

Manuale della Conservazione di InfoCert S.p.A.

Società soggetta a direzione e controllo di
Tecnoinvestimenti S.p.A.

REGISTRO DELLE VERSIONI

N° versione	Data emissione	Modifiche apportate	Osservazioni
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	

INDICE DEL DOCUMENTO

1.	SCOPO E AMBITO DEL DOCUMENTO	5
2.	TERMINOLOGIA (GLOSSARIO, ACRONIMI).....	5
3.	NORMATIVA E STANDARD DI RIFERIMENTO	13
3.1	Normativa di riferimento.....	13
3.2	Standard di riferimento.....	15
3.3	Procedure aziendali interne	16
4.	RUOLI E RESPONSABILITÀ	17
5.	STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	21
5.1	Profilo di InfoCert	21
5.2	Organigramma.....	24
5.3	Strutture organizzative	24
6.	OGGETTI SOTTOPOSTI A CONSERVAZIONE.....	27
6.1	Oggetti conservati	28
6.2	Pacchetto di versamento.....	31
6.3	Pacchetto di archiviazione.....	32
6.4	Pacchetto di distribuzione	33
7.	IL PROCESSO DI CONSERVAZIONE	34
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	36
7.2	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti	37
7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	38
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie	39
7.5	Preparazione e gestione del pacchetto di archiviazione	40
7.6	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione	42
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	44
7.8	Scarto dei pacchetti di archiviazione.....	45
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori.....	46
8.	IL SISTEMA DI CONSERVAZIONE.....	47
8.1	Componenti Logiche	49
8.2	Componenti Tecnologiche.....	49

8.2.1	Firewall.....	49
8.2.2	Back-up	50
8.2.3	Servizio di marcatura temporale	50
8.2.4	Posta Elettronica Certificata.....	50
8.3	Componenti Fisiche.....	51
8.3.1	Dispositivo HSM di firma digitale	51
8.3.2	Sistema Storage	51
8.3.3	Sincronizzazione dei sistemi	52
8.4	Procedure di gestione e di evoluzione.....	53
8.4.1	Criteri di organizzazione del contenuto	53
8.4.2	Organizzazione dei supporti.....	54
8.4.3	Archivio dei viewer consegnati dal Soggetto Produttore.....	54
8.4.4	Archivio dell'hardware e del software obsoleto	55
9.	MONITORAGGIO E CONTROLLI.....	56
9.1	Procedure di monitoraggio	58
9.1.1	Processi di monitoraggio del sistema di conservazione	59
9.1.2	Monitoring della disponibilità del sistema.....	59
9.2	Verifica dell'integrità degli archivi	60
9.3	Controlli	62
9.3.1	Controlli di versamento	62
9.3.2	Controlli di processo di progettazione e sviluppo dei servizi	63
9.3.3	Monitoraggio e registrazioni durante il ciclo produttivo	63
9.3.4	Monitoraggio e registrazioni per collaudo finale	64
9.3.5	Controlli periodici	64
9.4	Soluzioni adottate in caso di anomalie	64
9.4.1	Auditing generale del sistema	65
9.4.2	Incident management	66

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale della Conservazione di InfoCert S.p.A. (Società soggetta a direzione e controllo di Tecnoinvestimenti S.p.A.), ai sensi del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005 pubblicato in GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20.

Il Manuale della Conservazione illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

In caso di ispezione da parte delle autorità di vigilanza preposte, il Manuale della Conservazione permette un agevole svolgimento di tutte le attività di controllo.

[Torna al sommario](#)

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

ACCESSO	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
ACCREDITAMENTO	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione.
AFFIDABILITA'	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
AGGREGAZIONE DOCUMENTALE INFORMATICA	Aggregazione di documenti informatici o 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.
ARCHIVIAZIONE	Processo di trattamento e gestione dei documenti di uso

	corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.
AGID	Agenzia per l'Italia Digitale.
ARCHIVIO	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un Soggetto Produttore durante lo svolgimento dell'attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
AREA ORGANIZZATIVA OMOGENEA	Insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.
ASP	Application Service Provider.
ATTESTAZIONE DI CONFORMITA' 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.
AUTENTICITA'	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
BASE DATI	Collezione di dati registrati e correlati tra loro.
CA	Certification Authority.
CAD	Codice Amministrazione Digitale D.lgs. 82 del 7 marzo 2005 e successive modifiche.
CAS	Content Addressed Storage.
CONSERVATORE ACCREDITATO	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

CICLO DI GESTIONE	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
CLASSIFICAZIONE	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici titoli e classi.
CODICE (DELL'AMMINISTRAZIONE DIGITALE)	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
CODICE ESEGUIBILE	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
CONSERVATORE ACCREDITATO	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia Digitale.
CONSERVAZIONE	La conservazione dei documenti e dei fascicoli informatici, disciplinata dal DPCM 3 dicembre 2013, è l'attività volta a proteggere e mantenere nel tempo gli archivi di documenti e dati informatici. Il suo obiettivo primario è di impedire la perdita o la distruzione non autorizzata dei documenti e di mantenere nel tempo le loro caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.
COPIA ANALOGICA DI UN DOCUMENTO INFORMATICO	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
COPIA DI SICUREZZA	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 del DPCM del 3 dicembre 2013.
DATI SENSIBILI	Ai sensi dell'articolo 4, comma 1, lettera d) del Decreto Legislativo 30 giugno 2003, n.196 e la seguente deliberazione del Consiglio dei Ministri del 25 maggio 2012, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere filosofico,

	politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
D. LGS	Decreto Legislativo.
DPCM	Decreto della Presidenza del Consiglio dei Ministri.
DPR	Decreto del Presidente della Repubblica.
DOCUMENTO ANALOGICO	Rappresentazione analogica di atti, fatti o dati giuridicamente rilevanti.
DOCUMENTO INFORMATICO	Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
ESIBIZIONE	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
EVIDENZA INFORMATICA	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
EXTENSIBLE MARKUP LANGUAGE	Linguaggio derivato dall'SGML (Standard Generalized Markup Language), metalinguaggio che permette di creare altri linguaggi. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags).
FASCICOLO INFORMATICO	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
FIRMA DIGITALE	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1 comma 1 lettera s) Decreto Legislativo del 7 marzo 2005 n. 82).
FIRMA ELETTRONICA	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici,

	utilizzati come metodo di identificazione informatica (art. 1 comma 1 lettera q) Decreto Legislativo del 7 marzo 2005 n. 82).
FIRMA ELETTRONICA QUALIFICATA	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1 comma 1 lettera r) Decreto Legislativo del 7 marzo 2005 n. 82).
FIRMA ELETTRONICA AVANZATA	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1 comma 1 lettera q-bis) Decreto Legislativo del 7 marzo 2005 n. 82). Si vedano anche le regole tecniche, pubblicate nella G.U. il 21 maggio 2013.
FORMATO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
GU	Gazzetta Ufficiale della Repubblica Italiana.
HSM	Hardware Security Module.
IDENTIFICATIVO UNIVOCO (di seguito detto Token)	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione. Detto anche token LegalDoc.
IMMODIFICABILITA'	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 DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
I.N.R.I.M	Istituto Nazionale di Ricerca Metrologica.

INSIEME MINIMO DI METADATI DOCUMENTO INFORMATICO	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM del 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
INTEGRITA'	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
INTEROPERABILITA'	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
LEGALDOC	Servizio di conservazione digitale a norma di InfoCert.
LEGGIBILITA'	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
MARCA TEMPORALE	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (art. 1, lettera m del DPCM 22 febbraio 2013). La marca temporale emessa in conformità con quanto previsto dal DPCM 22 febbraio 2013, titolo IV è opponibile ai terzi ai sensi dell'art. 41 dello stesso decreto.
MEF	Ministero dell'Economia e delle Finanze.
METADATI	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM del 3 dicembre 2013.
NTP	Network Time Protocol.
OAIS	Open Archival Information System: è lo standard ISO 14721:2003 e definisce concetti, modelli e funzionalità inerenti agli archivi digitali e gli aspetti di digital preservation.
PACCHETTO INFORMATIVO	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.
PORTABLE DOCUMENT	Formato di file creato da Adobe Systems nel 1993 per lo

FORMAT	<p>scambio di documenti. Il PDF è un formato a schema fisso basato su un linguaggio di descrizione di pagina che permette di rappresentare documenti in modo indipendente dall'hardware, dal software e dal sistema operativo; ogni PDF incapsula una descrizione completa del documento, che include testo, caratteri, immagini e grafica.</p> <p>PDF è uno standard aperto; recentemente la versione PDF/A (PDF Reference Version 1.4) è stata riconosciuta dall'International Organization for Standardization (ISO) con la norma ISO 19005:2005.</p>
POSTA ELETTRONICA CERTIFICATA	Sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici.
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.
PRODUTTORE	Persona fisica o giuridica, 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 responsabile della gestione documentale.
PA	Pubblica Amministrazione.
PEC	Posta Elettronica Certificata.
PU	Pubblico Ufficiale.
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; in LegalDoc è l'insieme degli Indici del Pacchetto di Archiviazione associati ad ogni documento inviato in conservazione in un'unica sessione, che fanno parte del pacchetto di versamento.
REST	Representational State Transfer.
RESPONSABILE DELLA CONSERVAZIONE	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 del DPCM del 3 dicembre 2013.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	Risorsa di InfoCert, che, su affido del Responsabile della Conservazione, gestisce le politiche generali del sistema di conservazione, nel rispetto del modello organizzativo esplicitato nel presente Manuale e di quanto previsto nelle

	Specificità del Contratto (Atto di affidamento).
RESPONSABILE DELLA GESTIONE DOCUMENTALE O RESPONSABILE DEL SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al 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, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
RESPONSABILE DELLA SICUREZZA INFORMATICA	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
RESPONSABILE DEL TRATTAMENTO DEI DATI	Persona fisica o giuridica o pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
RIFERIMENTO TEMPORALE	Evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art. 1, lettera m del DPCM 22 febbraio 2013).
SaaS	Software as a Service.
SCARTO	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e/o di interesse storico culturale.
SISTEMA DI CLASSIFICAZIONE	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Nell'ambito della Pubblica Amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico.
STATICITA'	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.

TSA	Time Stamping Authority.
TSS	Time Stamping Service.
TU	Testo Unico.
URL	Universal Resource Locator.
UTC	Universal Coordinated Time – Tempo Universale Coordinato.
UTENTE	Persona fisica, 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 AGLI ARCHIVI DI STATO	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio 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.
WORM	Write Once Read Many.

[Torna al sommario](#)

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

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

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e ss.mm.ii. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss.mm.ii – Testo

Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

[Torna al sommario](#)

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle citate Regole Tecniche ai sensi del Codice:

- UNI EN ISO 9001:2015 Sistemi di gestione per la Qualità;
- ISO 14001:2015 Sistema di Gestione Ambientale;
- Norma ETSI 319 401 - Reg. UE 910/2014 – eIDAS (electronic IDentification Authentication and Signature);
- ISO 15489:2014 (cap. 5 Regulatory Environment; cap. 7 Records Management Requirements);
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- ISO/IEC 20000-1:2011 Gestione dei Servizi Informatici.
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

[Torna al sommario](#)

3.3 Procedure aziendali interne

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

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

[Torna al sommario](#)

4. RUOLI E RESPONSABILITÀ

Si riportano di seguito le figure di Responsabilità legate al servizio di conservazione e le rispettive attività di competenza che si sono susseguite nel tempo in InfoCert.

