

N. 1239

del Reg. Deliberazioni

del 13/09/2023

**DELIBERAZIONE
DEL DIRETTORE GENERALE**

**- Dott.ssa Patrizia Simionato -
nominato con Decreto del Presidente della Giunta Regionale del Veneto
n. 24 del 26.02.2021**

**OGGETTO: Approvazione del "Manuale dei processi documentali per la
Conservazione"**

Struttura UOC Servizi Tecnici e Patrimoniali

Si attesta l'avvenuta regolare istruttoria
del presente provvedimento proposto
per l'adozione in ordine alla legittimità
con ogni altra disposizione regolante la materia.

Il Direttore f.f. della Unità Operativa Complessa
Ing. Renzo Mantovani

Il Direttore f.f. della UOC Servizi Tecnici e Patrimoniali, riferisce quanto segue:

Il 3 dicembre 2013 è stato predisposto il Decreto del Presidente del Consiglio dei Ministri denominato “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-bis e 71, comma 1, del Codice dell’amministrazione digitale di cui al decreto legislativo n. 82 del 2005”, poi pubblicato in GU Serie Generale n. 59 del 12/03/2014 – Suppl. Ordinario n. 20 del Decreto del Ministero dell’Economia e delle Finanze 17 giugno 2014.

Tale DPCM, all’art. 8 prevede la predisposizione da parte degli enti pubblici del “Manuale di Conservazione”, il quale “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.

Tutto ciò premesso e considerato, il Direttore f.f. della UOC Servizi Tecnici e Patrimoniali, sentito il Responsabile Unico del Procedimento, attestata l’avvenuta regolare istruttoria della pratica, anche in ordine alla compatibilità con la vigente legislazione statale e regionale, propone di approvare per quanto espresso in premessa il documento allegato al presente provvedimento: "Manuale dei processi documentali per la Conservazione",

IL DIRETTORE GENERALE

In relazione a quanto sopra riferito e preso atto che il Direttore della UOC proponente, competente dell’istruzione dell’argomento in questione, ha attestato l’avvenuta regolare istruttoria della pratica, anche in ordine alla compatibilità con la vigente legislazione regionale e statale;

acquisito il parere favorevole del Direttore Amministrativo, Sanitario ai sensi dell’art. 3 del D.

Lgs.n. 502/92 e successive modificazioni ed integrazioni e del Direttore dei Servizi Socio-Sanitari, ai sensi dell’art. 16 della L.R. 56/94 e s.m.i.;

Vista la L. n. 241/1990 e, s.m.i.

Visto il CCNL Dirigenza

DELIBERA

di approvare per quanto espresso in premessa il documento allegato al presente provvedimento: "Manuale dei processi documentali per la Conservazione".

Responsabile del Procedimento ed estensore del provvedimento: Dott. Dario Sicchiero

* * * * *

Pareri favorevoli in quanto di competenza:

IL DIRETTORE AMMINISTRATIVO

Dott. Leopoldo Ciato

IL DIRETTORE SANITARIO

Dott. Alberto Rigo

Per IL DIRETTORE DEI SERVIZI SOCIO-SANITARI

Dott.ssa Domenica Lucianò

II DIRETTORE GENERALE

Dott.ssa Patrizia Simionato

Il presente atto, eseguibile dalla data di adozione:

- è soggetto a controllo ;
- non è soggetto a controllo

Rovigo, 18/09/2023

Il Direttore UOC Affari Generali

Dr.ssa Patrizia Davì

Attestazione di pubblicazione

Copia del presente atto è pubblicata all'Albo on line dell'Azienda per 15 giorni consecutivi da oggi.

Rovigo, 18/09/2023

Il Direttore UOC Affari Generali

Dr.ssa Patrizia Davì

Copia del presente atto viene inviata in data odierna al Collegio Sindacale (ex art. 10, comma 5, L.R. 56 del 14.9.94)

Rovigo, 18/09/2023

Il Direttore UOC Affari Generali

Dr.ssa Patrizia Davì

Copia conforme all'originale, per uso amministrativo

Rovigo,

Il Direttore UOC Affari Generali

Dr.ssa Patrizia Davì

Da distribuire a:					
DIRETTORE GENERALE	-	UOC GESTIONE RISORSE UMANE	-	UFFICIO PROTEZIONE DATI	-
DIRETTORE AMMINISTRATIVO	-	UOC DIREZIONE AMM.VA TERRITORIALE	-	UFF. TRASPARENZA E ANTICORRUZIONE	-
DIRETTORE SANITARIO	-	UOC DIREZIONE AMM.VA OSPEDALIERA	-	UFF. RELAZIONI CON IL PUBBL.E COMUNICAZIONE	-
DIRETTORE SERVIZI SOCIO-SANITARI	-	UOC CONTROLLO DI GESTIONE	-	_____	-
COLLEGIO DI DIREZIONE	-	UOC DIREZ. PROFESSIONI SANITARIE	-	_____	-
DIREZIONE FUNZIONE OSPEDALIERA	-	UOC ASS. FARMACEUTICA TERRITORIALE	-	_____	-
DIREZIONE FUNZIONE TERRITORIALE	-	UOC FARMACIA OSPEDALIERA	-	_____	-
DIPARTIMENTO SALUTE MENTALE	-	UOC DISABILITA' NON AUTOSUFFICIENZA	-	_____	-
DIPARTIMENTO DI PREVENZIONE	-	UOC INFANZIA, ADOL.E FAM.DISTRETTO 1	-	_____	-
UOC DISTRETTO 1 ROVIGO	-	UOC INFANZIA, ADOL.E FAM.DISTRETTO 2	-	_____	-
UOC DISTRETTO 2 ADRIA	-	UNITA' OPERATIVA PER IL SOCIALE	-	_____	-
UOC DIREZIONE MEDICA OSP. RO-TRE	-	UOC PSICHIATRIA	-	_____	-
UOC DIREZIONE MEDICA OSP. ADRIA	-	UOC SERD	-	_____	-
POLO FORMATIVO	-	UOS QUALITA' E RISCHIO CLINICO	-	_____	-
UOC AFFARI GENERALI	-	UOS ASSISTENZA SPECIALISTICA AMB.	-	_____	-
UOC CONTABILITA' E BILANCIO	-	UOS MEDICO COMPETENTE	-	_____	-
UOC PROV. ECONOM. LOGISTICA	-	UOS INTERNAL AUDITING E CERT.BIL.	-	_____	-
UOC SERVIZI TECNICI PATRIMONIALI	-				

