



ALLEGATO 12



Manuale dei processi per la conservazione digitale a norma (ADS)

Questa pagina è lasciata
intenzionalmente bianca

Indice

<u>1.....</u>	<u>Novità introdotte</u>	<u>5</u>
<u>2.....</u>	<u>Scopo e campo di applicazione del documento</u>	<u>6</u>
<u>3.....</u>	<u>Termini</u>	<u>7</u>
<u>3.1.....</u>	<u>Definizioni</u>	<u>7</u>
<u>3.2.....</u>	<u>Acronimi</u>	<u>12</u>
<u>4.....</u>	<u>Normativa e standard di riferimento</u>	<u>13</u>
<u>4.1 Normativa di riferimento.....</u>		<u>13</u>
<u>4.2 Standard di riferimento.....</u>		<u>14</u>
<u>5.....</u>	<u>Ruoli e responsabilità</u>	<u>15</u>
<u>5.1 Il Responsabile della Conservazione.....</u>		<u>15</u>
<u>5.2.....</u>	<u>Soggetto Produttore</u>	<u>16</u>
<u>5.3 InfoCert S.p.A.....</u>		<u>17</u>
<u>6.....</u>	<u>Oggetti sottoposti alla conservazione</u>	<u>18</u>
<u>6.1</u>	<u>Strumenti utilizzati</u>	<u>19</u>
<u>6.2</u>	<u>Formato dei documenti elettronici</u>	<u>19</u>
<u>6.3 Le tipologie documentali.....</u>		<u>19</u>
<u>8.Il Processo di Conservazione.....</u>		<u>22</u>
<u>8.1 Responsabilità del processo di conservazione.....</u>		<u>22</u>
<u>8.2 Fasi del processo di conservazione: dettaglio.....</u>		<u>23</u>
<u>8.2.1 Formazione del documento.....</u>		<u>23</u>
<u>8.2.2 Indicizzazione e archiviazione.....</u>		<u>23</u>
<u>8.2.3 Acquisizione documento e creazione del file delle direttive.....</u>		<u>23</u>
<u>8.2.4 Invio al sistema di conservazione.....</u>		<u>24</u>
<u>8.2.5 Verifica, accettazione e invio della ricevuta di accettazione del pacchetto.....</u>		<u>24</u>
<u>8.2.6 Creazione del pacchetto di archiviazione.....</u>		<u>25</u>
<u>8.2.7 Memorizzazione, creazione copia di sicurezza e chiusura della conservazione.....</u>		<u>25</u>
<u>9.Processo di ricerca ed esibizione.....</u>		<u>26</u>

<u>9.1 Procedura di esibizione: dettaglio.....</u>	<u>26</u>
--	-----------

9.1.1 Ricerca del documento da esibire.....	26
9.1.2 Invio della richiesta a LegalDoc.....	27
9.1.3 Ricerca del documento nel sistema ed esibizione.....	27
9.1.4 Verifica del documento.....	27
9.1.5 Verifica del documento.....	27
10. Il sistema di conservazione.....	28
10.1 Configurazione dei sistemi e modalità di erogazione.....	28
10.2 Componenti.....	28
10.2.1 Marca temporale.....	28
10.2.2 Firma digitale con dispositivo HSM.....	28
10.2.3 Posta Elettronica Certificata.....	29
10.3 Controlli.....	29
10.3.1 Controlli di processo.....	29
10.3.2 Controlli periodici.....	29
10.4 Ispezione del sistema da parte delle autorità competenti.....	29
10.5 Incident management.....	30
10.6 Sicurezza fisica.....	30
10.7 Gruppi di continuità.....	30
10.8 Connessione a Internet.....	30
10.9 Sicurezza delle reti: protezione da intrusioni.....	31
10.10 Protezione dei dati personali.....	31
11. Allegati.....	32

- **Novità introdotte**

Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	1.0	Data Versione/Release:	05/2017
Descrizione modifiche:	N.A.		
Motivazioni:	Prima release		

- **Scopo e campo di applicazione del documento**

Il presente documento è il Manuale dei processi documentali per la conservazione del Comune di

Occhiobello, ai sensi del DPCM 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) e del Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014.

Come richiesto dal DPCM del 2013 all'art. 8, il presente documento “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 dei processi documentali per la conservazione, permette un agevole svolgimento di tutte le attività di controllo.

Si precisa che il presente documento integra e dettaglia il Manuale della Conservazione di InfoCert, disponibile nei siti:

<https://www.infocert.it/>

<http://www.agid.gov.it/>

Più concretamente si rimanda la Manuale standard di InfoCert per:

- 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.

