



COMUNE DI MONSELICE

Manuale dei processi di formazione e conservazione dei documenti elettronici

Delibera di Giunta n. 70 del 16/04/2015



INDICE

1	Introduzione al documento	5
1.1	Gestione versioni documento.....	5
1.2	Scopo e campo di applicazione del documento.....	5
1.3	Principi di redazione.....	5
1.4	Termini e definizioni.....	6
1.5	Acronimi.....	8
2	Nomine e individuazione dei compiti	9
2.1	Cliente.....	9
2.2	Referenti di processo.....	9
2.3	Responsabile della conservazione.....	9
2.4	InfoCert SPA.....	10
2.4.1	Identificazione del sistema di conservazione.....	10
2.4.2	Supporto offerto dal sistema di conservazione.....	11
3	Fondamenti normativi	12
3.1	Introduzione.....	12
3.2	Il quadro normativo.....	12
3.3	Principali riferimenti normativi.....	13
3.4	La conservazione sostitutiva dei documenti.....	14
3.5	La deliberazione CNIPA n. 11 del 19 febbraio 2004.....	
3.6	Il responsabile della conservazione.....	
3.7	La normativa in pratica.....	17
4	Il sistema di creazione e gestione dei documenti	18
4.1	Strumenti utilizzati.....	18
4.1.1	Servizi di certificazione.....	18
4.2	Controlli.....	18
4.3	Indicizzazione dei documenti.....	18
4.4	Gestione delle anomalie.....	18
4.5	Formato dei documenti elettronici.....	18
5	Il sistema di conservazione documentale	19
5.1	Descrizione generale del servizio.....	19
5.2	Definizione di documento.....	19
5.3	Configurazione dei sistemi.....	20
5.3.1	Modalità di erogazione.....	20



5.4	Componenti.....	20
5.4.1	Marca temporale.....	20
5.4.2	Firma digitale con dispositivo HSM.....	21
5.4.3	Supporti di conservazione.....	21
5.4.4	Posta Elettronica Certificata.....	21
5.5	Controlli.....	21
5.5.1	Controlli di processo.....	21
5.5.2	Controlli periodici.....	22
5.5.3	Ispezione del sistema da parte delle autorità competenti.....	22
5.5.4	Incident management.....	22
6	Le tipologie documentali²³	
6.1	Contratti.....	23
6.2	Atti Amministrativi.....	23
6.3	Allegati.....	24
6.3.1	Fasi del processo.....	24
7	Il processo di conservazione 26	
7.1	Processi di front-end.....	26
7.2	Processi di back-end.....	26
7.3	Fasi del processo di conservazione: schema generale.....	27
7.4	Responsabilità del processo di conservazione.....	27
7.5	Fasi del processo di conservazione: dettaglio.....	28
7.5.1	Formazione del documento.....	28
7.5.2	Indicizzazione e archiviazione.....	28
7.5.3	Acquisizione documento e creazione del file delle direttive.....	29
7.5.4	Invio al sistema di conservazione.....	29
7.5.5	Verifica, accettazione e invio della ricevuta di accettazione del documento.....	29
7.5.6	Inserimento nel lotto e creazione del file di controllo.....	30
7.5.7	Chiusura del lotto e attestazione di corretto procedimento.....	30
7.5.8	Memorizzazione, creazione copia di sicurezza e chiusura della conservazione.....	30
8	Procedure di ricerca ed esibizione 32	
8.1	Procedura di esibizione: schema generale.....	32
8.2	Procedura di esibizione: dettaglio.....	33
8.2.1	Ricerca del documento da esibire.....	33
8.2.2	Invio della richiesta a LegalDoc.....	33
8.2.3	Ricerca del documento nel sistema ed esibizione.....	33
8.2.4	Verifica del documento.....	33
8.2.5	Verifica del documento.....	33
8.3	Requisiti software.....	34
9	Modifica dei documenti posti in conservazione 35	



9.1	La cancellazione di un documento.....	35
10	Misure di sicurezza	36
10.1	Comune di Monselice.....	36
10.2	InfoCert.....	36
10.2.1	Sicurezza fisica.....	36
10.2.2	Gruppi di continuità.....	36
10.2.3	Connessione a Internet.....	36
10.2.4	Sicurezza delle reti: protezione da intrusioni.....	37
11	Note conclusive	38
11.1	Procedure di riversamento.....	38
11.1.1	Riversamento diretto.....	38
11.1.2	Riversamento sostitutivo.....	38
11.2	Protezione dei dati personali.....	38
12	Allegati	39
12.1	Documentazione contrattuale di riferimento.....	39



1 Introduzione al documento

1.1 Gestione versioni documento

Versione:	01	Data Versione:	25/06/2014
Descrizione modifiche:	Nessuna		
Motivazioni:	Prima emissione		

1.2 Scopo e campo di applicazione del documento

Il presente documento è il Manuale dei processi di formazione e conservazione elettronica dei documenti (di seguito anche "Manuale della Conservazione") redatto dal Comune di Monselice.

Il Manuale ha lo scopo di raccogliere le diverse normative in materia e di documentare il processo di conservazione dei documenti elettronici.

Inoltre, descrive tutte le procedure e le prassi seguite dal Comune di Monselice (di seguito anche "Comune") in materia di gestione della sicurezza del servizio, dei documenti e delle informazioni trattate: questa parte costituisce il regolamento operativo di tutti i processi di digitalizzazione dei documenti di conservazione digitale.

In caso di ispezione da parte delle Autorità di Vigilanza o di altri organismi a ciò deputati, il Manuale permette un agevole svolgimento di tutte le attività di controllo e costituisce una importante dimostrazione dell'impegno dell'Ente al rispetto delle norme.

Il documento si applica al servizio LegalDoc fornito in modalità ASP (Application Service Providing) da InfoCert SpA secondo uno schema di Business Process Outsourcing (BPO).

Il Manuale è organizzato per sezioni:

1. la prima sezione (capitoli 1-3) contiene una panoramica di tutte le leggi e i decreti che regolano la materia, fornisce il profilo del Comune di Monselice, il profilo di InfoCert e dettaglia la configurazione dei sistemi utilizzati per l'erogazione;
2. la seconda sezione (capitoli 4-9) descrive il servizio LegalDoc, il responsabile della conservazione, descrive i macro flussi operativi definiti per la gestione della documentazione elettronica. Inoltre, è dettagliato il procedimento di conservazione posto sotto la responsabilità di InfoCert in virtù della delega allo svolgimento delle attività di competenza del Responsabile della Conservazione, sottolineando input, output e responsabilità di ogni fase. Infine, vengono descritti i controlli effettuati e i processi ricerca e esibizione a norma dei documenti conservati.
3. la terza sezione (capitoli 10-12) riporta le misure fisiche e logiche di sicurezza adottate, cenni sui riversamenti, i riferimenti alla normativa e alla policy sulla protezione dei dati personali e gli allegati al Manuale.