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
Responsabile del servizio di Conservazione	Antonio Borgo	<p>Dal</p> <ul style="list-style-type: none"> Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; Corretta erogazione del servizio di conservazione all'ente produttore; Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione. Definizione delle condizioni generali del contratto di servizio in coordinamento con la funzione legale e la funzione 	<p>Dal 15 luglio 2008.</p> <p>Assunzione a tempo indeterminato</p>	

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
		commerciale e funzione marketing di InfoCert.		
Responsabile del servizio di Conservazione precedente	Pio Barban	Come sopra	Dal 1° luglio 2007 al 15 luglio 2008.	
Responsabile Sicurezza dei sistemi per la conservazione	Alfredo Esposito	<ul style="list-style-type: none"> • Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • Segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive. 	Dal 1° gennaio 2011. Assunzione a tempo indeterminato.	
Responsabile funzione archivistica di conservazione	Marta Gaia Castellan	<ul style="list-style-type: none"> • Definizione e descrizione archivistica dei documenti e delle aggregazioni documentali per la fruizione del patrimonio documentario e informativo conservato; • Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; • Analisi archivistica per lo sviluppo di funzionalità del sistema di conservazione; • Collaborazione con l'ente produttore ai fini del trasferimento 	Dal 1° settembre 2015. Assunzione a tempo indeterminato.	

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
		<p>in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza;</p> <ul style="list-style-type: none"> • Definizione delle condizioni generali del contratto di servizio in coordinamento con la funzione legale e la funzione commerciale e funzione marketing di InfoCert; • Controlli periodici a campione sulla leggibilità dei documenti conservati. 		
Responsabile funzione archivistica di conservazione precedente	Silvia Loffi	Come sopra	Dal 2 dicembre 2014 al 31 agosto 2015.	
Responsabile trattamento dati personali	Alfredo Esposito	<ul style="list-style-type: none"> • Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; • Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza. 	Dal 1° gennaio 2011. Assunzione a tempo indeterminato.	
Responsabile sistemi informativi per la conservazione	Massimo Biagi	<ul style="list-style-type: none"> • Presidio ed evoluzione dei sistemi informativi per la conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000 • Gestione dell'esercizio delle componenti hardware e software di 	Dal 1° marzo 2014. Assunzione a tempo indeterminato.	

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
		<p>base del sistema di conservazione;</p> <ul style="list-style-type: none"> • Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore in collaborazione con Il Responsabile della manutenzione del sistema di conservazione; • Segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive; • Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; • Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione; • Coordinamento dello sviluppo e manutenzione delle componenti hardware e software di base del sistema di conservazione. 		
<p>Responsabile sviluppo e manutenzione del sistema di conservazione</p>	<p>Nicola Maccà</p>	<ul style="list-style-type: none"> • Sviluppo e manutenzione del sistema di conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000; • Coordinamento dello sviluppo e manutenzione delle componenti 	<p>Dal 1° gennaio 2013. Assunzione a tempo indeterminato.</p>	

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
		<p>software del sistema di conservazione;</p> <ul style="list-style-type: none"> • Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; • Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; • Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche in collaborazione con il Responsabile funzione archivistica di conservazione; • Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione. 		

[Torna al sommario](#)

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Profilo di InfoCert

Denominazione sociale	InfoCert S.p.A.
------------------------------	-----------------

<i>Sede Legale:</i>	Piazza Sallustio, 9, 00187 Roma Tel.+39 06 836691
<i>Sedi Operative:</i>	<ul style="list-style-type: none"> • Piazza da Porto, 3, 35131 Padova • Via Franco Russoli, 5, 20143 Milano • Via Marco e Marcelliano, 45, 00147 Roma Tel: +39 06836691
<i>Sito web</i>	www.infocert.it
<i>e-mail</i>	info@infocert.it
<i>PEC</i>	infocert@legalmail.it
<i>Codice Fiscale / Partita IVA</i>	07945211006
<i>Numero REA</i>	RM – 1064345

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

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

La mission aziendale si declina anche nel servizio di Conservazione digitale: innovazione, sicurezza, affidabilità e conformità normativa, con lo scopo di assicurare la corretta gestione,

archiviazione e conservazione dei documenti informatici di diversi soggetti produttori, assicurando l'esibizione a norma dei documenti conservati e la consulenza specialistica su progetti di paperless design.

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

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

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

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

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

- ISO 14001:2015 (Sistema di Gestione Ambientale)
- ISO/IEC 20000-1:2011 (Gestione dei Servizi Informatici)
- UNI EN ISO 9001:2015 (Sistemi di gestione per la qualità);
- ISO/IEC ISO 27001:2013 (Sistemi di gestione della sicurezza delle informazioni).

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

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

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

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

[Torna al sommario](#)

5.2 Organigramma

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

[Torna al sommario](#)

5.3 Strutture organizzative

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

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

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

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

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

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

Tutte le verifiche in carico al Responsabile del servizio della Conservazione sono garantite anche dal servizio di auditing interno. Il processo di conservazione è normalmente effettuato da procedure totalmente automatizzate, che non necessitano dell'intervento di altri soggetti o delegati.

InfoCert si riserva, come specificato nelle Condizioni generali del Contratto, la possibilità di avvalersi di partner tecnologici per l'esecuzione di operazioni, singole attività, servizi relativi a funzioni o fasi del processo di conservazione, a terzi soggetti, fornitori esterni, che per conoscenza, esperienza, capacità e affidabilità forniscano idonee garanzie.

[Torna al sommario](#)

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

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

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

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

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

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

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

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

[Torna al sommario](#)

6.1 Oggetti conservati

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

I visualizzatori dei formati standard, previsti nell’allegato 2 del DPCM 3 dicembre 2013, sono automaticamente assegnati all’atto dell’attivazione del proprio ambiente di conservazione e sono forniti da InfoCert al Soggetto Produttore all’atto di attivazione del servizio. Tutti i

documenti inviati in conservazione saranno associati al visualizzatore configurato per il particolare formato.