- **Termini**

- **Definizioni**

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.
AFFIDABILITÀ	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	è il 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 ORGANIZATIVA OMOGENEA	un 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 dell'Amministrazione Digitale.
CAS	Content Addressed Storage.
CERTIFICATORE ACCREDITATO	soggetto, pubblico o privato, che svolge attività di certificazione del processo 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.
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	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, descritto nel presente manuale di conservazione e che risponde a quanto stabilito nel DPCM 03/12/2013.
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.
DOCUMENTO ANALOGICO	Rappresentazione analogica di atti, fatti o dati giuridicamente rilevanti.
DOCUMENTO	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

INFORMATICO	
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.
DLGS	Decreto Legislativo.
DPCM	Decreto della Presidenza del Consiglio dei Ministri.
DPR	Decreto del Presidente della Repubblica.
ESIBIZIONE	operazione che consente di visualizzare un documento conservato e di ottenerne copia.
eIDAS	Regolamento UE 910/2014
EVIDENZA INFORMATICA	una 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. Mentre l'HTML è un'istanza specifica dell'SGML, XML costituisce a sua volta un metalinguaggio, più semplice dell'SGML, largamente utilizzato per la descrizione di documenti sul Web. 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). Diversamente dall'HTML, l'XML consente all'utente di definire marcatori personalizzati, dandogli il controllo completo sulla struttura di un documento. Si possono definire liberamente anche gli attributi dei singoli marcatori.
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 qualificata 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	dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (Art. 3 n.10 eIDAS).
FIRMA ELETTRONICA QUALIFICATA	una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (Art.3 n.12 eIDAS).
FIRMA ELETTRONICA AVANZATA	Una firma elettronica che 1) è connessa unicamente al firmatario, 2) è idonea a identificare il firmatario, 3) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo, 4) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati (Art.26 eIDAS).
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 DEL 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, così come definita all'art. 1 comma 1 lettera i) DPCM del 30 marzo 2009. La marca temporale è opponibile ai terzi, definita anche nel DPCM 22 febbraio 2013, titolo IV.
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 FORMAT	formato di file creato da Adobe Systems nel 1993 per lo 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. 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.
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	il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione ottica conformemente a quanto previsto all'art. 7 del DPCM 03/12/2013.
RIFERIMENTO TEMPORALE	informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici, così come definito all'art. 1 comma 1 lettera m) DPCM del 30 marzo 2009, definito anche nel DPCM 22 febbraio 2013.
SCARTO	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
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.
UTENTE	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
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.

- **Acronimi**

CA	Certification Authority
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione (successivamente DigitPA ora Agenzia per l'Italia Digitale)
D. LGS	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
GU	Gazzetta Ufficiale della Repubblica Italiana
HSM	Hardware Security Module
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
SG	Sistema di Gestione
SGD	Sistema di Gestione Documentale
SSL	Secure Socket Layer
TSA	Time Stamping Authority
TSS	Time Stamping Service
TU	Testo Unico
URL	Uniform Resource Locator
XML	Extensible Markup Language

- **Normativa e standard di riferimento**

- **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 s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- 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, 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;
- Decreto del Ministero dell'Economia e delle Finanze 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche.

- **Standard di riferimento**

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

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques – Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set,

Sistema di metadata del Dublin Core;

- ISO 14001:2013 Sistema di Gestione Ambientale;
- UNI EN ISO 20000- 1: 2011 Gestione dei Servizi Informatici;
- UNI EN ISO 9001:2008 Sistemi di gestione per la qualità.

- **Ruoli e responsabilità**

- **Il Responsabile della Conservazione**

Come già per la deliberazione AIPA n. 42/2001, la deliberazione CNIPA n. 11/2004 (art. 5) le Regole Tecniche del DPCM 03/12/2013 enfatizzano il ruolo del Responsabile della Conservazione di documenti in formato digitale che assume un ruolo fondamentale all'interno del processo di conservazione, insieme ai suoi delegati o ai terzi affidatari.

La presenza del Responsabile della Conservazione è necessaria sia in ambito privato sia in ambito pubblico e vi sono attribuiti compiti debitamente elencati, riguardanti le funzioni, gli adempimenti, le attività e le responsabilità. Il Responsabile della Conservazione è tenuto a gestire il processo in coerenza con quanto stabilito dalla normativa in vigore.

Uno degli obiettivi principali del Responsabile della Conservazione è di definire ed impostare il processo per il trattamento della documentazione soggetta a conservazione.