Manuale dei processi
documentali per la
Conservazione

ULSS POLESANA

INDICE

1.	Introduzione al documento.....	3
1.1.	Gestione versioni documento.....	3
1.2.	Scopo e campo di applicazione del documento.....	4
1.3.	Principi di redazione.....	4
1.4.	Termini e definizioni.....	5
1.5.	Acronimi.....	10
2.	Il quadro normativo.....	11
2.1.	Principali riferimenti normativi.....	11
2.2.	La normativa in ambito clinico-sanitario.....	12
2.3.	La normativa sulla fatturazione elettronica.....	13
	Nomine e individuazione dei compiti.....	15
2.4.	Soggetto Produttore: ULSS.....	16
2.5.	Responsabile della conservazione interno.....	16
2.6.	Responsabile del servizio della Conservazione.....	17
2.7.	InfoCert SPA – Conservatore.....	18
3.	Il sistema di creazione e gestione dei documenti.....	19
3.1.	Strumenti utilizzati.....	19
3.2.	Servizi di certificazione.....	19
3.3.	Controlli.....	19
3.4.	Indicizzazione dei documenti.....	20
3.5.	Formato dei documenti.....	20
4.	Il sistema di conservazione documentale.....	20
4.1.	Oggetti sottoposti alla conservazione.....	20
4.2.	Descrizione generale del servizio.....	21
4.3.	Definizione di documento.....	22
4.4.	Configurazione dei sistemi.....	23
4.5.	Componenti.....	23
4.5.1.	Componente locale L-Care.....	23
4.5.2.	Ambienti di conservazione.....	24
4.5.3.	Marca temporale sui pacchetti di archiviazione.....	24
4.5.4.	Firma digitale sui pacchetti di archiviazione con dispositivo HSM.....	24
4.5.5.	Supporti di conservazione.....	24
5.	Gestione degli Errori.....	26
5.1.	Controlli.....	26
5.1.1.	Controlli di processo.....	26
5.1.2.	Controlli periodici.....	26
5.1.3.	Ispezione del sistema da parte delle autorità competenti.....	27
5.1.4.	Incident management.....	27

6.	Le tipologie documentali.....	27
7.	Il processo di conservazione.....	30
7.1.	Tabella di Responsabilità.....	30
7.2.	Fasi del processo di conservazione della documentazione amministrativa e sanitaria.....	31
7.3.	Fasi del processo di conservazione delle Fatture PA.....	33
7.3.1.	Ciclo attivo	34
7.3.2.	Ciclo passivo	34
8.	Procedure di ricerca ed esibizione.....	35
8.1.	Broker Console LegalCare.....	35
8.2.	Procedura di esibizione: dettaglio.....	36
8.3.	Approfondimento della precedente versione di LegalDoc.....	37
8.4.	Requisiti software.....	38
9.	Modifica e scarto dei documenti conservati.....	39
10.	Misure di sicurezza	39
10.1.	InfoCert.....	39
10.1.1.	Sicurezza fisica	39
10.1.2.	Gruppi di continuità.....	40
10.1.3.	Connessione a Internet.....	40
10.1.4.	Sicurezza delle reti: protezione da intrusioni.....	40

1. Introduzione al documento

1.1. Gestione versioni documento

Versione/Release n°:	1	Data Versione/Release:	2015
Descrizione modifiche:	nessuna		
Versione/Release n°:	2	Data Versione/Release:	luglio 2016
Descrizione modifiche:	<ul style="list-style-type: none"> - Aggiornamento riferimenti normativi - Aggiunta tipologia documentale “Fattura elettronica PA attiva e passiva”, “Registro giornaliero di protocollo”, “Documento protocollato”. - Aggiornamento formati 		
Versione/Release n°:	3	Data Versione/Release:	Luglio 2023
Descrizione modifiche:	<ul style="list-style-type: none"> - Aggiornamento riferimenti normativi - Aggiornamento formati - Attivazione nuova versione LegalDoc - Fusione delle Ex Aziende Ulss 18 di Rovigo e Ulss 19 di Adria 		

1.2. Scopo e campo di applicazione del documento

Il presente documento è il Manuale dei processi documentali per la conservazione di InfoCert S.p.A., 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 3 dicembre 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/>

Il Manuale è organizzato per sezioni:

1. la prima sezione (capitoli 1-3) fornisce il profilo dell'ULSS, 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 del servizio 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 del servizio della Conservazione, sottolineando input, output e responsabilità di ogni fase. Infine, vengono descritti i controlli effettuati e i processi di ricerca e esibizione a norma dei documenti conservati.
3. la terza sezione (capitoli 10-11) riporta le misure fisiche e logiche di sicurezza adottate.

