ancora conservate</i>	Entro 12 giorni - al netto dei giorni festivi - dalla data di ricezione della "Richiesta di esibizione"
	<i>Richiesta di esibizione delle fatture elettroniche trasmesse attraverso il Sistema di Interscambio e non ancora conservate</i>	La richiesta non può essere effettuata; potrà essere riproposta a valle del completamento del processo di conservazione
Disponibilità dei pacchetti di distribuzione	<i>Disponibilità dei pacchetti di distribuzione o delle comunicazioni di anomalia della richiesta</i>	20 giorni a partire dalla data di disponibilità dei pacchetti di distribuzione o di comunicazione dell'anomalia
Scarto dei documenti	<i>Scarto automatico delle fatture</i>	15 anni a partire dalla messa in conservazione delle fatture, salvo che il Richiedente, per comprovata necessità, non ne chieda una proroga
Richiesta esportazione	<i>Richiesta di esportazione delle fatture elettroniche presenti nel Sistema di Conservazione o in attesa dell'avvio del processo di conservazione</i>	In base allo stato delle fatture (conservate, in attesa di conservazione) viene generata apposita comunicazione con indicazione dei tempi per la disponibilità al download dei dati

Tabella 4 - Modalità e tempi di erogazione del servizio

Le tempistiche indicate nella tabella precedente potranno subire variazioni in aumento, in caso di attività programmate di manutenzione del sistema o di picchi di gestione non prevedibili.

11.2 DURATA DELLA CONSERVAZIONE

Secondo quanto previsto dall'accordo di servizio, le fatture elettroniche saranno conservate per 15 anni dalla data di avvio del processo di conservazione, anche in caso di recesso o risoluzione effettuato dal Titolare dell'oggetto della conservazione o per il tramite di un suo incaricato. Nel caso di recesso o risoluzione con richiesta di export, le fatture restano comunque conservate per 15 anni qualora il Titolare dell'oggetto della conservazione, non confermi la cancellazione delle fatture restituite, a valle della quale le fatture saranno definitivamente eliminate dal sistema di conservazione dell'Agenzia e non potranno più essere esibite.

11.3 SCHEDA RIEPILOGATIVA DEL SERVIZIO

Le seguenti tabelle riassumono le caratteristiche e gli attributi del servizio di conservazione Fatturazione elettronica D.Lgs. 127/2015".

11.3.1 GENERALITÀ DEL SERVIZIO

Di seguito vengono riportate le caratteristiche generali del servizio di conservazione:

Generalità del servizio: FATTURAZIONE ELETTRONICA D.Lgs. 127/2015		
Attributo	Descrizione	Contenuto
Nome del servizio	Descrizione del servizio	FATTURAZIONE ELETTRONICA D.Lgs. 127/2015
Titolare dell'oggetto della conservazione	Soggetto titolare e produttore dei documenti da conservare	PIVA aderente al servizio.
	Codice fiscale	Codice fiscale
	Cognome Nome /Denominazione	Cognome Nome /Denominazione
Aderente all'accordo di servizio	Codice fiscale	È il Codice fiscale dell'aderente all'accordo di servizio o del soggetto che agisce per conto del titolare dell'oggetto della conservazione
	Cognome Nome	È il Cognome Nome dell'aderente all'accordo di servizio, o del soggetto

Generalità del servizio: FATTURAZIONE ELETTRONICA D.Lgs. 127/2015		
Attributo	Descrizione	Contenuto
		che agisce per conto del titolare dell'oggetto conservazione
Responsabile del servizio di conservazione	Nome responsabile Agenzia Entrate	È il nome del Responsabile del servizio di conservazione
	Cognome responsabile Agenzia Entrate	È il cognome del Responsabile del servizio di conservazione
Rilevanza fini tributari	Indica se il Servizio di conservazione contiene documenti rilevanti ai fini tributari	SI

Tabella 5 - Generalità del servizio

11.3.2 SPECIFICITÀ DEL SERVIZIO

Di seguito vengono riportate le caratteristiche specifiche del servizio di conservazione:

Specificità del servizio: "FATTURAZIONE ELETTRONICA D.Lgs. 127/2015"		
Caratteristica	Descrizione	Regola
Dimensione pacchetti di archiviazione	Indica il numero di documenti in un pacchetto di archiviazione in base ai volumi	1.000
Frequenza assemblaggio	Indica la frequenza con cui i documenti da conservare sono assemblati in pacchetti di archiviazione	Semestrale (o in occasione di richieste di esibizione riferiti a documenti conservati con modalità puntuale, presi in carico, ma ancora non conservati)
Apposizione Marcatura temporale	Indica se per il servizio è richiesta apposizione della marcatura temporale dei pacchetti di archiviazione	SI
Documenti Tributari	Indica se il documento è rilevante ai fini tributari	SI

Tabella 6 - Specificità del servizio

11.3.3 METADATI DEL DOCUMENTO

La tabella di seguito rappresenta l'elenco dei metadati previsti dalle linee guida di AgiD per il documento Fattura elettronica.

Si precisa che:

- per le fatture emesse precedentemente al 1° luglio 2018 non sono presenti i metadati minimi ad eccezione del "Identificativo" e non sono presenti gli altri metadati di Tabella 4;
- per le fatture transitate per il Sistema Di Interscambio (SDI) emesse precedentemente al 1° luglio 2022 e per le fatture inviate in conservazione in modalità puntuale prima del 1° dicembre 2022, sono valorizzati i soli campi previsti dalla precedente versione delle linee guida.

Metadati del documento: "Fattura elettronica"				
Metadato	Campi	Sottocampi	Descrizione	Regola
IdDoc	Impronta crittografica del documento	Impronta	Impronta del documento	È l'hash del file calcolato dal Sistema di Interscambio
		Algoritmo	SHA-256	
	Identificativo		È l'identificativo univoco assegnato dal Sdl o dal Portale Fatture e Corrispettivi	
Modalità di formazione			Modalità di formazione a): "creazione tramite utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti in allegato 2"	

Metadati del documento: "Fattura elettronica"				
Metadato	Campi	Sottocampi	Descrizione	Regola
Tipologia documentale			Fattura Elettronica	È un parametro di assemblaggio dei PdA; sono costituiti da pacchetti di archiviazione omogenei per classe documentale
Dati di registrazione	Tipologia di flusso		Tipologia di flusso in entrata: "E"	
	Tipo registro		Nessuno	
	Data registrazione		Data e ora di registrazione su documentale	È l'informazione contenente data e ora con riferimento al tempo universale coordinato (UTC), generato dal sistema documentale al momento dell'archiviazione del file fattura accettato dal Sistema di Interscambio
	Numero documento		Numero di registrazione del documento generato dal Sistema documentale dell'Agenzia	Il documento viene registrato ad esempio 1634293/2018

Metadati del documento: "Fattura elettronica"				
Metadato	Campi	Sottocampi	Descrizione	Regola
	Codice del Registro		N/A	N/A
Soggetti	Ruolo		<u>SOGGETTO CHE EFFETTUA LA REGISTRAZIONE</u>	Il sistema SdI gestito dall'Agenzia delle entrate
	Tipo soggetto		PG	
	-	Denominazione Organizzazione	Agenzia delle entrate	
	-	Codice fiscale / Partita Iva	CF dell'Agenzia delle entrate	
	Ruolo		<u>ALTRO</u>	Dati del soggetto titolare dell'accordo di servizio
	Tipo soggetto		PG / PAI	
	-	Codice fiscale / Partita Iva	Partita Iva (è un parametro utilizzato per la generazione dei PdA)	Se PG / PAI
	-	Denominazione	Denominazione	Se PG