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

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

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

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

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

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

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

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

[Torna al sommario](#)

6.2 Pacchetto di versamento

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

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

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

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

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

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

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

[Torna al sommario](#)

6.3 Pacchetto di archiviazione

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

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

In particolare nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA
- il token del documento (ovvero il suo identificativo univoco)

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

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

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

[Torna al sommario](#)

6.4 Pacchetto di distribuzione

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

Le procedure di esibizione permettono di estrarre dal sistema un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione utilizzando il relativo token (ovvero l'identificativo univoco del documento da esibire) o utilizzando uno o più metadati versati. Insieme ai file costituenti il pacchetto di distribuzione, sono rese disponibili anche le informazioni che qualificano il processo di conservazione, ossia il file IPdA e un'Attestazione di corretta conservazione e datacertazione firmata dal Responsabile del servizio di Conservazione.

Non è possibile esibire parti singole di documento.

L'esibizione può restituire il documento in due modalità differenti: in un unico pacchetto di distribuzione in formato zip, oppure un file alla volta. Quest'ultima modalità deve essere compatibile con il client di esibizione dell'utente.

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

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

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

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

[Torna al sommario](#)

7. IL PROCESSO DI CONSERVAZIONE

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

Il sistema consente le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati;
- **conservazione del pacchetto di archiviazione**: il documento, ricevuto nei Data Center di InfoCert in formato digitale statico non modificabile, viene conservato a norma di legge per tutta la durata prevista ed è contenuto in un pacchetto di archiviazione;

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

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

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

[Torna al sommario](#)

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

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

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

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

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

[Torna al sommario](#)

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

ATT.1 Validazione del pacchetto di versamento

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

[Torna al sommario](#)

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

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

ATT.1 Generazione del pacchetto di archiviazione

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

ATT.2 Memorizzazione e creazione copia di sicurezza

<i>INPUT</i>	<i>Pacchetto di archiviazione</i>
--------------	-----------------------------------

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

ATT.3 Invio dell'IPdA al soggetto Produttore

<i>INPUT</i>	<i>File IPdA</i>
	Invio dell'esito e del file IPdA al soggetto Produttore.
<i>OUTPUT</i>	<i>Esito conservazione inviato</i>

[Torna al sommario](#)

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

All'interno delle 'Specificità del Contratto' SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc è presente la griglia riassuntiva dei codici errore che il servizio LegalDoc restituisce in seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto. La griglia riporta le seguenti informazioni:

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

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

L'assistenza LegalDoc è contattabile mediante l'invio di un messaggio di posta elettronica certificata alla casella: assistenza.legaldoc@legalmail.it dalla casella di posta certificata del Produttore.

[Torna al sommario](#)

7.5 Preparazione e gestione del pacchetto di archiviazione

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

ATT.1 Verifica del pacchetto di versamento

<i>INPUT</i>	<i>Pacchetto di versamento</i>	
Sistema di conservazione	1	Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal soggetto Produttore, a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema di gestione del soggetto Produttore dell'errore intercorso. In questo caso, termine del flusso.
	2	Controllo dei valori indicati dal soggetto Produttore nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
	3	Controllo dei valori indicati dal soggetto Produttore nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione, non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.
	4	Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.

<i>OUTPUT</i>	<i>pacchetto di versamento verificato</i>
---------------	-------------------------------------------

ATT.2 Formazione del pacchetto di archiviazione

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

ATT.3 Memorizzazione del pacchetto di archiviazione

<i>INPUT</i>	<i>Pacchetto di archiviazione</i>	
<i>Sistema di conservazione</i>	1	Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali

	2	Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito.
	3	La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
<i>OUTPUT</i>	<i>Documenti conservati</i>	

[Torna al sommario](#)

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

ATT1. Ricerca del documento da esibire

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

ATT2. Richiesta di esibizione del documento conservato

<i>INPUT</i>	<i>Richiesta di esibizione da eseguire</i>	
<i>Sistema di Gestione documentale del Soggetto</i>		Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di session (IdSessionId).
		Invocazione del servizio di esibizione del sistema di conservazione secondo le

Produttore	modalità descritte nelle 'Specificità del Contratto' SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc. In questa chiamata viene utilizzato il token ricavato in precedenza.
OUTPUT	<i>Richiesta di esibizione eseguita</i>

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

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

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

INPUT	<i>Richiesta di esibizione acquisita</i>
	Ricerca dei file costituenti il documento e dei file attestanti il processo di conservazione corrispondenti al token inviato e preparazione del pacchetto di distribuzione.
	Invio della risposta al sistema del Soggetto Produttore.
OUTPUT	<i>Documento esibito</i>

[Torna al sommario](#)

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

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

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

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

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

Possono essere generati anche duplicati o copie attraverso l'Esibitore o su supporto ottico, su specifica richiesta del Soggetto Produttore.

Nel primo caso il Produttore/Utente agisce autonomamente con apposite credenziali attraverso l'Esibitore di LegalDoc. Nel secondo caso il Soggetto Produttore inoltra la richiesta ai suoi riferimenti abituali (help desk o account) che poi provvedono alla veicolazione verso gli operatori interni.

L'intervento di un Pubblico Ufficiale per attestare la conformità di una copia all'originale avviene secondo quanto previsto dagli articoli 22 e 23 del Codice e dalle Regole Tecniche del DPCM del 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

[Torna al sommario](#)

7.8 Scarto dei pacchetti di archiviazione

In LegalDoc esistono due diverse metodologie di ‘cancellazione’:

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

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

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

InfoCert, in quanto Conservatore, attiva la procedura di scarto sempre per richiesta e approvazione del Soggetto Produttore.

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, con l’indicazione a margine di eventuali errori occorsi durante lo svolgimento del processo, dei rimedi attuati e delle altre informazioni che ritiene meritevoli di annotazione.

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

[Torna al sommario](#)

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

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

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

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

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

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

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

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

Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di hand over tra conservatori'.