1.3. Principi di redazione

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

- **Principio di Trasparenza**, il Manuale mira a fornire una chiara spiegazione del sistema di conservazione documentale e dei processi erogati;
- **Ottica di processo**, il documento mira a descrivere le fasi dei processi, 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

<i>ACCESSO</i>	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
<i>ACCREDITAMENTO</i>	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.
<i>AFFIDABILITA’</i>	caratteristica che esprime il livello di fiducia che l’utente ripone nel documento informatico.
<i>AGGREGAZIONE DOCUMENTALE INFORMATICA</i>	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.
<i>ARCHIVIAZIONE</i>	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.
<i>ARCHIVIO</i>	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.
<i>ARCHIVIO INFORMATICO</i>	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
<i>AREA ORGANIZZATIVA OMOGENEA</i>	un insieme di funzioni e di strutture, individuate dall’ 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.
<i>ATTESTAZIONE DI CONFORMITA’ DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO</i>	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.

<i>AUTENTICITA'</i>	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.
<i>BASE DATI</i>	collezione di dati registrati e correlati tra loro.
<i>CERTIFICATORE ACCREDITATO</i>	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.
<i>CICLO DI GESTIONE</i>	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.
<i>CLASSIFICAZIONE</i>	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici.
<i>CODICE</i>	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
<i>CODICE ESEGUIBILE</i>	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
<i>CONSERVATORE ACCREDITATO</i>	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.
<i>CONSERVAZIONE</i>	la conservazione dei documenti e dei fascicoli informatici, disciplinata dal DPCM 3 dicembre 2013, è l'attività volta a proteggere e mantenere nel tempo gli archivi di documenti e dati informatici. Il tempo di conservazione, come ricordato dall'art. 43 del CAD può essere "permanente", cioè indefinito nel futuro o come viene spesso indicato "a lungo termine", cioè un arco temporale sufficientemente ampio da essere interessato da cambiamenti tecnologici. Il suo obiettivo primario è di impedire la perdita o la distruzione non autorizzata dei documenti e di mantenere nel tempo le loro caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.
<i>COPIA ANALOGICA DI UN DOCUMENTO INFORMATICO</i>	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
<i>COPIA DI SICUREZZA</i>	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 del DPCM del 3 dicembre 2013.
<i>DOCUMENTO ANALOGICO</i>	Rappresentazione analogica di atti, fatti o dati giuridicamente rilevanti.

<i>DOCUMENTO INFORMATICO</i>	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
<i>DATI SENSIBILI</i>	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.
<i>ESIBIZIONE</i>	operazione che consente di visualizzare un documento conservato e di ottenerne copia.
<i>EVIDENZA INFORMATICA</i>	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
<i>EXTENSIBLE MARKUP LANGUAGE</i>	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.
<i>FASCICOLO INFORMATICO</i>	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.
<i>FIRMA DIGITALE</i>	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).
<i>FIRMA ELETTRONICA</i>	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).
<i>FIRMA ELETTRONICA</i>	un particolare tipo di firma elettronica avanzata che sia basata su un

<i>QUALIFICATA</i>	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).
<i>FIRMA ELETTRONICA AVANZATA</i>	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.
<i>FORMATO</i>	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
<i>IDENTIFICATIVO UNIVOCO</i>	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.
<i>IMMODIFICABILITA'</i>	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.
<i>IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)</i>	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>INSIEME MINIMO DI METADATI DEL DOCUMENTO INFORMATICO</i>	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.
<i>INTEGRITA'</i>	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
<i>INTEROPERABILITA'</i>	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
<i>LEGGIBILITA'</i>	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
<i>MARCA TEMPORALE</i>	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.

<i>METADATI</i>	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.
<i>PACCHETTO INFORMATIVO</i>	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>PORTABLE DOCUMENT FORMAT</i>	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.
<i>POSTA ELETTRONICA CERTIFICATA</i>	sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici.
<i>PRESA IN CARICO</i>	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
<i>PRODUTTORE</i>	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.
<i>RAPPORTO DI VERSAMENTO</i>	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.
<i>RESPONSABILE DELLA CONSERVAZIONE</i>	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.
<i>RIFERIMENTO TEMPORALE</i>	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.
<i>SCARTO</i>	operazione con cui si eliminano, secondo quanto previsto dalla

	normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
<i>STATICITA'</i>	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.
<i>UTENTE</i>	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.
<i>VERSAMENTO AGLI ARCHIVI DI STATO</i>	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.

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. Il quadro normativo

2.1. Principali riferimenti normativi

- 1) Art. 2220, Codice Civile (“Conservazione delle scritture contabili”);
- 2) Norme sul procedimento amministrativo (L. n. 241/1990)
- 3) Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (“Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”);
- 4) Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. (“Codice in materia di protezione dei dati personali”);
- 5) D. Lgs. 22 gennaio 2004, n.42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio
Il codice garantisce e disciplina la tutela e la valorizzazione del patrimonio e dei beni culturali. Tra i beni culturali citati vi sono gli archivi dei soggetti pubblici oltre che dei soggetti privati dichiarati di interesse storico.
- 6) Decreto Legislativo 7 marzo 2005, n. 82 (“Codice dell'amministrazione digitale”);
- 7) Circolare Agenzia delle entrate n. 36 del 06 dicembre 2006 (“Decreto ministeriale 23 gennaio 2004 – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto”);
- 8) Art. 1, commi 209-213, della Legge 24 dicembre 2007, n. 244 (“Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato – Legge finanziaria 2008”);
- 9) Artt. 19-22 del Decreto Legge 22 giugno 2012, n. 83 (“Misure urgenti per la crescita del Paese”), convertito, con modificazioni, dalla Legge 7 agosto 2012, n. 134, con cui è stata istituita la “Agenzia per l’Italia Digitale” (AGID);
- 10) 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 artt. 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lett. b, 35, comma 2, 36 comma 2, e 71”);
- 11) 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 ai sensi dell’art. 1, commi da 209 a 213, L. 24 dicembre 2007, n. 244”);
- 12) Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 (“Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71, del Codice dell’amministrazione digitale di cui al D.Lgs. n. 82 del 2005”) per quanto applicabile a seguito delle abrogazioni introdotte dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, emanate da AgID il 9 settembre 2020;
- 13) Art. 25 (“Anticipazione obbligo fattura elettronica”) del Decreto Legge 24 aprile 2014, n. 66 (“Misure urgenti per la competitività e la giustizia sociale”), convertito, con modificazioni, dalla Legge 23 giugno 2014, n. 89;
- 14) Circolare Agenzia delle entrate n. 18/E del 24 giugno 2014 (“IVA – Ulteriori istruzioni in tema di fatturazione”);
- 15) REGOLAMENTO UE 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, abroga la direttiva 1999/93/CE-Regolamento eIDAS;