Più in particolare (art. 7 del DPCM 03 dicembre 2013):

- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- 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;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo

stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

• **Soggetto Produttore**

Ente	Comune di Occhiobello
Sede Amministrativa	Piazza Giacomo Matteotti n.15, 45030 Occhiobello (RO)
Recapiti	0425766111
Sito web	www.comune.occhiobello.ro.it
Partita IVA	00197740293
Codice Fiscale	00131010290

Responsabile	Responsabile della Conservazione interno: RESPONSABILE AREA 1 – AFFARI GENERALI DELEGATO: RESPONSABILE AREA 2 - RAGIONERIA, CONTABILITÀ, CONTROLLO DI GESTIONE E FINANZE per la classe documentale delle fatture elettroniche attive e passive, mandati e reversali e per tutte le altre classi in caso di assenza del Responsabile della conservazione interno
Ente/Società	COMUNE DI OCCHIOBELLO
Data inizio incarico	partire dall'approvazione del presente Manuale
Data termine incarico	Fino a revoca

Il Responsabile della conservazione, avvalendosi della facoltà prevista dall'art. 5, comma 1, b) del DPCM 03/12/2013 ha affidato lo svolgimento delle attività del Responsabile del servizio della Conservazione ad un soggetto terzo che, per competenza ed esperienza, garantisce lo svolgimento delle suddette attività (si veda in proposito l'Allegato 2 - Affidamento del procedimento di conservazione).

Le attività sono state affidate ad InfoCert S.p.A., gestore del servizio di conservazione sostitutiva e digitale in outsourcing LegalDoc, Conservatore Accreditato presso AgID.

InfoCert assume l'incarico di svolgere le attività affidate dal Responsabile della Conservazione in accordo con quanto previsto dal contratto, dagli allegati contrattuali e dall'articolo dall'art. 5, comma 1, b) del DPCM 03/12/2013.

Per il dettaglio delle figure di Responsabilità interne al Conservatore si rimanda al Manuale della Conservazione standard di InfoCert.

L'atto di affidamento allo svolgimento delle attività del Responsabile della Conservazione è stato conferito dal Comune ad InfoCert contestualmente alla sottoscrizione del contratto di adesione al servizio LegalDoc.

- **InfoCert S.p.A.**

Denominazione sociale	InfoCert S.p.A.
Sede Legale	Piazza Sallustio, 9 00187 Roma Tel. +39 06 836691
Sedi Operative	Via Russoli, 5 20143 Milano Tel. +39 06836691
	Piazza da Porto, 3 35131 Padova Tel. +39 06836691
	Via Marco e Marcelliano, 45 00147 Roma Tel. +39 06836691
Sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
Codice Fiscale / Partita IVA	07945211006
Numero REA	RM – 1064345

InfoCert S.p.A. è il Primo Ente Certificatore per la firma digitale in Italia, leader di mercato per i processi di conservazione dei documenti a norma di legge e per i servizi di PEC.

InfoCert S.p.A. progetta e sviluppa soluzioni informatiche ad alto valore tecnologico per la dematerializzazione dei processi documentali di imprese, associazioni, ordini professionali, Pubblica Amministrazione e professionisti.

- **Oggetti sottoposti alla 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.

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nel documento 'Specifiche tecniche per l'integrazione'. Ad ogni documento il Sistema di conservazione associa un file XLM, detto Indice del Pacchetto di Archiviazione. L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto 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".

Il fine ultimo del processo di conservazione è rendere un documento inalterabile e imm modificabile, in modo che possa essere disponibile nel tempo nella propria autenticità ed integrità.

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 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 documento, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte
- eventuali informazioni relative al documento rettificante e rettificato
- il tempo di creazione (timestamp) del file IPdA
- l'impronta di Hash del documento.

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

LegalDoc integra il sistema di gestione documentale del Comune e ne estende i servizi consentendo di organizzare liberamente le fasi di creazione, utilizzo e archiviazione dei documenti, intervenendo solamente nella fase di conservazione e solamente per i documenti che il Comune sceglie di conservare.

• **Strumenti utilizzati**

Si rimanda al Manuale di Gestione del Protocollo e degli Archivi per la descrizione funzionale ed operativa del sistema di gestione informatica dei documenti adottato dal Comune, con particolare riferimento alle fasi di creazione, ricezione e smistamento.

Il principale strumento di lavoro per la gestione documentale è l'applicativo ADS, attraverso cui avviene la formazione automatica dei pacchetti di versamento. I documenti inseriti nei pacchetti di versamento sono statici, non modificabili e sono corredati da appositi indici di metadati, come specificato nell'Allegato 3 – Dati Tecnici di attivazione.

Il sistema di conservazione LegalDoc è configurato per accettare solo documenti in formati prestabiliti, con metadati minimi obbligatori e dimensioni massime concordate. Al venir meno di una di queste condizioni, sopraggiungendo l'impossibilità per LegalDoc di accettare il documento, lascia in attesa il documento in entrata senza immetterlo nel sistema di conservazione e contestualmente segnala l'anomalia a ADS. Il trattamento delle anomalie avviene mediante l'utilizzo di un'interfaccia web accessibile alle risorse preposte al monitoraggio degli invii in conservazione.