Metadati del documento: "Fattura elettronica"				
Metadato	Campi	Sottocampi	Descrizione	Regola
	-	Denominazione Amministrazione / Codice IPA	Denominazione Amministrazione	Se PAI
	Ruolo		<u>DESTINATARIO</u>	Cessionario / Committente
	Tipo soggetto		PG / PF / PAI / PAE	
	-	Codice fiscale / Partita Iva	per PF il campo è valorizzato con il CF	Se PF
			per PAI, PAE o PG il campo è valorizzato con la Partita Iva se è presente, altrimenti con il CF	Se PAI, PAE o PG
	-	Denominazione	Denominazione	Se PG
	-	Cognome	Cognome	Se PF
	-	Nome	Nome	Se PF
	-	Denominazione Amministrazione / Codice IPA	Denominazione Amministrazione	Se PAI o PAE

Metadati del documento: "Fattura elettronica"				
Metadato	Campi	Sottocampi	Descrizione	Regola
	Ruolo		<u>MITTENTE</u>	Cedente / Prestatore
	Tipo soggetto		PG	Il mittente potrebbe essere un soggetto PG o anche PAI, ma non è possibile identificare in alcun modo la tipologia di soggetto dalle informazioni contenute in fattura; si è scelto quindi di valorizzare tale campo sempre come PG (organizzazione)
	-	Denominazione	Denominazione Amministrazione / Denominazione	Se PAI e PG
	-	Codice fiscale / Partita Iva	Partita IVA	Se PAI e PG

Metadati del documento: "Fattura elettronica"				
Metadato	Campi	Sottocampi	Descrizione	Regola
Chiave descrittiva	Oggetto		È l'oggetto del documento	CONCATENAZIONE DI: id SdI - data accoglienza - CF/P.Iva Cedente - CF/P.Iva Cessionario - numero delle fatture contenute nel file XML
Allegati	Numero allegati		0	Le fatture elettroniche non hanno allegati esterni al file fattura XML
	Indice allegati		N/A	
	-	IdDoc	N/A	
	-	Descrizione	N/A	
Riservato			FALSO	

Metadati del documento: "Fattura elettronica"				
Metadato	Campi	Sottocampi	Descrizione	Regola
Identificativo del formato	Formato		È il formato della fattura	Il campo è valorizzato con la versione XSD di riferimento di quando è stata emessa la fattura
	Prodotto Software			Non rilevabile
	-	Nome prodotto	N/A	
	-	Versione	N/A	
	-	Produttore	N/A	
Verifica	Firmato Digitalmente		Impostato con vero se la fattura è firmata digitalmente, altrimenti falso	
	Sigillato elettronicamente		Impostato con vero se la fattura è sigillata elettronicamente, altrimenti falso	
	Marcatura Temporale		FALSO	
	Conformità copie immagine su supporto informatico		FALSO	
Nome del documento			Nome del file fattura XML	
Versione del documento			1	Esiste solo una versione di file fattura conservato

Metadati del documento: "Fattura elettronica"				
Metadato	Campi	Sottocampi	Descrizione	Regola
Tracciateure modifiche documento	Tipo modifica		N/A	
	Soggetto autore della modifica		N/A	
	Data e ora modifica		N/A	
	IdDoc versione precedente		N/A	
Tempo di conservazione			15	
Note			Note	

Tabella 7 - Metadati del documento

11.3.4 METADATI AGGIUNTIVI DEL DOCUMENTO

La seguente tabella contiene ulteriori metadati associati al documento "Fattura elettronica":

Metadati aggiuntivi del documento: "Fattura elettronica"		
Metadato	Descrizione	Regola
Soggetto trasmittente	<i>Codice fiscale del soggetto trasmittente</i>	La fattura elettronica è trasmessa al Sistema di Interscambio dal soggetto obbligato ad emetterla; la fattura elettronica può essere trasmessa, per conto del soggetto obbligato ad emetterla, da un intermediario
Canale di trasmissione	<i>Descrizione in base ai canali previsti</i>	È il canale tramite il quale è trasmessa la fattura elettronica al Sistema di Interscambio
Data ricezione SdI	<i>Data accoglienza nel sistema SdI</i>	È l'informazione contenente data e ora con riferimento al tempo universale coordinato (UTC), generato dal Sistema di Interscambio per i documenti che vengono accettati dal sistema di accoglienza

Tabella 8 - Metadati aggiuntivi del documento