- 16)REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR);
 17)Misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017;
 18)Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, emanate da AgID nel mese di Maggio 2021.

2.2. La normativa in ambito clinico-sanitario

TESTO NORMATIVO	CONTENUTO
Decreto del Presidente del Consiglio dei Ministri del 14 novembre 2015 Definizione delle modalità di attuazione del comma 2 dell'articolo 13 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modifiche, dalla legge 17 dicembre 2012, n. 221.	In materia di prescrizioni farmaceutiche in formato digitale.
Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015, n. 178 Regolamento in materia di fascicolo sanitario elettronico	Fornisce tutte le regole per la formazione e l'utilizzo del Fascicolo Sanitario Elettronico.
Decreto Lgs 21 giugno 2013, n. 69 Disposizioni urgenti per il rilancio dell'economia; art.17 (Misure per favorire la realizzazione del Fascicolo sanitario elettronico)	Sancisce che entro il 31 dicembre 2013, le regioni e le province presentano all'Agenzia per l'Italia digitale il piano di progetto per la realizzazione del FSE
Decreto-legge 18 ottobre 2012, n. 179 - Ulteriori misure urgenti per la crescita del Paese.	Agli articoli 12 e 13 tratta di Fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario, Prescrizione medica e cartella clinica digitale
La diagnostica per immagini - Linee guida nazionali di riferimento - 4 aprile 2012, Intesa tra il Governo, le Regioni e le Province autonome di Trento e di Bolzano	Fornisce le istruzioni per la produzione e la conservazione di immagini diagnostiche e referti digitali.
Decreto - legge n. 78/2010 - Dematerializzazione della ricetta medica cartacea	Fornisce le istruzioni per formare la cosiddetta ricetta rossa digitale
Autorità Garante della Privacy, Linee guida in tema di referti on-line – 19/11/2009	Sul tema della refertazione digitale
Autorità Garante della Privacy, Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario – 16/07/2009	Traccia le principali regole da seguire in tema di privacy e oscuramento del dato
Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere, 2005	Atto di indirizzo che reca indicazioni sui tempi di conservazione dei documenti generati e/o custoditi da Aziende Sanitarie pubbliche ed accreditate, redatto dal Ministero per i Beni e la Attività Culturali, raccogliendo quanto stabilito dalla normativa diffusa in tema. Come per la Circolare 61/86, è possibile mantenere i documenti all'interno del sistema di Conservazione anche a durata illimitata,

grazie a controlli periodici della leggibilità di essi e della loro integrità.

D.lgs 26 maggio 2000, n. 187

Attuazione della direttiva 97/43/Euratom in materia di protezione sanitaria delle persone contro i pericoli delle radiazioni ionizzanti connesse ad esposizioni mediche

Il nucleo della norma è rivolto alla protezione delle persone contro i pericoli delle radiazioni ionizzanti, pur individuando, in allegato 4, dei requisiti specifici per i sistemi di rilevamento delle immagini, nonché dello sviluppo di queste su pellicola. Se il sistema di Conservazione è integrato al PACS, il sistema di Conservazione accoglie al suo interno i medesimi documenti posti all'interno dei sistemi sanitari, non andando ad inficiare la qualità di essi ma anzi garantendo la loro sicurezza, immodificabilità e integrità.

2.3. La normativa sulla fatturazione elettronica

Con il Decreto del 3 aprile 2013 n. 55, emanato dal Consiglio dei Ministri, sono state individuate le regole tecniche e le linee guida per la gestione dei processi di fatturazione elettronica verso la Pubblica Amministrazione. Questo passo rappresenta l'ultimo passaggio del lungo percorso legislativo attivato con la Legge Finanziaria 2008 (più in dettaglio, la Legge 244 del 2007, articolo 1, commi da 209 a 214). Le disposizioni di cui alla suddetta legge finanziaria del 2008 prevedono che, al fine di semplificare il procedimento di fatturazione e registrazione delle operazioni imponibili, l'emissione, la trasmissione, la conservazione e l'archiviazione delle fatture emesse nei rapporti con le pubbliche amministrazioni, anche ad ordinamento autonomo, e con gli enti pubblici nazionali, anche sotto forma di nota, conto, parcella e simili, deve essere effettuata esclusivamente in forma elettronica.

A livello normativo, quindi, tutte le PA destinatarie non potranno né accettare le fatture emesse o trasmesse in forma cartacea né procedere al pagamento, neppure parziale, sino all'invio del documento in forma elettronica.

I fornitori delle amministrazioni pubbliche dovranno invece gestire il proprio ciclo di fatturazione esclusivamente in modalità di fatturazione elettronica.