1.3 Principi di redazione

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



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

1.4 Termini e definizioni

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.
CONSERVAZIONE SOSTITUTIVA	vedi conservazione
CONSERVAZIONE	il processo che consente di conservare i documenti in modalità informatica a norma di legge e che risponde a quanto stabilito nel DPCM 03/12/2013
DOCUMENTO ANALOGICO ORIGINALE	documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
DOCUMENTO INFORMATICO	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
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
EVIDENZA INFORMATICA	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (all. 1 DPCM 03/12/2013)
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.
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)	la sequenza dei simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (all. 1 DPCM 03/12/2013).
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
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.
RESPONSABILE DELLA CONSERVAZIONE	il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione ottica sostitutiva 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.
HARDWARE SECURITY MODULE	dispositivo crittografico ad alte prestazioni utilizzato per apporre automaticamente la firma digitale e la validazione temporale ad elevati volumi di documenti informatici
POSTA ELETTRONICA CERTIFICATA	sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici



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.
-----------------------------------	---

1.5 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



2 Nomine e individuazione dei compiti

In questo capitolo sono individuati i differenti soggetti che intervengono a vario titolo nelle diverse fasi del processo di creazione dei documenti elettronici, digitalizzazione dei documenti cartacei e conservazione elettronica documentale.

2.1 Cliente

Ente	Comune di Monselice
Sede Amministrativa	Piazza San Marco n. 1 – 35043 Monselice (Padova)
Recapiti	Telefono 0429 786911 Fax 0429 73092
Sito web	www.comune.monselice.padova.it
Partita IVA	00654440288
Codice Fiscale	00654440288

2.2 Referenti di processo

Nominativo dei soggetti del Comune di Monselice incaricati della gestione del sistema di creazione dei documenti e di invio dei documenti in conservazione.

Nome e Cognome	Maurizio Montin
Ente	Comune di Monselice

2.3 Responsabile della conservazione

Il Comune di Monselice, avvalendosi della facoltà prevista dalla Deliberazione CNIPA 11/2004, articolo 5, commi 2 e 3, e dal DPCM 03/12/2013, art. 5, comma 2 b), ha affidato lo svolgimento delle attività del Responsabile della Conservazione ad un soggetto terzo che, per competenza ed esperienza, garantisce lo svolgimento delle suddette attività.

Le attività sono state affidate ad InfoCert SpA, gestore del servizio di conservazione sostitutiva in outsourcing LegalDoc.

InfoCert assume l'incarico di svolgere le attività delegate dal Responsabile della Conservazione in accordo con quanto previsto dal contratto, dagli allegati contrattuali e dall'articolo 5 della Deliberazione CNIPA 11/2004, che ne delinea i compiti.

InfoCert SpA provvede ad affidare lo svolgimento delle attività delegate dal Responsabile della Conservazione ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dagli allegati contrattuali.

L'incaricato di InfoCert può delegare lo svolgimento di parte del processo a una o più persone con adeguata competenza ed esperienza, secondo quanto previsto nella documentazione interna di organizzazione e gestione del servizio di conservazione.



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

2.4 InfoCert SPA

Denominazione sociale	InfoCert SpA
Sede Legale:	Piazza Sallustio, 9 00187 Roma Tel. +39 06 442851 Fax +39 06 44285255
Sedi Operative:	Via Russoli, 5 20143 Milano Tel. +39 02 87286700
	Corso Stati Uniti, 14 35127 Padova Tel. +39 049 8288111 Fax +39 049 8288406
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 sostitutiva dei documenti a norma di legge e per i servizi di Posta Elettronica Certificata.

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.

Identificazione del sistema di conservazione

Il Responsabile della Conservazione InfoCert viene identificato nel sistema LegalDoc grazie alla definizione di un particolare utente con il ruolo di "responsabile del procedimento di conservazione".

Gli estremi identificativi di questo particolare utente (organizzazione di appartenenza, cognome, nome, codice fiscale) sono, inoltre, riportati anche nelle informazioni associate ai documenti conservati (nelle informazioni relative ad ogni documento e nel file di chiusura lotto).



Supporto offerto dal sistema di conservazione

LegalDoc supporta il Responsabile della Conservazione InfoCert nel controllo dell'effettiva leggibilità dei documenti conservati e mantiene la tracciatura delle esibizioni effettuate, considerate una ulteriore prova di leggibilità.

Il sistema gestisce in maniera automatica i parametri di organizzazione del contenuto dei supporti di memorizzazione e le procedure di sicurezza e di tracciabilità, fondamentali per la corretta conservazione del documento conservato.

Il sistema supporta il Responsabile della Conservazione nell'archiviazione delle informazioni relative a ogni supporto di memorizzazione utilizzato attraverso specifiche funzionalità, sulle quali egli esercita l'attività di controllo e di supervisione.

LegalDoc, inoltre, fornisce al Responsabile della Conservazione InfoCert un set di funzionalità per il mantenimento dell'archivio delle diverse versioni del software in gestione e il monitoraggio sia del flusso di documenti elaborati dal sistema, sia dei server specializzati. Il sistema, infatti, segnala ogni anomalia riscontrata, consentendo un pronto intervento e assicurando un monitoraggio costante.



3 Fondamenti normativi

3.1 Introduzione

Le realtà aziendali e di Pubblica Amministrazione avvertono in maniera sempre crescente la necessità di ottenere e gestire informazioni corrette, tempestive, aggiornate, autentiche, integre, logicamente accessibili, protette e disponibili nel tempo. Riuscire a garantire queste caratteristiche permette alla dirigenza di rispondere in maniera adeguata alle richieste interne o esterne all'ente e di trasformarle in un reale vantaggio.

Al crescere dei volumi della documentazione prodotta, il costo per archiviare e conservare nel tempo le informazioni in modo organizzato è ingente e può creare inutili processi di burocratizzazione. Per questi motivi una ben organizzata adozione del documento digitale consente di ridurre i costi e supportare efficacemente l'attività dell'ente.

3.2 Il quadro normativo

Il contesto normativo in cui si inquadra la conservazione sostitutiva risale al 1994, ma è solo a partire dall'anno 2004 che interventi più significativi hanno reso possibile la conservazione dei documenti in formato digitale valevole anche ai fini fiscali. Senza ripercorrere in dettaglio tutto l'exkursus legislativo, se ne fornisce di seguito una panoramica per una più agevole comprensione dell'intero quadro normativo.

La legge numero 537 del 24 dicembre 1993 "Interventi correttivi di finanza pubblica" (GU n. 303 del 28 dicembre 1993) affronta per la prima volta il tema di una modalità alternativa di conservare (e conseguentemente esibire) dei documenti a fini amministrativi. La norma introduce nell'ordinamento la possibilità di conservare scritture e documenti contabili "sotto forma di registrazioni su supporti di immagini" ed estende questa possibilità anche a tutte le scritture e i documenti rilevanti ai fini delle disposizioni tributarie.

Le relative modalità operative, tuttavia, sono rimandate ad un decreto del Ministero delle Finanze, emanato solamente dieci anni più tardi (23 gennaio del 2004) permettendo l'avvio concreto del processo.

Nel frattempo, è stato completato il quadro normativo relativo al documento informatico, alla firma digitale e alla fattura elettronica (a titolo non esaustivo si citano il Testo Unico sulla documentazione amministrativa – TU 445/2000, il Decreto del Presidente del Consiglio dei Ministri 8/02/1999 ora sostituito dal Decreto del Presidente del Consiglio dei Ministri del 13/01/2004, le numerose deliberazioni AIPA – poi divenuta CNIPA, ora DigitPA –, il Decreto Ministero Economia e Finanze 23 gennaio 2004 e il Decreto Legislativo 52 del 20 febbraio 2004, relativi a specifiche tipologie di documenti).