- **Formato dei documenti elettronici**

Le Regole Tecniche del DPCM del 3 dicembre 2013 elencano in modo specifico i formati documentali da adottare per la conservazione a lungo termine dei documenti nel loro Allegato 2.

Il Comune ha deciso l'invio in conservazione dei seguenti formati:

- PDF
- XML
- TIFF
- TXT
- DOCX
- ODT
- XLS
- XLSX
- JPG
- GIF
- PNG
- PPTX
- ZIP
- RAR
- **Tutti eventualmente firmati digitalmente e/o marcati temporalmente.**
- DOC solo se firmato e/o marcato temporalmente

- **Le tipologie documentali**

Tipologie documentali, metadati e formati sono sempre concordati con il Soggetto Produttore e dettagliati nell'Allegato 3 – Dati Tecnici di attivazione.

<i>Tipologia di documento</i>	Fattura elettronica PA attiva
<i>Natura del documento</i>	Originale digitale in formato xml eventualmente firmato digitalmente
<i>Data di decorrenza del processo di conservazione elettronica</i>	14/06/2017
<i>Modalità di versamento</i>	Tipologia documentale inviata in conservazione tramite LegalDoc

<i>Tipologia di documento</i>	Fattura elettronica PA passiva
<i>Natura del documento</i>	Originale digitale in formato xml eventualmente firmato digitalmente
<i>Data di decorrenza del processo di conservazione elettronica</i>	04/04/2017
<i>Modalità di versamento</i>	Tipologia documentale inviata in conservazione tramite applicativo "JCONS" di ADS

Tipologia di documento	Contratto
Natura del documento	Originale digitale firmato digitalmente
Data di decorrenza del processo di conservazione elettronica	12/06/2017
Modalità di versamento	Tipologia documentale inviata in conservazione tramite LegalDoc

Tipologia di documento	Atto collegiale
Natura del documento	Originale digitale firmato digitalmente
Data di decorrenza del processo di conservazione elettronica	04/07/2017
Modalità di versamento	Tipologia documentale inviata in conservazione tramite applicativo "SFERA" di ADS

Tipologia di documento	Atto monocratico
Natura del documento	Originale digitale firmato digitalmente
Data di decorrenza del processo di conservazione elettronica	04/07/2017
Modalità di versamento	Tipologia documentale inviata in conservazione tramite applicativo "SFERA" di ADS

Tipologia di documento	Registro giornaliero di protocollo
Natura del documento	Originale digitale eventualmente firmato digitalmente
Data di decorrenza del processo di conservazione elettronica	12/04/2017
Modalità di versamento	Tipologia documentale inviata in conservazione tramite applicativo "JCONS" di ADS

Tipologia di documento	Documento protocollato
Natura del documento	Originale digitale firmato digitalmente oppure copia per immagine (scansione) di originale analogico
Data di decorrenza del processo di conservazione elettronica	12/04/2017
Modalità di versamento	Tipologia documentale inviata in conservazione tramite applicativo "JCONS" di ADS

Tipologia di documento	Siope+ - Flussi ordinativi
Natura del documento	Originale digitale in formato xml eventualmente firmato digitalmente
Data di decorrenza del processo di conservazione elettronica	12/07/2019
Modalità di versamento	Tipologia documentale inviata in conservazione tramite applicativo "JCONS" di ADS

- **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 servizio LegalDoc 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 pacchetto, 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 si applica al pacchetto di archiviazione;
- **cancellazione logica 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, per cui sia conclusa l'apposita procedura di sdeamianizzazione presso la Soprintendenza archivistica di competenza occorre formulare apposita richiesta a InfoCert (scarto archivistico);
- **ricerca dei documenti informatici indicizzati**: il Soggetto Produttore 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**: 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).

La descrizione dell'architettura generale del sistema di conservazione è stata depositata in AgID in fase di accreditamento e per ogni dettaglio infrastrutturale si rimanda al Manuale della Conservazione standard di InfoCert.

- **Responsabilità del processo di conservazione**

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

Responsabilità> Attività	Comune	GestionaleADS	LegalDoc	Responsabile del servizio della Conservazione
• Formazione del documento	R – E			
• Indicizzazione e archiviazione	R – E			
• Acquisizione documento e creazione del file con le direttive di conservazione	V	R - E		
• Invio al sistema di conservazione	V	R – E		
• Verifica e accettazione del documento e produzione del rapporto di versamento			E - V	
• Sottoscrizione del rapporto di versamento			E	R - V* - A
• Marca temporale del rapporto di versamento			E	R - V* - A
• Memorizzazione, creazione “copia di sicurezza” e chiusura del processo			E	R - V* - A
[R-responsabile; E-esegue; V- verifica; A-approva]				

(*) Tutte le verifiche in carico al Responsabile del servizio della Conservazione sono garantite anche dal servizio di auditing InfoCert.