[Torna al sommario](#)

8. IL SISTEMA DI CONSERVAZIONE

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

Il sistema è organizzato su più siti (a Padova e a Modena).

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

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

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

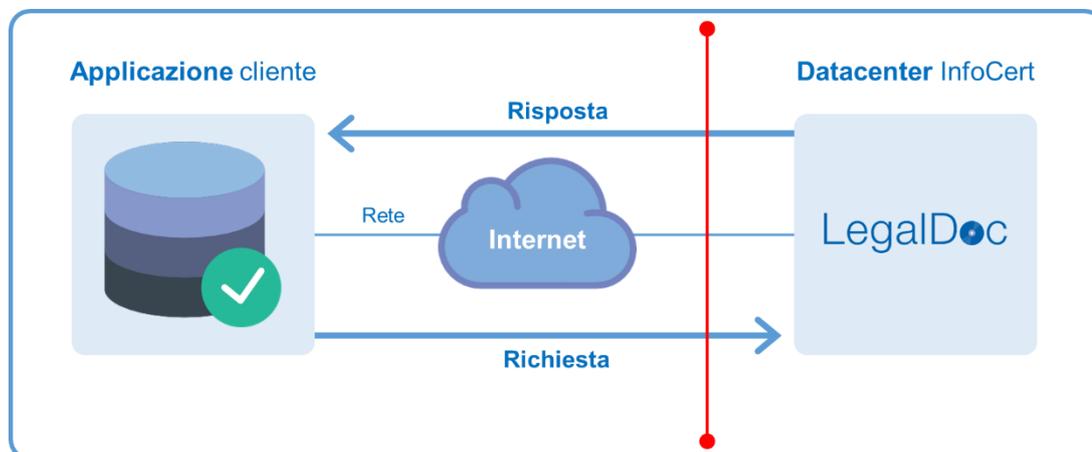


Figura1: Rappresentazione del servizio attraverso la rete

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

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

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

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

Attraverso l'esibizione a norma diventa possibile:

- estrarre un documento e visualizzarlo a video;
- produrre copia cartacea o su altro supporto informatico del documento;
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione;

- prendere visione dei file a corredo che formano il pacchetto di distribuzione e che qualificano il processo di conservazione attestandone il corretto svolgimento (Indice di Conservazione UNI SINCRO, altrimenti detto Indice del Pacchetto di Archiviazione, File di parametri, File di indici, File di dati, Attestato di conservazione);

- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione;

- verificare l'integrità del documento.

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

[Torna al sommario](#)

8.1 Componenti Logiche

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

[Torna al sommario](#)

8.2 Componenti Tecnologiche

8.2.1 Firewall

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

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

[Torna al sommario](#)

8.2.2 Back-up

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

[Torna al sommario](#)

8.2.3 Servizio di marcatura temporale

Per l'emissione delle marche temporali il sistema si avvale del servizio di marcatura di InfoCert, Certification Authority accreditata, compliant eIDAS. Il Piano per la Sicurezza del Certificatore è depositato presso AgID.

La marca temporale viene richiesta al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert. Il root-certificate della TSA è depositato presso AgID.

Il TSS è sincronizzato via radio con l'I.N.R.I.M di Torino (Istituto Nazionale di Ricerca Metrologica, già Istituto Elettrotecnico Nazionale “Galileo Ferraris”) ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

[Torna al sommario](#)

8.2.4 Posta Elettronica Certificata

Il sistema di conservazione si avvale del servizio di posta elettronica certificata di InfoCert: in sede di attivazione del sistema, viene definita per il Soggetto Produttore una casella di posta certificata (PEC) tramite la quale richiedere supporto alla casella di amministrazione del sistema.

La PEC configurata all'attivazione è utilizzata, inoltre, per ogni comunicazione al Soggetto Produttore che interessa il funzionamento del sistema.

[Torna al sommario](#)

8.3 Componenti Fisiche

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

[Torna al sommario](#)

8.3.1 Dispositivo HSM di firma digitale

Il sistema si avvale dei servizi di firma digitale forniti dalla CA InfoCert. In particolare, il servizio di firma automatica (firma massiva) permette di apporre automaticamente la firma digitale e la validazione temporale ad elevati volumi di documenti informatici, senza che sia necessaria la presenza del titolare nel momento preciso della firma.

I dispositivi utilizzati rispondono ai requisiti di sicurezza previsti per i dispositivi sicuri di firma.

[Torna al sommario](#)

8.3.2 Sistema Storage

Il sistema di conservazione di InfoCert e dei suoi partner tecnologici, utilizza storage magnetici ad alte performance come sistema primario e secondario per la memorizzazione dei dati. Tali storage, scelti tra i primari fornitori di tecnologie presenti sul mercato, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato.

Tali storage rispondono all'esigenza di memorizzazione a lungo termine dei fixed content, ossia dei files che devono essere conservati con garanzia nel tempo di integrità e disponibilità del contenuto.

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni. Nel caso di documenti che contengono dati sensibili i dati vengono memorizzati cifrati con chiave in disponibilità al solo Responsabile del servizio della Conservazione.

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

Nell'ambito del sistema di conservazione, lo storage rappresenta sia il supporto primario di conservazione posto fisicamente presso la sede InfoCert di Padova, sia il supporto secondario posto nel sito di disaster recovery di Modena. I due sistemi sono interconnessi mediante collegamenti ad alta velocità dedicati, completamente ridondati e protetti da misure di sicurezza. I collegamenti consentono la replicazione dei dati conservati eliminando il rischio di distruzione di tutte le copie delle informazioni in caso di danno irreparabile a livello di sito.

Questo secondo sistema funge anche da copia di sicurezza.