Inoltre, è stato emanato il "Codice Dell'Amministrazione digitale", il D.Lgs n. 82 del 7 marzo del 2005 (GU 16/05/2005 s.o. n. 93/L) entrato in vigore a partire dal 1 gennaio 2006, che vuole contribuire a rendere ancora più omogeneo il quadro di riferimento; da questa data tutte le disposizioni non riunite e coordinate all'interno del Codice sono state abrogate. Il Codice è stato recentemente rivisto dal D.Lgs. n. 235 del 30 dicembre 2010, allo scopo di rendere il quadro normativo più coerente alle innovazioni tecnologiche occorse negli ultimi anni.

Infine il DPCM 03/12/2013 (GU n. 59 del 12-03-2014) 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, traccia le regole per la conservazione a norma, andando ad abrogare la Deliberazione CNIPA 11/2004. Si precisa che i sistemi di conservazione già esistenti alla data di entrata in vigore del presente decreto sono adeguati entro e non oltre 36 mesi dall'entrata in vigore del decreto 03/12/13 secondo un piano dettagliato. Fino al completamento di tale processo per tali sistemi possono essere applicate le previgenti regole tecniche. Fino al completamento di tale processo restano validi i sistemi di conservazione realizzati ai sensi della deliberazione CNIPA n. 11/2004. Il Responsabile della conservazione valuta l'opportunità di riversare nel nuovo sistema di conservazione gli archivi precedentemente formati o di



mantenerli invariati fino al termine di scadenza di conservazione dei documenti in essi contenuti, così come previsto dall'Art. 14 del DPCM 03/12/13.

3.3 Principali riferimenti normativi

1. *Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445* – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. Testo coordinato con le modifiche apportate dal D.Lgs 23 gennaio 2002, n. 10 e dal DPR 7 aprile 2003, n. SQ01-00-02 Procedura per la gestione della documentazione.
Questo DPR è stato per la maggior parte sostituito dal Codice dell'amministrazione digitale in vigore dal 1° gennaio 2006.
2. *Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche* – Codice in materia di Protezione dei Dati Personali
3. *Decreto del 23 gennaio 2004 del Ministero dell'Economia e delle Finanze* – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto.
4. *Deliberazione CNIPA n. 11 del 19 febbraio 2004* – Regole tecniche per la riproduzione e conservazione su supporto ottico idoneo a garantire al conformità dei documenti agli originali.
5. *Decreto Legislativo del 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale* – Testo che rappresenta la base per tutti i successivi interventi che verranno in tema di uso dei documenti digitali. In dettaglio si definiscono nuovamente i ruoli e le caratteristiche dei documenti informatici e se ne amplia l'utilizzo; in particolare, la PA vede imporre un uso delle tecnologie informatiche e la pressoché totale dematerializzazione dei documenti nei rapporti tra cittadini, imprese e pubblica amministrazione.
6. *Decreto-Legge 29 novembre 2008, n. 185, coordinato con la legge di conversione 28 gennaio 2009, n. 2 – Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale* – Modifiche al CAD in materia di copie informatiche di documenti analogici, modifiche al Codice Civile in materia di documentazione informatica
7. *Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009* – Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici
8. *Decreto Legislativo del 30 dicembre 2010* – Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.
9. *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 (GU n.117 del 21-5-2013).
10. Il Decreto denominato sviluppo-bis, (dl 179/2012 convertito in legge 221/2012) modificando l'articolo 11, comma 13, del Codice dei contratti pubblici (D.L.vo 163/2006), ha introdotto nell'ordinamento l'obbligo che i contratti della pubblica amministrazione si stipulino esclusivamente in forma elettronica e non cartacea, almeno quando siano stipulati per atto pubblico notarile o in forma pubblica amministrativa.



11. *Il DPCM 03/12/2013 (GU n. 59 del 12-03-2014) 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, traccia le regole per la conservazione a norma, andando ad abrogare la Deliberazione CNIPA 11/2004.*

3.4 La conservazione sostitutiva dei documenti

L'implementazione e la gestione dei processi di creazione e conservazione dei documenti elettronici e di conservazione sostitutiva è una operazione che si avvale di numerosi strumenti ed elementi, regolata da apposite discipline che vanno raccordate alla disciplina generale della conservazione.

Di seguito si richiamano i principali strumenti ed elementi:

- **Documento informatico:** è una realtà immateriale e il tipo di supporto fisico sul quale esso è registrato è irrilevante per la natura del documento stesso.
Del documento informatico, a differenza di quello cartaceo, è possibile avere molteplici esemplari, tutti giuridicamente rilevanti e aventi identico valore legale. Per le sue caratteristiche, il documento informatico necessita di strumenti di validazione informatica efficaci e sicuri affinché ne siano garantite, in particolare, l'integrità e l'autenticità. Esemplicando, la gestione di un documento informatico non può prescindere dalla disponibilità di un elaboratore e dei relativi programmi necessari sia per "formare" il documento che per "leggerlo" e verificarne autenticità, integrità e paternità.
- **Documento analogico:** in generale, è quello che per la sua formazione utilizza una grandezza fisica che assume valori continui come, ad esempio, le tracce continue su carta per il documento cartaceo o le immagini continue per il film. Il supporto fisico su cui si può formare il documento analogico non è necessariamente quello cartaceo, ma può essere film, lastra o pellicola radiologica, microfiche e microfilm, nastro audio e video. Il documento analogico può essere originale, a sua volta distinto in originale unico e non unico, o copia.
- **Supporto di memorizzazione:** il supporto può essere ottico o non ottico, in quanto il documento esiste a prescindere dal supporto su cui è memorizzato. La deliberazione CNIPA 11/2004 autorizza l'utilizzo di un qualsiasi tipo di supporto di memorizzazione che consenta la registrazione mediante tecnologia laser (dischi ottici WORM e CD-R, dischi magneto-ottici o DVD). È data, inoltre, la possibilità di utilizzare un qualsiasi altro supporto di memorizzazione, oltre a quelli a tecnologia laser, nel rispetto delle regole tecniche previste ed in mancanza di altri motivi ostativi.
Si è, infatti, raggiunta la consapevolezza del fatto che gli strumenti di firma digitale e di marca temporale garantiscono idoneamente l'integrità del documento nel processo di conservazione, indipendentemente dal supporto scelto. Gli stessi strumenti garantiscono anche la possibilità di trasmissione telematica dei documenti, senza che questo processo di trasmissione possa portare ad alterazioni di sorta.
- **Firma digitale:** è l'elemento principale che interviene nella gestione elettronica del documento informatico dalla formazione, alla trasmissione, fino alla conservazione, poiché conferisce piena validità legale al documento cui è apposta, assicurando autenticità, integrità, non ripudiabilità.
- **Attestazione temporale:** per stabilire il momento temporale in cui un documento informatico è stato formato è necessario attribuirgli una "validazione temporale", definita come il risultato di una procedura informatica in grado di offrire un riferimento temporale opponibile ai terzi. Lo strumento per ottenere



questo risultato è la marca temporale, una particolare firma elettronica che contiene l'ora e la data in cui è stata generata ed è opponibile ai terzi.