- **Fasi del processo di conservazione: dettaglio**

- **Formazione del documento**

INPUT	<i>Documento da generare</i>	
Comune	1.1	Il Comune genera/riceve i documenti da conservare
OUTPUT	<i>Documento generato/ricevuto</i>	

- **Indicizzazione e archiviazione**

INPUT	<i>Documento da archiviare</i>	
Comune	2.1	I documenti da inviare in conservazione vengono corredati dei relativi metadati attraverso il gestionale ADS
OUTPUT	<i>Documento indicizzato</i>	

- **Acquisizione documento e creazione del file delle direttive**

INPUT	<i>File delle direttive da predisporre</i>	
Gestionale ADS	3.1	Il servizio web service acquisisce i documenti informatici predisposti dal Comune e li prepara alla conservazione.
	3.2	Il servizio predispose il pacchetto di versamento contenente i documenti da conservare e i file di metadati ad essi associati. In particolare:

		• Predisposizione del file con le direttive di conservazione; • Predisposizione del file di indice; • Calcolo delle impronte dei file costituenti il documento; • Inserimento delle impronte nel file delle direttive; • Costruzione del messaggio contenente i file che costituiscono il documento.
OUTPUT	<i>Pacchetto di versamento predisposto</i>	

• **Invio al sistema di conservazione**

INPUT	<i>Pacchetto di versamento da inviare a LegalDoc</i>	
Gestionale ADS	4.1	Invoca i servizi di LegalDoc e invia il pacchetto di versamento e la relativa richiesta di conservazione.
OUTPUT	<i>Pacchetto di versamento inviato a LegalDoc</i>	

• **Verifica, accettazione e invio della ricevuta di accettazione del pacchetto**

INPUT	<i>Pacchetto da verificare</i>	
LegalDoc	5.1	Acquisizione del documento.
	5.2	Sbustamento del messaggio e verifica della firma elettronica apposta sul file delle direttive di conservazione.
	5.3	Presa in carico dei file costituenti il documento.
	5.4	Esecuzione di una serie di verifiche sulla completezza e sulla correttezza delle informazioni contenute nel file delle direttive di conservazione.
	5.5	Generazione dell'impronta di ogni file del documento.
	5.6	Confronto dell'impronta generata con la corrispondente inviata dal Produttore per garantire l'integrità del documento ricevuto.
	5.7	Nel caso di esito negativo delle verifiche, il documento viene respinto con l'indicazione che descrive l'errore intercorso. In questo caso il flusso termina.
	5.8	Generazione del file di ricevuta a partire dal file delle direttive.
	5.9	Generazione di un identificativo univoco per il documento (Token LegalDoc) e firma digitale sul file di ricevuta.
	5.10	Invio del file di ricevuta di presa in carico della richiesta di conservazione.
Gestionale ADS	5.11	Riceve il file di ricevuta di presa in carico della richiesta di conservazione e ne estrae il Token LegalDoc.
	5.12	Il Token LegalDoc è memorizzato presso il <i>Gestionale ADS</i> .
OUTPUT	<i>Documento verificato</i>	

• **Creazione del pacchetto di archiviazione**

INPUT	<i>Pacchetto di archiviazione da formare</i>	
LegalDoc	6.1	Predisposizione del file di controllo del documento contenente l'indice del documento, le impronte dei file che lo costituiscono, la classificazione anagrafica del documento, gli estremi di identificazione del Responsabile del servizio della Conservazione.
	6.2	Apposizione della firma digitale del Responsabile del servizio della Conservazione sul file di controllo e sul file di indice.

OUTPUT	<i>Pacchetto di archiviazione conservato</i>
---------------	--

- **Memorizzazione, creazione copia di sicurezza e chiusura della conservazione**

INPUT	<i>Pacchetto di archiviazione da memorizzare</i>	
LegalDoc	7.1	Memorizzazione del pacchetto su supporto magnetico.
	7.2	Creazione della copia di sicurezza.
	7.3	Termine della procedura di conservazione.
OUTPUT	<i>Pacchetto conservato</i>	

- **Processo di ricerca ed esibizione**

Le procedure di ricerca ed esibizione di un documento conservato in LegalDoc permettono di estrarre dal sistema un documento di cui sia completata la procedura di conservazione, utilizzando il token LegalDoc o uno o più metadati associati al documento in fase di versamento.

L'accesso all'esibitore è consentito attraverso l'apposita interfaccia di LegalDoc WEB, per la quale sono state configurate 6 utenze:

NUMERO UTENZE	CODICE RIFERIMENTO TIPOLOGIA	FUNZIONALITA'	
		VERSAMENTO	ESIBIZIONE
1	Tutte (tramite web service ADS)	x	x
1	Fatture PA attive e passive		x
1	Atti collegiali e monocratici		x
1	Contratti	X	x
1	Registro giornaliero di protocollo e documento protocollato	X	x
1	Ordinativi e Certificati	x	x

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 una qualsiasi postazione di lavoro (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 qualificano il processo di conservazione attestandone il corretto svolgimento;
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione;

- verificare l'integrità del documento.