Decreto ministeriale 3 aprile 2013, numero 55

Art.2, comma 1. *Ai fini del presente regolamento, la fattura elettronica reca i dati e le informazioni indicati e definiti nel documento recante «Formato della fattura elettronica» che costituisce l'allegato A del regolamento.*

Art.2, comma 2. *La fattura elettronica trasmessa alle amministrazioni attraverso il Sistema di interscambio di cui al decreto del Ministro dell'economia e delle finanze 7 marzo 2008 riporta obbligatoriamente le informazioni di cui ai paragrafi 3 e 4 dell'allegato A al presente regolamento.*

Art.2, comma 3 *Le regole tecniche relative alle modalità di emissione della fattura elettronica, nonché alla trasmissione e al ricevimento della stessa attraverso il Sistema di interscambio, sono quelle del documento che costituisce l'allegato B del presente regolamento.*

Art.2, comma 3 *La fattura elettronica si considera trasmessa per via elettronica, ..., e ricevuta dalle amministrazioni di cui all'articolo 1, comma 2, solo a fronte del rilascio della ricevuta di consegna, di cui al paragrafo 4 del documento che costituisce l'allegato B del presente regolamento, da parte del Sistema di interscambio.*

Art.3, comma 1 *Le amministrazioni identificano i propri uffici deputati in via esclusiva alla ricezione delle fatture elettroniche da parte del Sistema di interscambio e ne curano l'inserimento nell'Indice delle Pubbliche Amministrazioni (IPA), ..., in tempo utile per garantirne l'utilizzo in sede di trasmissione delle fatture elettroniche; le stesse amministrazioni curano altresì, agli stessi fini, l'aggiornamento periodico dei propri uffici nel predetto Indice, che provvede ad assegnare il codice in modo univoco.*

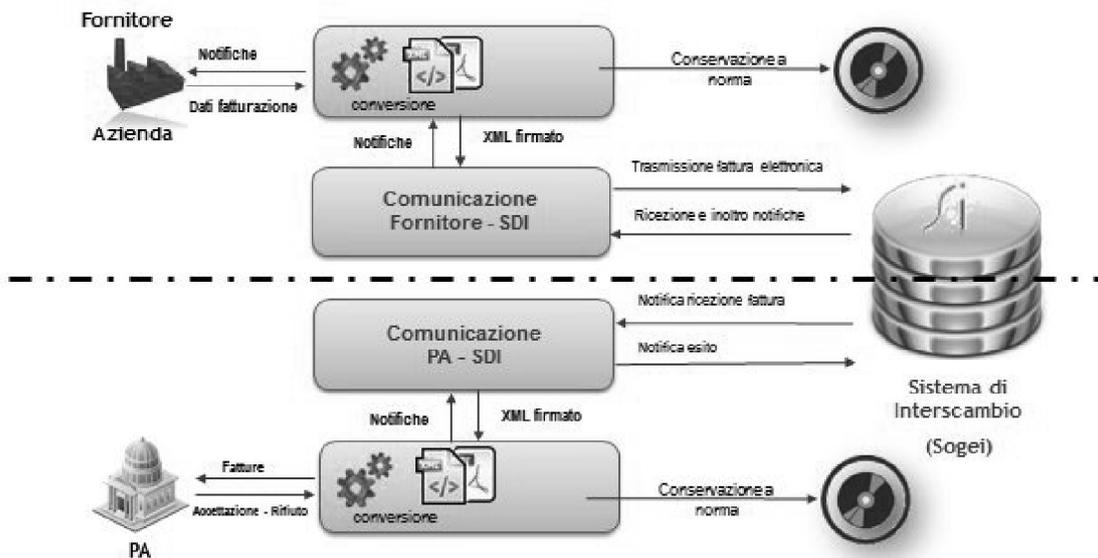
cco le principali novità:

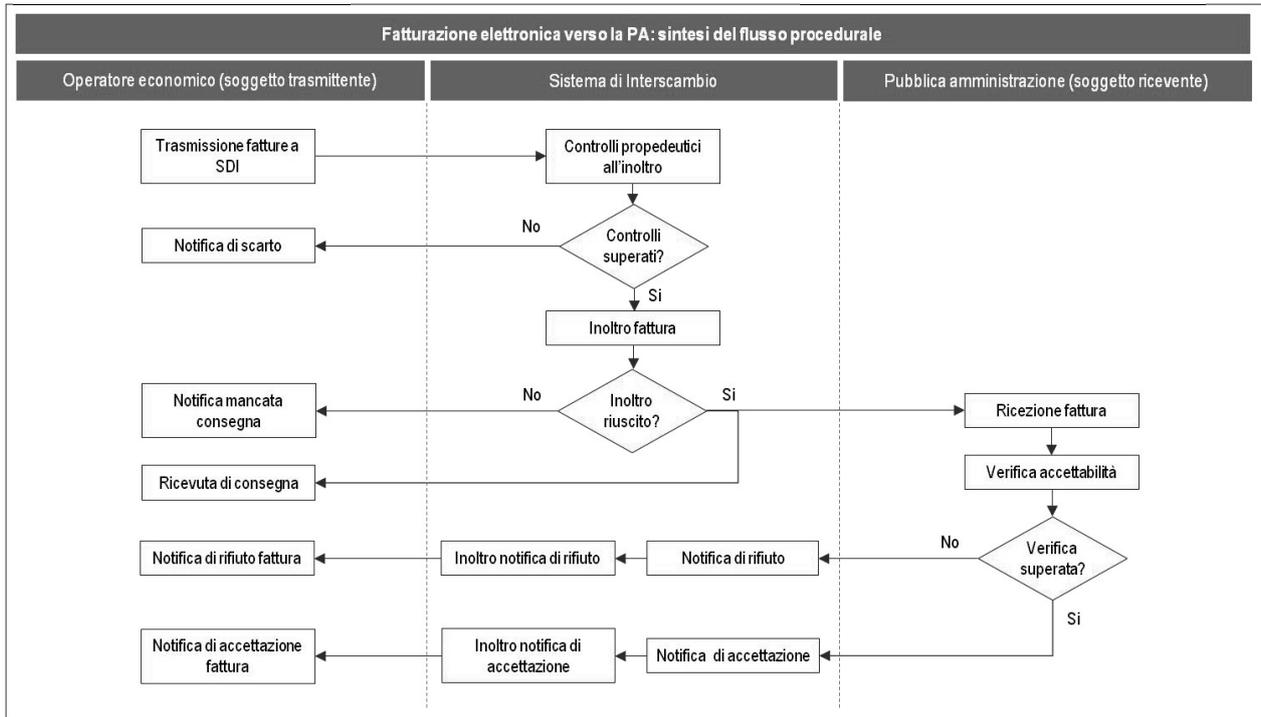
Obblighi e modalità di invio delle fatture elettroniche in conservazione digitale sono regolati dal Decreto MEF del 17 giugno 2014.