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

In linea generale non sono previste autorizzazioni preventive per l'adozione di criteri operativi per effettuare la conservazione sostitutiva. Per effettuare la riproduzione e la conservazione dei documenti su supporti digitali, tuttavia, è necessario rispettare le regole tecniche previste dalla normativa, previste nella deliberazione CNIPA n. 11 del 19 febbraio 2004, in vigore dal 9 marzo 2004 ed integrate, per quanto concerne i documenti rilevanti ai fini tributari, dal Decreto 23 gennaio 2004 del Ministero dell'Economia e delle Finanze.

3.5 La deliberazione CNIPA n. 11 del 19 febbraio 2004 e le Regole Tecniche del DPCM 03/12/2013

Le Regole Tecniche del DPCM 03/12/2013 dettano le regole vevoli, in generale, per le procedure per la riproduzione e conservazione dei documenti su supporto idoneo a garantire la conformità dei documenti agli originali.

Il Decreto, che sostituisce integralmente la precedente Deliberazione del 2004, aggiorna le regole tecniche per la riproduzione e conservazione dei documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali, come previsto all'articolo 6, commi 1 e 2, del TU delle disposizioni legislative e regolamentari in materia di documentazione amministrativa di cui al DPR 28 dicembre 2000, n. 445.

Il Decreto ridefinisce il quadro normativo di riferimento, mutato grazie al progresso tecnologico, adattandolo alle nuove situazioni.

Si precisa che i sistemi di conservazione già esistenti alla data di entrata in vigore del presente decreto sono adeguati entro e non oltre 36 mesi dall'entrata in vigore del decreto 03/12/13 secondo un piano dettagliato. Fino al completamento di tale processo per tali sistemi possono essere applicate le previgenti regole tecniche. Fino al completamento di tale processo restano validi i sistemi di conservazione realizzati ai sensi della deliberazione CNIPA n. 11/2004. Il Responsabile della conservazione valuta l'opportunità di riversare nel nuovo sistema di conservazione gli archivi precedentemente formati o di mantenerli invariati fino al termine di scadenza di conservazione dei documenti in essi contenuti, così come previsto dall'Art. 14 del DPCM 03/12/13.

3.6 Il Responsabile della Conservazione

Come già per la deliberazione AIPA n. 42/2001, la deliberazione CNIPA n. 11/2004 (art. 5) e 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 sostitutiva, 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 dei obiettivi principali del Responsabile della Conservazione sostituiva è di definire ed impostare il processo per il trattamento della documentazione soggetta a conservazione sostituiva.

Più in particolare (art. 7 del DPCM 03/12/2013):



- a) 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;
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c) genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- g) 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;
- h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;
- j) 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;
- k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l) 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;
- m) predisporre 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.

[...]

Art. 5

Ai sensi dell'art. 44 del Codice, la conservazione può essere svolta:

[...]

- b) affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

Al Responsabile della Conservazione sono attribuiti compiti cruciali in ragione del controllo e della supervisione che egli attua sull'intero procedimento di conservazione sostitutiva.

Gli adempimenti comprendono non solo attività di pianificazione, ma anche attività di tipo operativo/esecutivo, che può essere necessario svolgere in sedi diverse e magari distanti tra di loro. L'utilizzo degli strumenti telematici, infatti, consente di memorizzare documenti e scritture contabili con estrema facilità e a costi minori in sedi accentrate specializzate.

Le Regole Tecniche all'art. 5 consentono di delegare in tutto o in parte le attività previste ad altri soggetti interni alla struttura e/o di affidarle a soggetti terzi (pubblici o privati) i quali sono tenuti ad osservare le disposizioni contenute nella deliberazione stessa.



3.7 La normativa in pratica

Tipologia	Emissione	Conservabile in modalità sostitutiva
Documento cartaceo "non unico"	Cartacea	Sì
Documento cartaceo "unico"	Cartacea	Sì, con l'intervento del Pubblico Ufficiale
Documento elettronico semplice	Nessuna condizione (la sua validità è sottoposta alla valutazione del giudice)	Sì
Documento elettronico con valenza di "forma scritta"	Documento "statico" Firma elettronica qualificata o firma digitale	Sì



4 Il sistema di creazione e gestione dei documenti

Si rimanda al Manuale di Gestione del Comune di Monselice per la descrizione funzionale ed operativa del sistema di gestione del protocollo informatico, dei flussi documentali e degli archivi adottato dal Comune di Monselice con particolare riferimento alle modalità di utilizzo dello stesso.

4.1 Strumenti utilizzati

La redazione di contratti e degli atti amministrativi da conservare attraverso il sistema di conservazione sostitutiva avviene utilizzando i software di videoscrittura Microsoft Word e Open Document. I documenti vengono convertiti in file formato pdf attraverso l'applicativo PdfCreator ovvero analoghi software di conversione.

Servizi di certificazione

Il Segretario Comunale, i dirigenti nonché i soggetti individuati nel Manuale di gestione del protocollo informatico sono dotati di firma digitale attraverso smartcards o business keys.

4.2 Controlli

Ai sensi di legge, il Comune di Monselice assicura che i documenti inviati in conservazione sono statici non modificabili, ovvero redatti in modo tale per cui il contenuto non possa essere alterabile durante le fasi di conservazione ed accesso ed è immutabile nel tempo.

4.3 Indicizzazione dei documenti

Il Comune di Monselice provvede all'indicizzazione dei documenti utilizzando le funzioni messe a disposizione dal sistema di creazione e gestione dei documenti.

4.4 Gestione delle anomalie

Il sistema di conservazione LegalDoc è configurato per accettare solo documenti in formati prestabiliti e dimensioni non superiori ai 50 MB. 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 al Comune di Monselice.

4.5 Formato dei documenti elettronici

Le nuove 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 (GU Serie Generale n. 59 del 12-3-2014 - Suppl. Ordinario n. 20) elencano in modo specifico i formati documentali da adottare per la conservazione a lungo termine dei documenti, ovvero le modalità di organizzazione delle informazioni in un codice binario nel loro allegato. Pertanto il Comune ha deciso l'invio in conservazione soltanto di PDF eventualmente firmati digitalmente e marcati temporalmente.



5 Il sistema di conservazione documentale

5.1 Descrizione generale del servizio

LegalDoc è un servizio di conservazione dei documenti erogato in modalità ASP e sviluppato sulle esigenze di imprese, professionisti, associazioni, Pubblica Amministrazione centrale e locale, che permette di mantenere e garantire nel tempo l'integrità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

LegalDoc consente le funzionalità di:

- conservazione del documento: il documento, ricevuto negli Internet Data Center di InfoCert in formato digitale statico non modificabile, ovvero redatto in modo tale per cui il contenuto non possa essere alterabile durante le fasi di conservazione ed accesso, viene conservato a norma di legge per tutta la durata prevista dal contratto;
- rettifica di un documento conservato: un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica non comporta la cancellazione del documento originario dall'archivio a norma ma è una modifica logica, nel pieno rispetto del principio di tracciabilità del documento;
- cancellazione di un documento conservato: un documento inviato in conservazione può essere cancellato, allegando eventualmente la motivazione della cancellazione. Il sistema terrà comunque traccia del documento all'interno dell'archivio a norma, nel rispetto del principio di tracciabilità del documento;
- visualizzazione di un documento conservato (esibizione a norma): il documento richiesto viene richiamato via web direttamente dal servizio di conservazione sostitutiva LegalDoc ed esibito con garanzia della sua opponibilità a terzi.