L'esibizione del documento ottenuto tramite interrogazione al sistema LegalDoc rappresenta un'esibizione completa, legalmente valida ai sensi delle Regole Tecniche del 03 dicembre 2013.

- **Procedura di esibizione: dettaglio**

- **Ricerca del documento da esibire**

<i>INPUT</i> <i>Lista di documenti</i>	
LegalDoc WEB 1.1	La ricerca avviene nel portale LegalDoc WEB, utilizzando gli indici di metadati con cui è stato versato il documento.
<i>OUTPUT</i> <i>Token relativo al documento da esibire</i>	

- **Invio della richiesta a LegalDoc**

<i>INPUT</i> <i>Richiesta di esibizione da preparare</i>	
LegalDoc WEB	2.1 LegalDoc WEB seleziona il token relativo al documento da esibire.
	2.2 Creazione del file delle direttive di esibizione, contenente il token LegalDoc relativo al documento da esibire, e sua sottoscrizione digitale.
	2.3 Chiamata al servizio LegalDoc.
<i>OUTPUT</i> <i>Richiesta di esibizione presa in carico da LegalDoc</i>	

- **Ricerca del documento nel sistema ed esibizione**

<i>INPUT</i> <i>Richiesta di esibizione acquisita</i>	
LegalDoc	3.1 Ricezione della richiesta di esibizione del documento.
	3.2 Controllo di corrispondenza tra il token LegalDoc inviato dal Produttore e quelli dei documenti conservati.
	3.3 Predisposizione delle copie di: • file costituenti il documento conservato; • file di ricevuta; • file di controllo del documento.
	3.4 Passaggio del pacchetto di distribuzione all'Esibitore.
<i>OUTPUT</i> <i>Documento passato all'Esibitore</i>	

- **Verifica del documento**

<i>INPUT</i> <i>Documento ricevuto dal sistema di conservazione</i>	
Esibitore LegalDoc 4.1	Visualizzazione del pacchetto di file ed effettuazione di tutte le verifiche.
<i>OUTPUT</i> <i>Documento esibito</i>	

- **Verifica del documento**

<i>INPUT</i> <i>Documento esibito</i>	
Esibitore LegalDoc 5.1	Download del documento e memorizzazione dello stesso in locale.

- **Il sistema di conservazione**
- **Configurazione dei sistemi e modalità di erogazione**

Il sistema di conservazione LegalDoc 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 servizio è accessibile dalla apposita URL di rete, e ADS richiama i servizi di LegalDoc attraverso chiamate web service concordate.

La figura 1 offre uno schema esemplificativo del dialogo tra l'applicazione del Soggetto Produttore e LegalDoc, distinguendo le parti che rimangono sotto la responsabilità del Produttore da quelle di competenza di InfoCert.

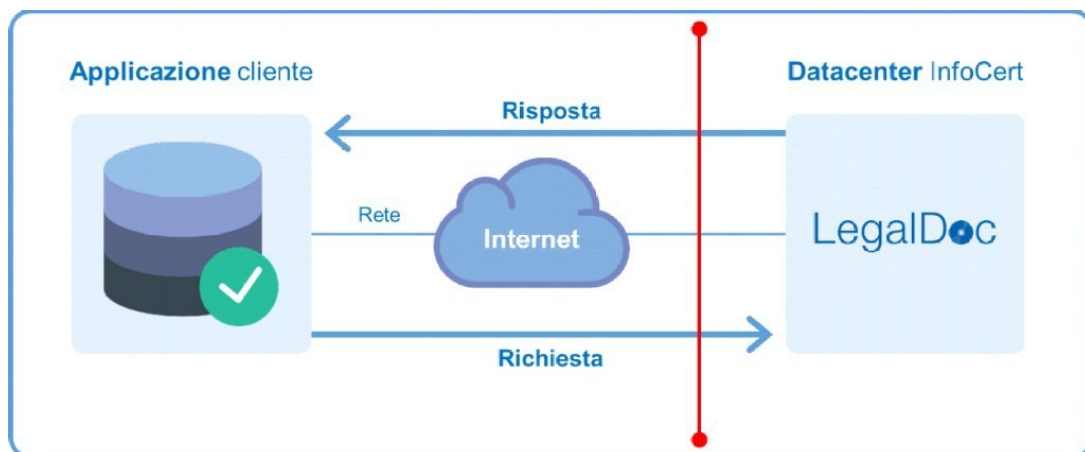


Figura 1 - Dialogo tra il sistema di gestione e il sistema di conservazione documentale LegalDoc

- **Componenti**
- **Marca temporale**

Per l'emissione delle marche temporali LegalDoc si avvale del sistema di marcatura di InfoCert, Certification Authority accreditata. 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 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.