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

[Torna al sommario](#)

8.3.3 Sincronizzazione dei sistemi

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

Il meccanismo di allineamento temporale tra i sistemi fornisce la certezza della successione temporale degli avvenimenti nel sistema. La sincronizzazione delle macchine infatti, genera dei file di log temporalmente omogenei tra loro, che permettono di ricostruire con certezza l'ordine di accadimento degli eventi intervenuti a tutti i livelli del sistema, e di individuare la sequenza di svolgimento delle varie operazioni.

[Torna al sommario](#)

8.4 Procedure di gestione e di evoluzione

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

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

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

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

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

[Torna al sommario](#)

8.4.1 Criteri di organizzazione del contenuto

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi in cui i documenti sono corredati da tutta una serie di metadati. I documenti inviati

al sistema di conservazione, infatti, vengono aggregati secondo criteri di omogeneità secondo le informazioni di configurazione definite in fase contrattuale. In particolare, vengono concordati i parametri fondamentali (bucket, policy, classi documentali) con i quali sono organizzati i documenti presi in carico, per consentire la maggiore interoperabilità possibile tra i sistemi di conservazione.

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

[Torna al sommario](#)

8.4.2 Organizzazione dei supporti

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

[Torna al sommario](#)

8.4.3 Archivio dei viewer consegnati dal Soggetto Produttore

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

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

Se il Soggetto Produttore invia documenti in formato non standard senza depositare il relativo visualizzatore, oppure nel caso di invio di documenti in modalità cifrata, è sua cura la

conservazione degli strumenti necessari per la decifrazione e/o la visualizzazione di quanto conservato.

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

[Torna al sommario](#)

8.4.4 Archivio dell'hardware e del software obsoleto

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

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

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

InfoCert ha scelto di introdurre in azienda un Service Management System - SMS conforme alla norma ISO/IEC 20000 [standard internazionale per l'IT Service Management] allo scopo di mantenere e migliorare l'allineamento e la qualità dei servizi di business erogati, attraverso un ciclo costante di monitoraggi, reporting e revisione degli SLA concordati.

InfoCert ha individuato nella Certificazione ISO 20000 un obiettivo di qualificazione dell'offerta in grado di conferire valore aggiunto ai servizi offerti e una maggiore garanzia dei livelli di servizio concordati con i propri clienti.

L'adozione di un modello di Service Management System – SMS InfoCert 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 InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti evitando di assecondare aspettative cliente non erogabili;
- garantire un controllo dei fornitori che concorrono alla erogazione dei nostri servizi;
- migliorare la qualità dei servizi di business erogati.

Di seguito lo schema rappresentativo del Modello adottato da InfoCert:

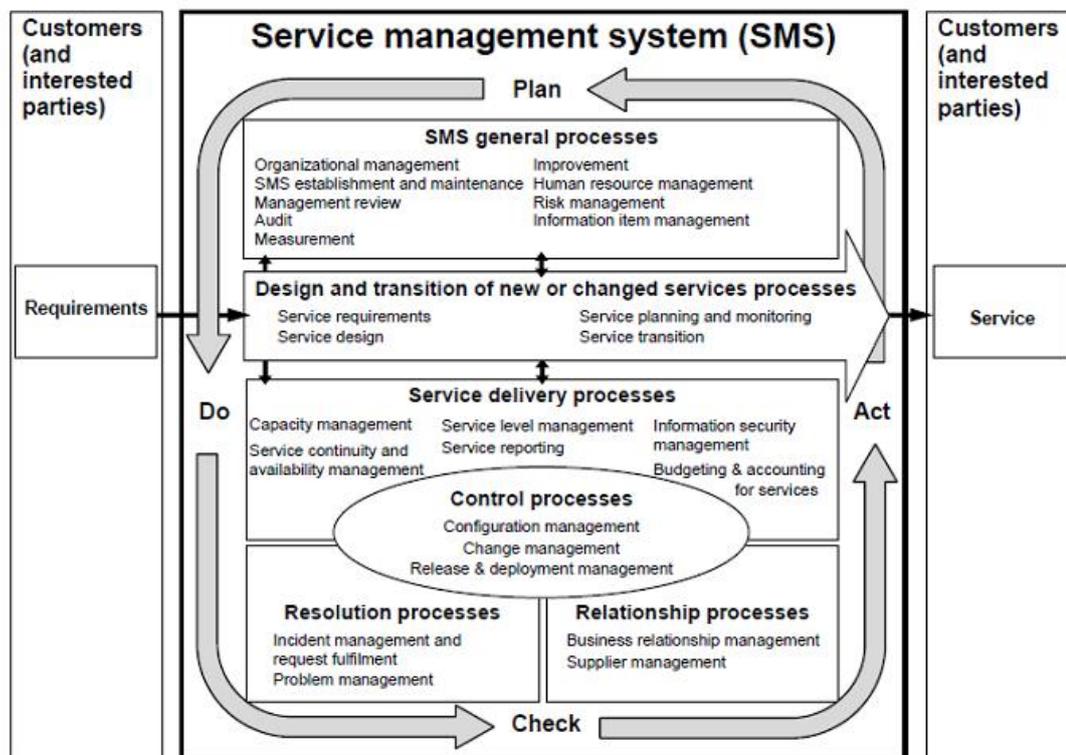


Figura2: Rappresentazione grafica processi della norma ISO/IEC 20000:11

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

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche e i requisiti per la gestione dei servizi inerenti il campo di applicazione;
- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement dei servizi sulla base di quanto definito nel *service management plan*;
- 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 InfoCert ha definito degli SLA baseline di riferimento in relazione ai seguenti KPI (Key Performance Indicator):

- Orario di servizio
- Disponibilità di servizio.

[Torna al sommario](#)

9.1 Procedure di monitoraggio

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

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

La piattaforma è costruita a partire da una versione customizzata del noto software open source Nagios e per rilevare i dati dai diversi componenti utilizza diverse tecnologie (SNMP, NRPE, Sahi, ecc.). I monitoraggi possono essere eseguiti in modalità attiva (quindi la piattaforma interroga puntualmente le diverse componenti) oppure in modalità passiva (ovvero sono le singole componenti che inviano dati alla piattaforma, senza il bisogno di venire interrogate da essa).