LegalDoc integra il sistema di gestione documentale in uso dal Comune di Monselice e ne estende i servizi con funzionalità di stoccaggio digitale; il servizio consente di organizzare liberamente le fasi di creazione, utilizzo e archiviazione dei documenti, intervenendo solamente nella fase di conservazione e solamente per i documenti che l'ente sceglie di conservare.

5.2 Definizione di documento

In LegalDoc il documento è un insieme di uno o più file digitali, anche di diverse tipologie. Ad ogni documento è associato un file di controllo e un file delle direttive di conservazione, nonché un identificativo univoco generato da LegalDoc ("Token LegalDoc"). Il documento rappresenta l'unità minima di elaborazione nel senso che viene memorizzato ed esibito come un tutt'uno; non è possibile estrarre da LegalDoc parti di un documento.

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

- è costituito da uno o più file;
- è memorizzato sui supporti previsti dalla procedura di conservazione;
- è identificato in maniera univoca attraverso il token LegalDoc;
- appartiene a un lotto di documenti, a sua volta identificato univocamente nel sistema di conservazione;
- è conservato insieme al file delle direttive di conservazione, al file di ricevuta e al file di controllo del documento.

I documenti inviati nei formati standard, dettagliati nella documentazione contrattuale a disposizione del Cliente, sono visualizzabili mediante i relativi software definiti e messi a disposizione da InfoCert. Al momento dell'attivazione del servizio, il Cliente verifica che i documenti inviati siano nel formato standard leggibile con il software definito da InfoCert.



5.3 Configurazione dei sistemi

Modalità di erogazione

Il servizio di conservazione sostitutiva LegalDoc è implementato da una 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).

LegalDoc è reso in modalità ASP (Application Service Providing) e consente al Cliente di accedere ai servizi di conservazione sostitutiva dei documenti informatici su un elaboratore elettronico, gestito da InfoCert e fisicamente posto nei locali di quest'ultima, in conformità a quanto descritto nel documento [1] *Condizioni Generali di Contratto* e nella relativa documentazione tecnica da questo referenziata.

Il servizio è accessibile dalla apposita URL di rete; il Cliente richiama i servizi di LegalDoc secondo le modalità indicate da InfoCert nella documentazione contrattuale.

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

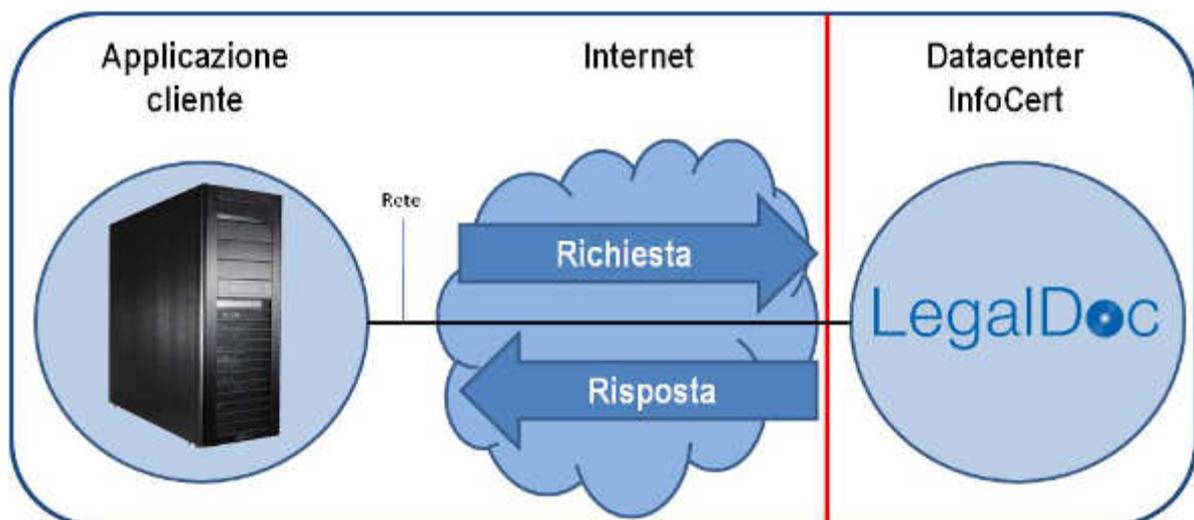


Figura 1 - Dialogo tra il sistema di gestione del Cliente e il sistema di conservazione documentale LegalDoc

5.4 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 della Conservazione InfoCert appone la propria firma digitale sul file di chiusura lotto mediante un sistema di firma automatica erogato dalla CA InfoCert, che si avvale di un dispositivo crittografico ad altre prestazioni HSM.

Supporti di conservazione

Ai fini della conservazione i documenti vengono raggruppati in lotti e ciascun lotto è corredato da un file indice (file di chiusura lotto) che contiene gli hash dei documenti appartenenti al lotto.

L'apposizione della firma digitale del RdC e della marca temporale sul file di chiusura lotto attestano la conservazione la conservazione del lotto.

I lotti prodotti vengono archiviati mediante procedure e sistemi che consentono la memorizzazione permanente in più copie e l'immodificabilità di quanto memorizzato.

Inoltre, possono essere prodotte ulteriori copie di back-up su supporti ottici rimovibili, stoccati da InfoCert o inviati al Cliente su espressa richiesta.

Posta Elettronica Certificata

Il servizio LegalDoc si avvale del servizio PEC di InfoCert: in sede di attivazione del servizio, è stata definita per il Cliente 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.

5.5 Controlli

I processi del servizio di conservazione sostituiva 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 RdC 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 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 della Conservazione mantiene il verbale degli incidenti e delle contromisure attuate, che divengono oggetto di opportuni incontri di miglioramento.



6 Le tipologie documentali

I Contratti e gli Atti Amministrativi vengono creati mediante sistemi di videoscrittura in uso presso l'Ente in maniera statica e non modificabile; vengono poi firmati digitalmente da controparti e responsabili.

I documenti vengono poi inviati al sistema di conservazione sostitutiva a seguito del caricamento manuale tramite una postazione pc, inserito nella rete internet del Comune di Monselice.

6.1 Contratti

Tipologia di documento	Contratti
Natura del documento	Documento elettronico
Conservabile in modalità elettronica	Si
Data di decorrenza del processo di conservazione elettronica	01/10/2014

I Contratti vengono creati mediante sistemi di videoscrittura in uso presso l'Ente in maniera statica e non modificabile in formato pdf, vengono poi firmati digitalmente dalle parti contrattuali e, se assumono la forma di atto pubblico, vengono firmati digitalmente dall'ufficiale rogante (Segretario Generale o Vicesegretario generale).

6.2 Atti Amministrativi

Tipologia di documento	Atti Amministrativi
Natura del documento	Documento elettronico
Conservabile in modalità elettronica	Si
Data di decorrenza del processo di conservazione elettronica	15/09/2014

Gli atti amministrativi (che comprendo altresì le Deliberazioni di Consiglio Comunale, le Deliberazioni di Giunta Comunale e le Determinazioni dirigenziali) vengono creati mediante sistemi di videoscrittura utilizzati dal software prodotto da Halley Informatica S.r.l. attraverso l'applicativo che gestisce gli atti amministrativi dell'Ente. Gli atti amministrativi vengono sottoscritti digitalmente dai responsabili attraverso l'applicativo che genera il documento digitale.