- **Firma digitale con dispositivo HSM**

Al buon esito del processo di conservazione, il Responsabile del servizio della Conservazione di InfoCert appone la propria firma digitale su ogni pacchetto di archiviazione, mediante un sistema di firma

automatica erogato dalla CA InfoCert, che si avvale di un dispositivo crittografico ad altre prestazioni HSM.

- **Posta Elettronica Certificata**

Il servizio LegalDoc si avvale del servizio PEC di InfoCert: in sede di attivazione del servizio, è stata definita una casella di posta certificata tramite la quale richiedere attività di supporto e inviare messaggi in genere alla casella di amministrazione assistenza.legaldoc@legalmail.it.

- **Controlli**

I processi del servizio di conservazione sostitutiva LegalDoc sono fortemente automatizzati; i sistemi di erogazione sono dotati di molteplici funzioni di controllo in grado di rilevare e segnalare eventuali anomalie in essere o potenziali.

I controlli effettuati possono essere distinti secondo le seguenti tipologie:

- controlli di processo;
- controlli periodici.

- **Controlli di processo**

I controlli di processo sono i controlli che hanno luogo durante l'elaborazione dei documenti soggetti al processo di conservazione.

LegalDoc è un processo complesso che movimentata una consistente mole di dati, dei quali è necessario garantire costantemente l'integrità e la coerenza: per questo motivo sono attivati numerosi controlli automatici, che richiedono l'intervento del Responsabile del servizio della Conservazione solo al verificarsi di eventuali eventi anomali non gestibili in modo automatico.

Oltre a questi, le procedure di gestione del sistema prevedono un elenco di controlli manuali effettuati direttamente dal Responsabile della Conservazione interno o da un suo delegato.

- **Controlli periodici**

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

La struttura si avvale di un gruppo di lavoro trasversale all'azienda e utilizza strumentazioni di varia natura per la raccolta di dati relativi al funzionamento dei servizi. Il gruppo si riunisce periodicamente per discutere dei malfunzionamenti registrati nel periodo e delle soluzioni adottate o potenziali per evitare il ripresentarsi dell'inconveniente.

- **Ispezione del sistema da parte delle autorità competenti**

In occasione delle ispezioni del sistema di conservazione da parte delle autorità competenti, gli esiti delle stesse e gli eventuali rilievi apposti sono registrati su appositi verbali.

Qualora dalle attività di ispezione e controllo emergessero punti critici o aree di miglioramento, è impegno di InfoCert l'attivazione delle strutture competenti per la tempestiva analisi della situazione e

l'approntamento di tutte le misure necessarie al miglioramento del sistema e/o delle performance.

- **Incident management**

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

I fornitori dei sistemi tecnologici utilizzati forniscono ad InfoCert tutte le opportune assicurazioni, rese per iscritto, contro il rischio di perdita dei documenti conservati.

Qualora si verificassero incidenti di sistema o di processo, le operazioni di ripristino della funzionalità seguono le procedure definite e documentate; per ogni incidente con impatti sul rispetto della normativa, è redatto un apposito verbale secondo la procedura definita.

Il Responsabile del servizio della Conservazione mantiene il verbale degli incidenti e delle contromisure attuate, che divengono oggetto di opportuni incontri di miglioramento.

- **Sicurezza fisica**

I locali che ospitano il sistema LegalDoc sono in un immobile la cui zona d'ubicazione non presenta rischi ambientali dovuti alla vicinanza ad installazioni pericolose. Durante la progettazione dello stabile sono stati presi opportuni accorgimenti per isolare i locali potenzialmente pericolosi, quali quelli contenenti il gruppo elettrogeno e la centrale termica. Per questi locali sono presenti le apparecchiature e gli accessori di controllo e di sicurezza previsti dalle norme in vigore. Lo stabile è inoltre sorvegliato da personale specializzato 24 ore al giorno.

La sala CED è l'area protetta all'interno dello stabile, accessibile mediante utilizzo del badge autorizzato, dove si trovano i dispositivi hardware e software dei diversi sistemi InfoCert.

L'accesso alla sala CED è consentito solamente alle persone autorizzate, ossia quelle con un ruolo operativo nell'erogazione del servizio e nella gestione dell'infrastruttura.

All'interno della sala CED sono collocate le sale denominate locale CA, accessibili mediante badge autorizzato e PIN (Personal Identification Number) di accesso. L'accesso ai singoli locali della CA necessita di un ulteriore badge autorizzato.