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

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

Alle quattro probe fisiche si aggiunge un pool di macchine virtuali posizionate nella server farm di Clouditalia.

Le probe fisiche si occupano di effettuare i monitoraggi sull'infrastruttura ed i servizi ospitati nei locali nei quali sono installate mentre le macchine virtuali si occupano di effettuare le navigazioni dei servizi sia da rete interna che tramite internet. Tutti i dati raccolti vengono infine centralizzati su una piattaforma resa disponibile online per una veloce e facile consultazione degli stessi.

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

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

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

[Torna al sommario](#)

9.1.1 Processi di monitoraggio del sistema di conservazione

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

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

[Torna al sommario](#)

9.1.2 Monitoring della disponibilità del sistema

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

monitorate con i tool definiti nella piattaforma di monitoraggio TMS precedentemente descritta.

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

[Torna al sommario](#)

9.2 Verifica dell'integrità degli archivi

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

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

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

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

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

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

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

Vengono eseguiti i seguenti passi operativi:

- verifica della validità della firma digitale e della marcatura temporale apposte all'atto della conservazione dal Responsabile del servizio della Conservazione sul file IPdA e, se presenti, verifica della firma digitale e della marcatura temporale del documento;
- calcolo dell'impronta del documento e confronto con quella contenuta all'interno del file IPdA;
- generazione di un report che viene automaticamente sottoposto alla conservazione nell'area dedicata al Responsabile del servizio della Conservazione (quindi a sua volta firmato e marcato temporalmente dal Responsabile del servizio della Conservazione stesso).

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

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

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

In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio della

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

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

9.3 Controlli

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

I controlli effettuati si distinguono nelle tre tipologie: controlli di versamento, controlli di processo e controlli periodici.

[Torna al sommario](#)

9.3.1 Controlli di versamento

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

- Formato del documento da conservare (in coerenza con i 'Dati Tecnici di attivazione' e con la configurazione degli ambienti);
- Correttezza della struttura del file di Parametri (contenente le informazioni per la leggibilità nel tempo del documento da conservare);
- Correttezza della struttura del file di Indici (contente i metadati del documento da conservare, alcuni dei quali obbligatori, in coerenza con i 'Dati Tecnici di attivazione');
- Presenza in conservazione sul medesimo path di un documento con lo stesso nome-file del documento da conservare;
- Abilitazione Utenza all'attività di versamento in quel dato ambiente; l'associazione tra utenza (username e password) e singola persona fisica è in capo al Produttore. La password di accesso è inviata da InfoCert al Produttore tramite canale PEC.

- Validità sessione in uso (di default della durata di un'ora tra login e logout);
- Dimensione massima del documento da conservare (di default 256 megabyte, variabile su richiesta);
- Validità del certificato qualificato di firma digitale con cui è sottoscritto il documento da conservare (su richiesta).

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

[Torna al sommario](#)

9.3.2 Controlli di processo di progettazione e sviluppo dei servizi

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

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

[Torna al sommario](#)

9.3.3 Monitoraggio e registrazioni durante il ciclo produttivo

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

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

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

autorizza il rilascio.

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

[Torna al sommario](#)

9.3.4 Monitoraggio e registrazioni per collaudo finale

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

[Torna al sommario](#)

9.3.5 Controlli periodici

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

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

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

[Torna al sommario](#)

9.4 Soluzioni adottate in caso di anomalie

Ad ogni semestre il Responsabile del servizio della Conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema

al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

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

[Torna al sommario](#)

9.4.1 Auditing generale del sistema

Il Piano delle verifiche ispettive è definito annualmente dal gestore della qualità e approvato dal Rappresentante della direzione.

Le verifiche ispettive sono condotte all'interno della società sulla base della procedura “MG/325 Gestire Verifiche Ispettive InfoCert” volte a determinare se i processi aziendali ed i risultati ottenuti:

- sono orientati alle politiche per la qualità e al raggiungimento degli obiettivi
- sono in accordo con quanto previsto nei documenti di riferimento
- sono compliance alla normativa di riferimento
- sono compliance agli standard adottati dal sistema di conservazione
- sono attuate efficacemente
- sono idonee al conseguimento degli obiettivi della Qualità e miglioramento servizi

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

- strutture organizzative
- risorse utilizzate
- procedure
- processi
- prodotti e i risultati dell'attività
- documentazione
- addestramento

- le segnalazioni dei clienti e terze parti.

Gli audit sono coordinati dall'Esecutivo Qualità ed eseguiti direttamente o da personale interno o esterno qualificato e debitamente addestrato.

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

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

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

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

Il Responsabile delle verifiche e ispezioni (auditing) pianifica e implementa processi di audit che coinvolgono aspetti di processo, organizzazione, tecnologici e logistici. L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto, alla documentazione generale del sistema, ai principi che ispirano il sistema qualità e al presente Manuale della Conservazione.

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

[Torna al sommario](#)

9.4.2 Incident management

L'ambito completo del processo si applica alla gestione degli incidenti informatici che possono interessare uno o più servizi tecnologici eventualmente interconnessi ed è formalmente

descritto dalla procedura ‘PR455-Incident Management InfoCert’. La procedura definisce anche la metodologia di assegnazione della gravità di un incidente e della relativa priorità di gestione in base alla matrice di analisi di impatto/urgenza effettuata utilizzando le informazioni sul servizio di riferimento e sui relativi SLA del servizio o nelle istruzioni /policy specifiche relative alla sicurezza informatica.

Urgenza ⇔	ALTA	MEDIA	BASSA
Impatto ⇓			
ALTO	Critica	Alta	Media
MEDIO	Alta	Media	Bassa
BASSO	Media	Bassa	Molto bassa

L’impatto è definito in base alla BIA [Business Impact Analysis] del servizio.