I documenti vengono poi inviati al sistema di conservazione sostitutiva a seguito del caricamento manuale tramite una postazione pc, inserito nella rete internet del Comune di Monselice. In alternativa, potranno essere utilizzati applicativi che permettono l'invio automatico degli atti amministrativi al sistema di conservazione sostitutiva previa individuazione delle modalità applicative informatiche necessarie per fare interagire i sistemi informatici.



6.3 Allegati

Tipologia di documento	Allegati a contratti e atti amministrativi
Natura del documento	Documento elettronico
Conservabile in modalità elettronica	Si
Data di decorrenza del processo di conservazione elettronica	15/09/2014

6.3.1 Fasi del processo

Fase / Attività	Soggetti incaricati	Afferenza / Applicativi	Descrizione
Redazione	Utenti Ente	Sistemi di videoscrittura	Viene redatto il testo dell'atto, in formato elettronico e convertito in formato immutabile
Approvazione	Organo competente	Firma digitale	Sull'atto viene apposta la firma digitale sul documento da parte dei soggetti competenti.
Repertoriatura	Ente	Gestore documentale	Si provvede alla registrazione dell'atto utilizzando le funzionalità del sistema
Invio dei documenti	Ente	Manualmente con LegalDoc Folders	I documenti vengono inviati al sistema di conservazione sostitutiva a seguito del caricamento manuale tramite una postazione pc, inserito nella rete intranet del Comune di Monselice.
Invio in conservazione	Ente	LegalDoc Folders	Il sistema invia il documento in conservazione, richiedendo che il processo si concluda a riempimento dei lotti. È possibile richiedere la chiusura forzata del lotto



<i>Completamento del processo di conservazione</i>	InfoCert	LegalDoc	Il sistema di conservazione LegalDoc eroga il processo di conservazione dei documenti secondo quanto dettagliato al capitolo 7. LegalDoc restituisce al sistema di protocollo il Token univoco del documento.
<i>Custodia dei supporti</i>	InfoCert	LegalDoc	La custodia dei supporti è demandata ad InfoCert come da accordi contrattuali.



7 Il processo di conservazione

Il processo di conservazione attuato da InfoCert prevede l'utilizzo di diversi strumenti e l'intervento di soggetti che concorrono a rendere l'erogazione del servizio affidabile e rispondente ai requisiti richiesti dalla legge.

Ai fini del trattamento dei documenti destinati alla conservazione, il servizio si divide in due categorie di processi:

- processi di front-end;
- processi di back-end.

7.1 Processi di front-end

I processi di front-end sono erogati in modalità batch dal sistema LegalDoc Folders, e sono finalizzati a mettere in comunicazione i sistemi gestionali del Cliente con i servizi di LegalDoc e sono richiamati in modalità on-line.

Per ciascuno dei servizi indicati di seguito si eseguono opportuni controlli di autenticazione del soggetto chiamante e di correttezza e accettabilità delle richieste:

- invio di un documento informatico o di un documento analogico opportunamente digitalizzato in conservazione sostitutiva;
- rettifica o cancellazione per via telematica di un documento già conservato in modalità sostitutiva;
- esibizione di un documento direttamente dal sistema LegalDoc;
- elaborazione ed invio della richiesta di chiusura forzata del lotto;
- ottenimento per via telematica delle informazioni sullo stato di un documento o di un lotto.

7.2 Processi di back-end

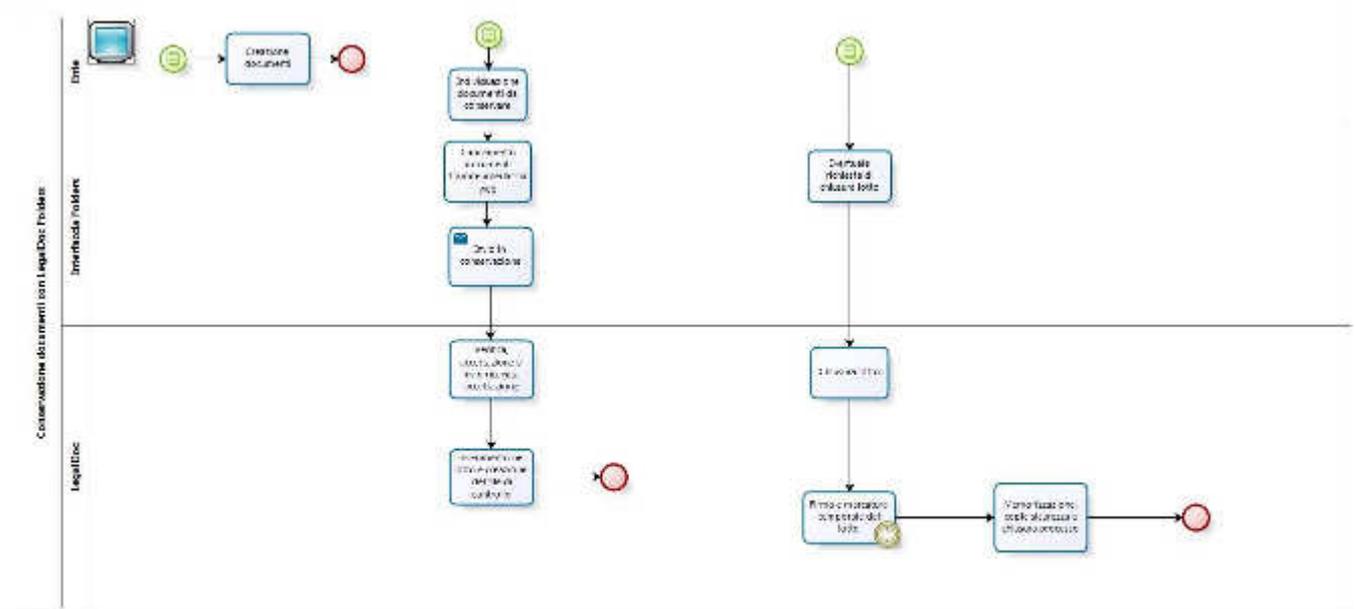
I processi di back-end sono eseguiti dal sistema LegalDoc in modalità differita e sono i processi che, a partire dai documenti caricati sul sistema LegalDoc Folders dal Comune di Monselice, implementano la conservazione sostitutiva in conformità alle regole tecniche.

Il processo di conservazione si suddivide in due macro fasi:

- **elaborazione del singolo documento:** in questa fase viene analizzato il singolo documento, che viene assegnato a un lotto di documenti. Il documento viene corredato da un file di controllo, firmato digitalmente dal Responsabile della Conservazione, contenente informazioni sensibili ai fini della conservazione (indice del documento, impronte dei file che lo costituiscono, classificazione anagrafica dei firmatari, lotto di appartenenza);
- **elaborazione e chiusura del lotto:** quando si raggiungono le condizioni per la chiusura del lotto, questo viene corredato da un file di chiusura lotto contenente informazioni sensibili ai fini della conservazione (identificativo univoco del lotto – tokenlotto –, criteri di omogeneità, hash del file di controllo). Al file di chiusura lotto viene apposta la firma digitale del Responsabile della Conservazione e la marca temporale; infine, l'insieme di documenti appartenenti al lotto, corredati dai rispettivi file di controllo e dal file di chiusura lotto, viene memorizzato nei supporti di conservazione e nelle copie di sicurezza.