Articolo 1 commi dal 209 al 214 Legge numero 244 del 2007, Finanziaria 2008

- **Emissione:** esclusivamente in forma elettronica (XML) delle fatture, note, parcelle, conti e simili.
- **Trasmissione:** esclusivamente con strumenti elettronici, utilizzando il Sistema di Interscambio gestito dall’Agenzia delle Entrate, tramite il «braccio operativo» Sogei.
- **Conservazione:** esclusivamente e obbligatoriamente in forma elettronica, secondo le regole tecniche (DPCM del 3 dicembre 2013 e DMEF del 17 giugno 2014).
- **Pagamento:** le PA destinatarie non potranno né accettare le fatture emesse o trasmesse in forma cartacea né procedere al pagamento, neppure parziale, sino all’invio del documento in forma elettronica.

Di seguito uno schema che descrive le attività previste per il processo di fatturazione elettronica verso la PA





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 e conservazione elettronica documentale.

2.4. Soggetto Produttore: ULSS

Ente	ULSS 5 Polesana
Sede Amministrativa	Viale tre martiri 89 45100 Rovigo
Recapiti	Rovigo - Tel.: 04253931 Trecenta - Tel.: 04257251 Adria - Tel. 0426 940111 protocollo.aulss5@pecveneto.it
Sito web	http://www.aulss5.veneto.it/home/50554.html
Partita IVA	01013470297

2.5. Responsabile della conservazione interno

Ruolo	Responsabile della Conservazione interno al soggetto produttore
Nome e Cognome	Emanuela Terribile
Ente/Società	AZIENDA Ulss 5 Polesana
Data inizio e termine incarico	18 dicembre 2012
Nome e Cognome	Direttore Sanitario
Ente/Società	ULSS5 Polesana - documentazione sanitaria (referti)
Data inizio e termine incarico	21 giugno 2021
Ruolo	Direttore Amministrativo
Nome e Cognome	Leopoldo Ciato
Ente/Società	ULSS5 Polesana - documentazione fiscale (fatturazione)
Data inizio e termine incarico	1 Settembre 2023

Ruolo	Responsabile gestione documentale
Nome e Cognome	Dr.ssa Patrizia Davì
Ente/Società	Azienda ULSS 5 Polesana
Data inizio e termine incarico	1 gennaio 2021
ruolo	Referente Ufficio protezione Dati
Nome e Cognome	Dario Sicchiero
Ente/Società	Azienda Ulss 5 Polesana
Data inizio e termine incarico	10 luglio 2019

2.6. Responsabile del servizio della Conservazione

L'ULSS, 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.

Le attività sono state affidate ad InfoCert SpA, gestore del servizio di conservazione 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 dall'art. 5, comma 1, b) del DPCM 03/12/2013 e dalla precedente Deliberazione CNIPA 11/2004.

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

Più in particolare l'art. 7 del DPCM 03/12/2013 precisa che il Responsabile della Conservazione:

- 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) 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.

2.7. InfoCert SPA – Conservatore

Denominazione sociale	InfoCert S.p.A.
Sede Legale:	Piazza Sallustio, 9, 00187 Roma Tel.+39 06 836691
Sedi Operative:	<ul style="list-style-type: none"> ● Piazza da Porto, 3, 35131 Padova ● Via Carlo Bo, 11, 20143 Milano ● 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 un 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.

3. Il sistema di creazione e gestione dei documenti

Si rimanda al Manuale di Gestione del protocollo e degli archivi dell'ULSS per la descrizione funzionale ed operativa del sistema di gestione, protocollazione e fascicolazione informatica dei documenti. Il riferimento è contenuto nelle seguenti deliberazioni:

- deliberazione del Direttore Generale n. 916 del 27 dicembre 2011 *“Linee guida sull'utilizzo della posta elettronica e della posta elettronica certificata (PEC).”*
- deliberazione del Direttore Generale n. 965 del 22 novembre 2018 *“Adozione del Prontuario di selezione per lo scarto dei documenti dell'Azienda Ulss 5 Polesana “*
- Manuale Utente HelthCare - Ditta Westpole del 15 luglio 2021

3.1. Strumenti utilizzati

Preliminarmente al processo di Conservazione dei documenti e delle immagini vi è quello di archiviazione interna in appositi Database aziendali (con identificazione univoca dei singoli documenti):

1. Repository di GPI per i referti (sanitario)
2. Sistemi PACS EBIT per le immagini diagnostiche (sanitario)
3. Protocollo informatico Healthcare di Westpole per il registro giornaliero di protocollo, documenti protocollati e i fascicoli
4. Gestionale di contabilità di Dedalus con LegalCareLegalinvoicePA per la fatturazione attiva e passiva. (bilancio)

Da questi Repository e Sistemi di Gestione i documenti vengono estratti e inviati in conservazione attraverso LegalCare, come si specificherà in seguito.