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

Il processo di gestione degli incidenti, condotto secondo le raccomandazioni delle Best Practice ITIL e in conformità alle norme ISO 27001, si focalizza sulle modalità di gestione e di ripristino tempestivo degli incidenti informatici. La funzione InfoCert coinvolta in tale processo è il Service Desk che opera anche come interfaccia per gli altri processi, quali il Change Management, il Problem Management e il Configuration Management.

Il modello organizzativo prevede che il supporto specialistico sistemistico sia fornito dalla funzione di Service Desk InfoCert (SD) che gestisce il ciclo di vita dell’incidente con lo strumento per la tracciatura dell’evento e che si avvale della collaborazione di tutte le strutture aziendali coinvolte.

Il processo d’Incident Management è supportato dall’attività di Problem Management (procedura PR456) che mira a ridurre gli impatti negativi a seguito di incidenti che possono essere provocati da errori/malfunzioni nelle infrastrutture IT e a prevenire il verificarsi e il ripetersi di tali errori.

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

La gestione dei problemi può essere sia reattiva che proattiva e riguarda l'identificazione e la risoluzione di problemi prima che si verifichino degli incidenti.

InfoCert è impegnata nel continuo affinamento e aggiornamento del sistema di conservazione, in modo da individuare ogni potenziale causa d'incidente e provvedere alla sua rimozione, scongiurando il blocco del sistema o il danneggiamento dei file in esso contenuti.

Il Responsabile del servizio della Conservazione mantiene il verbale degli incidenti e delle contromisure attuate, che divengono oggetto della successiva riunione di riesame e sono inviate al sistema di conservazione.

[Torna al sommario](#)

SPECIFICITÀ DEL CONTRATTO

Il sistema di conservazione di InfoCert è fruibile dal Produttore in diverse modalità:

1. Tramite il servizio “LegalDoc LITE”: è un client desktop che consente di utilizzare il servizio di conservazione direttamente dal proprio sistema operativo. È l’unico servizio InfoCert di conservazione digitale “standardizzato” e acquistabile direttamente da e-commerce.
2. Tramite il servizio “LegalDoc Web”: è un’interfaccia web che consente il versamento e l’esibizione manualmente attraverso un portale web accessibile con apposite credenziali.
3. Tramite il servizio “LegalDoc Connector”: è uno strumento che consente di automatizzare il versamento attraverso una cartella FTP protetta.
4. Tramite chiamate web services: in questo caso le applicazioni gestionali del cliente sono integrate con il sistema di conservazione di InfoCert.

I servizi relativi ai punti 2,3,4 sono regolati dai seguenti documenti contrattuali, che contengono e descrivono tutte le esigenze richieste dai Soggetti Produttori. La documentazione contrattuale e tecnica elencata è resa disponibile all’atto del perfezionamento dell’accordo di servizio al Produttore e condivisa internamente sullo sharepoint aziendale InfoCert.

1. **Condizioni Generali di Contratto** che regola la vendita del servizio di conservazione nelle diverse modalità di erogazione;
2. **Richiesta di attivazione** che comporta l’adesione al servizio;
3. **Dati tecnici per l’attivazione** con cui il Soggetto Produttore fornisce tutte le informazioni necessarie su tipologie documentali, metadati e credenziali di accesso di cui necessita;
4. **File di configurazione** redatto da InfoCert all’attivazione del servizio, contiene i dati di configurazione del soggetto produttore, delle user d’accesso, delle policy associate e delle tipologie documentali, comprensivi di metadati e formati configurati;
5. **Atto di affidamento** che rappresenta una formalizzazione dell’affidamento ad InfoCert del processo di conservazione e stabilisce espressamente quali attività di fatto vengano assunte da InfoCert e quali, al contrario, rimangano a carico dell’affidatario, come stabilito dagli articoli 5 e 6 del DPCM del 3 dicembre 2013;

6. **Specifiche Tecniche di integrazione (sia per i web services che per LegalDoc Connector)** che fornisce tutte le informazioni tecniche necessarie ad operare l'integrazione tra i Sistemi di Gestione documentali del Produttore e il sistema di conservazione di InfoCert;
7. **Impegno alla riservatezza;**
8. **Allegato Tecnico** che descrive le modalità di fornitura del servizio e l'infrastruttura tecnico-tecnologica utilizzata per la sua erogazione;
9. **Manuale Utente** che risponde alla necessità di documentare operativamente il processo dal punto di vista del Produttore/Utente;
10. **Descrizione dei codici di errore** per fornire una casistica esaustiva dei possibili messaggi di errore del servizio di conservazione e delle azioni che è necessario intraprendere per porvi rimedio;

Relativamente al servizio “LegalDoc LITE”, poiché veicolato direttamente da e-commerce, la documentazione di riferimento è pubblicata sul sito istituzionale di InfoCert www.infocert.it e differisce leggermente da quella appena elencata per accogliere delle specificità relative alla natura “standard” del prodotto. Di seguito i documenti pubblicati:

1. Condizioni Generali di Contratto
2. Dati tecnici di attivazione
3. Allegato tecnico
4. Manuale utente
5. Modulo per la disdetta del servizio
6. Richiesta di attivazione e atto di affidamento: compilabili e visibili dopo aver effettuato l'acquisto sull'e-commerce InfoCert

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

Per i Soggetti Produttori con una infrastruttura tecnologica complessa viene redatto un ‘Manuale dei processi per la conservazione’, che rimanda al presente Manuale per quanto riguarda le sezioni standard (es. Struttura organizzativa e Ruoli di responsabilità del Conservatore, Dettaglio tecnico del sistema di conservazione e trattazione dei pacchetti di

archiviazione, Monitoraggio e controlli del Conservatore), e dettaglia le specificità del singolo Produttore (es. modalità di versamento o esibizione, tipologie documentali, metadati scelti, infrastrutture tecnologiche particolari).

[Torna al sommario](#)