7.3 Fasi del processo di conservazione: schema generale



7.4 Responsabilità del processo di conservazione

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



<i>Attività</i> ↗	<i>Responsabilità</i> ↗	<i>Comune di Monselice</i>	<i>LegalDoc Folders</i>	<i>LegalDoc</i>	<i>Responsabile della Conservazione</i>
1. Formazione del documento		R - E			
2. Indicizzazione e archiviazione		R - E			
3. Acquisizione documento e creazione del file con le direttive di conservazione		V	R - E		
4. Invio al sistema di conservazione		R - E	R - E		
5. Verifica e accettazione del documento e invio della ricevuta di accettazione dei documenti				E - V	
6. Inserimento nel lotto e creazione del file di controllo				E	R - V* - A
7. Chiusura del lotto e attestazione di corretto procedimento				E	R - V* - A
8. 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 della Conservazione sono garantite anche dal servizio di auditing InfoCert.

7.5 Fasi del processo di conservazione: dettaglio

Formazione del documento

<i>INPUT</i>	<i>Documento da generare</i>	
Comune di Monselice	1.1	Il Comune di Monselice genera i documenti secondo le procedure descritte nel capitolo 4
<i>OUTPUT</i>	<i>Documento generato</i>	

Indicizzazione e archiviazione

<i>INPUT</i>	<i>Documento da archiviare</i>	
Comune di Monselice	1.1	I documenti vengono inviati al sistema di conservazione sostitutiva a seguito del caricamento manuale tramite una postazione pc, inserito nella rete internet del Comune di Monselice.
<i>OUTPUT</i>	<i>Documento indicizzato e archiviato</i>	



Acquisizione documento e creazione del file delle direttive

INPUT	<i>File delle direttive da predisporre</i>	
LegalDoc Folders	2.1	Il sistema LegalDoc Folders acquisisce i documenti informatici caricati manualmente dal Comune di Monselice e li prepara all'invio conservazione
LegalDoc	2.2	Il sistema LegalDoc esegue le seguenti operazioni: <ul style="list-style-type: none"> • Predisposizione del file con le direttive di conservazione; • Calcolo delle impronte dei file costituenti il documento; • Inserimento delle impronte nel file delle direttive; • Apposizione della firma elettronica sul file delle direttive; • Costruzione del messaggio contenente i file che costituiscono il documento
OUTPUT	<i>File delle direttive predisposto</i>	

Invio al sistema di conservazione

INPUT	<i>Documento da inviare a LegalDoc</i>	
LegalDoc Folders	3.1	Invoca i servizi di LegalDoc e invia il documento, il file degli indici di ricerca e la relativa richiesta di conservazione.
OUTPUT	<i>Documento inviato a LegalDoc</i>	

Verifica, accettazione e invio della ricevuta di accettazione del documento

INPUT	<i>Documento da verificare</i>	
LegalDoc	4.2	Acquisizione del documento.
	4.3	Sbustamento del messaggio e verifica della firma elettronica apposta sul file delle direttive di conservazione
	4.4	Presenza in carico dei file costituenti il documento.
	4.5	Esecuzione di una serie di verifiche sulla completezza e sulla correttezza delle informazioni contenute nel file delle direttive di conservazione.
	4.6	Generazione dell'impronta di ogni file del documento.
	4.7	Confronto dell'impronta generata con la corrispondente inviata dal Cliente per garantire l'integrità del documento ricevuto.
	4.8	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.
	4.9	Generazione del file di ricevuta a partire dal file delle direttive.
	4.10	Generazione di un identificativo univoco per il documento (token LegalDoc) e firma elettronica sul file di ricevuta.
	4.11	Invio a LegalDoc Folders del file di ricevuta di presa in carico della richiesta di conservazione.



LegalDoc Folders	4.12	Riceve il file di ricevuta di presa in carico della richiesta di conservazione, ne estrae il token LegalDoc e lo memorizza presso i propri archivi, in associazione con gli indici di ricerca.
OUTPUT	<i>Documento verificato</i>	

Inserimento nel lotto e creazione del file di controllo

INPUT	<i>Documento da conservare</i>	
LegalDoc	5.1	Verifica per ogni documento se esiste già un lotto di documenti aperto che possiede le caratteristiche specificate dal file delle direttive in cui inserire il documento; in caso contrario si predispongono un nuovo lotto.
	5.2	Predisposizione del file di controllo del documento contenente l'indice del documento, le impronte dei file che lo costituiscono, la classificazione anagrafica del documento, il lotto di appartenenza, gli estremi di identificazione del Responsabile della Conservazione.
	5.3	Apposizione della firma elettronica del Responsabile della Conservazione sul file di controllo.
	5.4	Inserimento del file di controllo e del relativo documento nel lotto di conservazione.
OUTPUT	<i>Documento inserito in un lotto di conservazione</i>	

Chiusura del lotto e attestazione di corretto procedimento

INPUT	<i>Lotto da chiudere</i>	
LegalDoc	7.1	Chiusura del lotto dopo il raggiungimento delle condizioni di chiusura lotto: <ul style="list-style-type: none">• raggiungimento della data massima di chiusura del lotto.• In base a criteri temporali definiti insieme al Comune di Monselice. Il lotto viene chiuso al verificarsi del primo dei precedenti eventi o in seguito alla ricezione della richiesta di chiusura forzata del lotto inviata dal Cliente.
	7.2	Generazione del file di chiusura lotto e inserimento degli hash dei file di controllo del documento.
Responsabile della Conservazione	7.3	Apposizione della firma digitale, necessaria ad attestare il corretto svolgimento del procedimento sul file di chiusura lotto.
	7.4	Apposizione della marca temporale sul file di chiusura lotto.
OUTPUT	<i>Lotto chiuso</i>	

Memorizzazione, creazione copia di sicurezza e chiusura della conservazione

INPUT	<i>Documenti da memorizzare</i>	
LegalDoc	8.1	Memorizzazione del lotto su supporto magnetico.
	8.2	Creazione della copia di sicurezza.



	8.3	Termine della procedura di conservazione.
<i>OUTPUT</i>		<i>Documenti conservati</i>



8 Procedure di ricerca ed esibizione

Le procedure di esibizione del documento integrate in LegalDoc permettono, a partire dalla funzione di ricerca in LegalDoc Folders, di estrarre dal sistema un documento di cui sia completata la procedura di conservazione, utilizzando il token LegalDoc.

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 stazione di lavoro (computer), purché collegata in rete e con disponibilità di un browser web.

L'interfaccia è organizzata a schede, ognuna delle quali tratta un aspetto relativo alla conservazione del documento.