La sala CED è dotata di telecamere a circuito chiuso, rilevatori combinati microonde e infrarossi, rilevatori ottici di fumo sul soffitto e nel sottopavimento, avvisatori manuali di allarme, avvisatori ottici acustici d'allarme per avviso locale, sensori piezodinamici per la rilevazione della rottura dei vetri. Tutte le porte sono dotate di allarme.

- **Gruppi di continuità**

Tutte le apparecchiature del centro dati di InfoCert a Padova sono collegate alla rete elettrica attraverso gruppi di continuità che consentono di mantenere l'alimentazione alle apparecchiature in caso di interruzione dell'energia elettrica da parte del fornitore. In caso di assenza dell'alimentazione per pochi cicli, intervengono automaticamente delle batterie tampone in grado di mantenere la continuità elettrica. Qualora l'assenza di alimentazione si protragga per più di pochi secondi, vengono automaticamente avviati dei gruppi elettrogeni che iniziano a fornire l'alimentazione al gruppo di continuità.

- **Connessione a Internet**

Il centro dati di InfoCert è connesso alla rete Internet con due collegamenti ATM separati, entrambi con velocità massima di 155 Mbit/sec.

Tali collegamenti sono attestati su POP distinti, con percorsi fisici e apparati di interfaccia separati e completamente ridondati.

InfoCert è impegnata a mantenere tempi di attraversamento rete inferiori a 20 ms tra il proprio Centro Servizi e i nodi d'interconnessione con i principali provider italiani e internazionali.

- **Sicurezza delle reti: protezione da intrusioni**

I sistemi e le reti di InfoCert sono connessi ad Internet in modo controllato da sistemi firewall che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet, reti DMZ (DeMilitarized Zone) o Perimetrali, Reti Interne. Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del firewall, sulla base di un set di regole stabilite.

Le regole definite sui firewall vengono progettate in base a due principi: in primis il “default deny”, ossia quanto non è espressamente permesso è vietato di default ed è, quindi, consentito solo quanto è strettamente necessario al corretto funzionamento dell'applicazione. Il secondo principio consiste nel “defense in depth”, secondo il quale vengono organizzati livelli successivi di difesa, prima a livello di rete, tramite successive barriere firewall, poi a livello di sistema (hardening).

InfoCert provvede alla gestione e all'implementazione delle regole di sicurezza dei firewall. I sistemi firewall sono configurati in alta affidabilità (HA), ovvero sono formati da coppie di macchine indipendenti, collegate tra loro e gestite tramite appositi software in modo che, in caso di guasto di una delle macchine, il traffico venga dirottato sulla macchina di backup.

- **Protezione dei dati personali**

Nelle fasi di creazione, digitalizzazione, trattamento e invio in conservazione della documentazione cartacea e elettronica, il Comune pone la massima cura nel rispetto delle disposizioni stabilite dal D.Lgs n. 196/2003 “Codice in materia di protezione dei dati personali”.

Ai sensi dell'articolo 29 del Codice, il Comune ha nominato InfoCert S.p.A. Responsabile dei trattamenti dei dati necessari all'esecuzione del servizio (Atto di Affidamento - Allegato 2).

In particolare, anche in considerazione del ruolo di Responsabile del servizio della Conservazione ricoperto, i compiti affidati ad InfoCert S.p.A. attengono a qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la selezione, l'estrazione, l'interconnessione, la comunicazione, la cancellazione e la distruzione di dati.

InfoCert opera quale Responsabile del trattamento applicando le misure di sicurezza in base alle disposizioni legislative e regolamentari in vigore.

L'informativa di cui all'articolo 13 del D.Lgs. 196/2003 per i dati relativi al contratto è resa al Comune nell'Atto di Affidamento Allegato al materiale contrattuale da questi sottoscritto, ove viene altresì allo stesso consentito di esprimere il consenso per gli ulteriori trattamenti indicati.

- **Allegati**

Si fornisce di seguito un elenco dei documenti contrattuali a cui il Manuale si riferisce.

I documenti sotto riportati si intendono come riferimenti ufficiali: eventuali discrepanze fra quanto indicato nel Manuale e quanto presente nei documenti presenti nel seguente elenco si risolvono in favore

di questi ultimi.

- Condizioni Generali di Contratto – Regola il rapporto tra InfoCert e il Comune;
- Atto di affidamento del procedimento di conservazione sostitutiva – formalizza l'affidamento ad InfoCert del processo di conservazione, delineandone l'ambito di applicazione;
- Richiesta di attivazione – contenente gli accordi economici per l'attivazione del servizio;
- Dati tecnici di attivazione – contenente il dettaglio delle tipologie documentali, dei formati e dei metadati concordati;
- Manuale utente esibitore LegalDoc WEB.
- File di Configurazione dell'ambiente di conservazione;