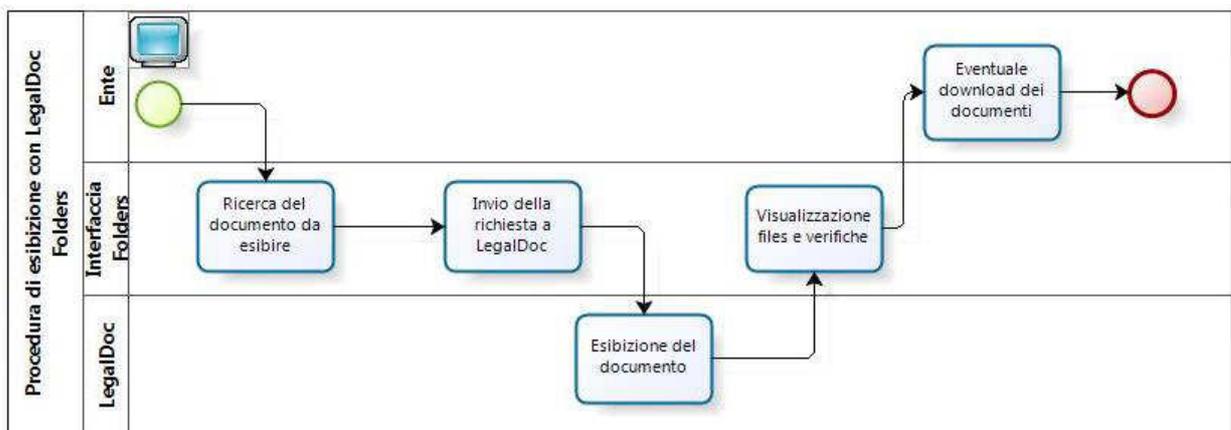
Visualizzando il contenuto di ciascuna scheda diventa possibile:

- 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 del secondo comma dell'articolo 6 della deliberazione CNIPA 11/04.

Di seguito si descrivono le fasi della procedura di ricerca ed esibizione.

8.1 Procedura di esibizione: schema generale





8.2 Procedura di esibizione: dettaglio

Ricerca del documento da esibire

INPUT	<i>Lista di documenti</i>	
Comune di Monselice	1.1	Attraverso LegalDoc Folders utilizzando gli indici archiviati nel proprio gestore documentale, ricerca il documento da esibire
OUTPUT	<i>Token relativo al documento da esibire</i>	

Invio della richiesta a LegalDoc

INPUT	<i>Richiesta di esibizione da preparare</i>	
LegalDoc Folders	2.1	LegalDoc Folders 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.
OUTPUT	<i>Richiesta di esibizione presa in carico da LegalDoc</i>	

Ricerca del documento nel sistema ed esibizione

INPUT	<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 Cliente e quelli dei documenti conservati.
	3.3	Predisposizione delle copie di: <ul style="list-style-type: none">• file costituenti il documento conservato• file di ricevuta• file di controllo del documento.
	3.4	Passaggio del pacchetto di file all'Esibitore
OUTPUT	<i>Documento passato all'Esibitore</i>	

Verifica del documento

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

Verifica del documento

INPUT	<i>Documento esibito</i>	
--------------	--------------------------	--



Esibitore	5.1	Download del documento e memorizzazione dello stesso in locale
OUTPUT		<i>Documento salvato</i>

8.3 Requisiti software

Per la visualizzazione e la stampa del documento ottenuto con la procedura di esibizione da LegalDoc, il Comune di Monselice utilizza, per ognuno dei file costituenti il documento, il relativo viewer definito da InfoCert per i formati standard o depositato presso il sistema di conservazione per le altre tipologie di file.



9 Modifica dei documenti posti in conservazione

In caso di modifica dei documenti già posti in conservazione, il Comune di Monselice provvede ad emanare ex novo un documento di rettifica che verrà a sua volta conservato a norma; la riconducibilità del documento modificante a quello modificato è resa possibile grazie agli indici predisposti dal Comune di Monselice in fase di caricamento, che ne assicura la sistematicità e la coerenza.

9.1 La cancellazione di un documento

LegalDoc è configurato in modo da non consentire la cancellazione fisica di quanto conservato: il servizio di cancellazione consiste nella cancellazione logica del documento dal database.

La cancellazione può essere richiesta solo dal sistema di interfaccia a LegalDoc che ha fatto la richiesta di invio in conservazione del documento da cancellare.



10 Misure di sicurezza

10.1 Comune di Monselice

Per le misure di sicurezza nel trattamento dei documenti del Comune di Monselice si rimanda alla procedure vigenti da esso predisposto.

10.2 InfoCert

Il sistema LegalDoc è pienamente conforme ai requisiti di sicurezza prescritti dalle norme. Nel seguito sono descritte le modalità generali tecniche e le infrastrutture che InfoCert utilizza all'interno del proprio data center di Padova, in quanto fornitore del servizio di conservazione.

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 del locale 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.



11 Note conclusive

11.1 Procedure di riversamento

Riversamento diretto

Il primo comma, lettera n), dell'articolo 1 della deliberazione CNIPA n. 11/2004 definisce il riversamento diretto come il "processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica".

Le norme non pongono particolari obblighi nello svolgimento del processo, che è parte integrante del servizio.

Riversamento sostitutivo

Qualora fosse necessario, o in presenza di una espressa richiesta del Comune di Monselice, il Responsabile della Conservazione InfoCert provvede al riversamento sostitutivo del contenuto dei supporti, inteso come il "processo che trasferisce uno o più documenti informatici conservati da un supporto ottico ad un altro, modificando la loro rappresentazione informatica" (deliberazione CNIPA 11/2004, articolo 1 comma 1 lettera o.).

Alla data di redazione del presente documento non sono riscontrabili motivazioni tecnologiche, legali o di altra natura che impongano o possano richiedere nei prossimi anni l'effettuazione del riversamento sostitutivo e la conseguente conversione dei documenti conservati in altri con differente rappresentazione informatica.

I controlli periodici messi in atto dal Responsabile della Conservazione InfoCert permettono di monitorare costantemente l'evoluzione dei diversi scenari di riferimento (tecnologico, normativo...) al fine di rispondere all'esigenza di riversamento sostitutivo dei documenti conservati non appena questa dovesse manifestarsi.

Il riversamento sostitutivo verrà effettuato secondo procedure che saranno definite e documentate al bisogno, in relazione al futuro scenario normativo e tecnologico di riferimento.

11.2 Protezione dei dati personali

Nelle fasi di creazione, digitalizzazione, trattamento e invio in conservazione della documentazione cartacea e elettronica, il Comune di Monselice 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 Codice, il Comune di Monselice ha nominato InfoCert SpA Responsabile dei trattamenti dei dati necessari all'esecuzione del servizio (allegato [2]).

In particolare, anche in considerazione del ruolo di Responsabile della Conservazione ricoperto, i compiti affidati ad InfoCert SpA 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 in allegato al materiale contrattuale da questi sottoscritto, ove viene altresì allo stesso consentito di esprimere il consenso per gli ulteriori trattamenti indicati.



12 Allegati

12.1 Documentazione contrattuale di riferimento

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.

- [1] Richiesta di attivazione con Condizioni Generali di Contratto – Regola il rapporto tra InfoCert e Comune di Monselice;
- [2] Affidamento del procedimento di conservazione sostitutiva – formalizza l'affidamento ad InfoCert del processo di conservazione, delineandone l'ambito di applicazione;
- [3] Allegato Tecnico al contratto – descrive le modalità di fornitura del servizio e l'infrastruttura utilizzata per la sua erogazione.
- [4] Manuale di gestione