3.2. Servizi di certificazione

L'ULSS ha dotato di firma digitale tramite smartcard/badge tutti i medici e tutti i caposala.

La marcatura temporale dei documenti sottoscritti digitalmente avviene all'interno del processo di conservazione LegalDoc, a cura di InfoCert, come descritto in seguito.

3.3. Controlli

Ai sensi di legge, l'ULSS 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.

3.4. Indicizzazione dei documenti

L'ULSS provvede all'indicizzazione dei documenti utilizzando le funzioni messe a disposizione dai sistemi di creazione e gestione dei documenti sopra elencati secondo le specifiche di metadattazione concordate nei documenti tecnico-contrattuali allegati al presente Manuale.

3.5. Formato dei documenti

Il DPCM del 3 dicembre 2013 elenca in allegato i formati adatti alla conservazione a lungo termine.

L'ULSS ha deciso di inviare in conservazione i seguenti formati:

PDF, PDF/A, XML, JPEG/JPG, GIF, MSG, EML, ZIP, MCDA2, RTF, TIFF, TXT, HTML.

Eventualmente firmati digitalmente e/o marcati temporalmente.

Per i documenti ricevuti a Protocollo in formati non conformi alla citata normativa (formati non statici o soggetti all'acquisto di licenze) nel pregresso (anni 2005-2016) si è scelto di realizzare dei pacchetti di versamento in formato ZIP.

Ad oggi il Protocollo filtra i formati non conformi alla normativa vigente.

L'ULSS si impegna a mantenere gli strumenti necessari alla leggibilità dei documenti contenuti all'interno dei formati EML e ZIP.

Il sistema permette di aggiornare e inserire nuovi formati in base alle esigenze dell'ULSS e della normativa vigente.

4. Il sistema di conservazione documentale

4.1. 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.

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 XML, detto Indice del Pacchetto di Archiviazione (IPdA). L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto è detto Rapporto di Versamento.

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:

1. informazioni sull'applicazione che ha generato l'IPdA;
2. il token del documento (ovvero il suo identificativo univoco);
3. l'operazione eseguita (conservazione, rettifica, scarto e cancellazione);
4. il bucket (ovvero l'area di conservazione) associato al Soggetto Produttore e la policy utilizzata;
5. il nome dei file che compongono il documento, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte;
6. eventuali informazioni relative al documento rettificante e rettificato;
7. il tempo di creazione (timestamp) del file IPdA;
8. 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 ospedaliero 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 l'ULSS sceglie di conservare.

4.2. Descrizione generale del servizio

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 sdemanializzazione 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.

LegalDoc integra il sistema di gestione documentale in uso da ULSS 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 ULSS sceglie di conservare.

4.3. Definizione di documento

In LegalDoc il documento è un insieme di uno o più file digitali. Ad ogni documento è associato un Indice 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 un file;
- è memorizzato sui supporti previsti dalla procedura di conservazione;
- è identificato in maniera univoca attraverso il token LegalDoc;
- è conservato insieme al file Indice di Conservazione (è il file XML contenente i metadati associati al documento automaticamente firmato digitalmente e marcato temporalmente dal Responsabile del servizio della Conservazione).

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

4.4. Configurazione dei sistemi

LegalCare è la soluzione integrata, costituita da una componente locale (L-Care), installata presso l'ULSS, che si occupa del recupero dei documenti dai sistemi nativi e monitorizza i flussi documentali verso la componente remota (LegalDoc, in ASP) che invece si occupa della vera e propria conservazione a norma.

Il vantaggio dell'adozione di L -Care sta nel fatto di utilizzare una componente che risolve tutte le problematiche di acquisizione dei dati sollevando il Soggetto Produttore dalle incombenze dovute alla integrazione tra sistemi complessi (RIS, PACS, Repository, ecc..).

L'architettura generale è schematizzata a titolo di esempio nella seguente figura:

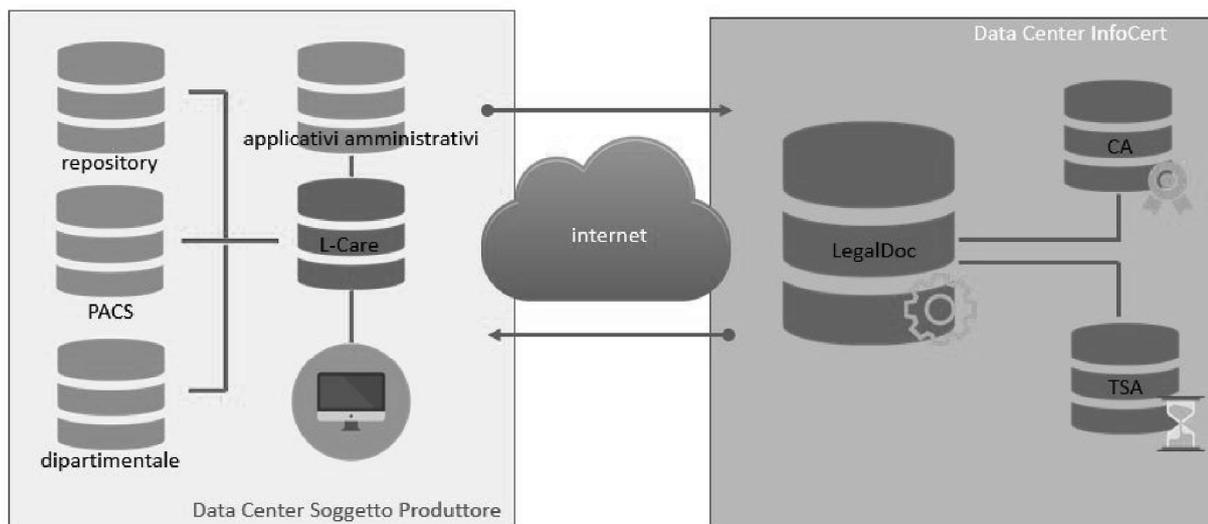


Figura 1 – Infrastruttura tecnologica LegalCare

4.5. Componenti

4.5.1. Componente locale L-Care

La componente locale L-Care si configura come il punto di consolidamento prima delle operazioni di conservazione a norma in ASP. Questo elemento, fortemente specifico dell'ambito ospedaliero, è in grado di interfacciarsi con i flussi di lavoro sanitari per ricevere, prelevare o catturare documenti e metadati ad essi associati al fine di costituire l'insieme dei dati da sottoporre al flusso di conservazione.

Il ruolo di L-Care è quello di mediare il più possibile la molteplicità e l'eterogeneità dei flussi informativi ospedalieri con una piattaforma di conservazione estremamente stabile, collaudata e general-purpose come LegalDoc.

L-Care si presenta dunque come uno strumento dinamico e ricco di plug-in per la comunicazione con altri applicativi: HL7 (v2.x o v3, via socket, web-service, filesystem, etc.), DICOM (store e print), SOAP (programmabile, es. conforme AS-SEVO-SELG#04), supporto database multi-protocollo (JDBC, ODBC, Perl::DBI, etc.), network filesystem (es. SMB/CIFS, NFS, etc.), file transfer protocol (es. FTP, SFTP, etc.), HTTP/HTTPS, WebDAV, SMTP, JMS, sistemi di cattura del traffico (es. packet capture) e diversi formati di file per i metadati (es. TXT, XML, XLS, CSV, MDB, etc.).

L-Care, inoltre, si occupa di effettuare tutte le verifiche e i controlli necessari prima del versamento in LegalDoc (verifica di firme digitali e marche temporali, formato-file, ecc..).

Un altro punto forte di L-Care è l'architettura interna, studiata per eseguire contemporaneamente un grande numero di processi per smaltire rapidamente agevolmente i processi di consolidamento, unitamente alle caratteristiche di alta disponibilità, in grado di dare luogo al failover in tempi estremamente rapidi (qualche secondo).

La componente L-Care locale è installata presso la sala server dell'ULSS 5 Polesana.

4.5.2. Ambienti di conservazione

Per l'ULSS 5 Polesana sono stati mantenuti due ambienti separati (bucket): B130 per il Distretto di Adria e B131 per il Distretto di Rovigo.

4.5.3. Marca temporale sui pacchetti di archiviazione

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.

4.5.4. Firma digitale sui pacchetti di archiviazione con dispositivo HSM

Al buon esito del processo di conservazione, il Responsabile del servizio della Conservazione InfoCert appone la propria firma digitale sul file di indice di conservazione mediante un sistema di firma automatica erogato dalla CA InfoCert, che si avvale di un dispositivo crittografico ad altre prestazioni HSM.

4.5.5. Supporti di conservazione

Ai fini della conservazione i documenti vengono raggruppati in pacchetti di versamento, di archiviazione e di distribuzione.

L'apposizione della firma digitale del Responsabile del servizio della Conservazione per ogni indice di conservazione su ogni file attesta la conservazione stessa.

5. Gestione degli Errori

Il sistema di conservazione LegalDoc è configurato per accettare solo documenti in formati prestabiliti e caratteristiche concordate. Al venir meno di una di queste condizioni, sopraggiungendo l'impossibilità per LegalDoc di accettare il documento, L-Care lascia in attesa il documento in entrata senza immetterlo nel sistema di conservazione e contestualmente segnala l'anomalia all'ULSS tramite la Broker Consolle di amministrazione, accessibile mediante autenticazione.

I Responsabili designati dell'ULSS possono in qualsiasi momento monitorare lo stato (Conservato/Errore) dei documenti attraverso Broker Consolle.

In caso di incident vengono predisposti e conservati appositi verbali.

5.1. 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.

5.1.1. 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 del servizio della Conservazione o da un suo delegato.

5.1.2. 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.

5.1.3. 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 esposti 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.

5.1.4. 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.

6. Le tipologie documentali

1. REGISTRO GIORNALIERO E ANNUALE DI PROTOCOLLO

<i>Natura del documento</i>	Registro dei protocolli formato e versato automaticamente ogni giorno e Registro annuale formato ogni anno
<i>Data di decorrenza del processo di conservazione elettronica</i>	12 ottobre 2015 REGISTRO GIORNALIERO 31 dicembre 2005 REGISTRO ANNUALE
<i>Modalità di versamento</i>	I documenti vengono inviati al sistema di conservazione tramite messaggi scambiati attraverso le tabelle di frontiera tra il sistema LegalCare

2. DOCUMENTO PROTOCOLLATO

Natura del documento	Documenti originali digitali o analogici scansionati, protocollati e allegati all'interno dell'applicativo, Healthcare
Data di decorrenza del processo di conservazione elettronica	19 luglio 2021
Modalità di versamento	I documenti vengono inviati al sistema di conservazione tramite messaggi scambiati attraverso le tabelle di frontiera tra i sistemi Healthcare e LegalCare.

3. REFERTI

Natura del documento	Referti di Laboratorio Analisi firmati digitalmente dai medici refertanti referti di diagnostica per immagini e documenti clinici specialistici prodotti con la cartella informatizzata
Data di decorrenza del processo di conservazione elettronica	2013
Modalità di versamento	I documenti vengono inviati al sistema di conservazione tramite messaggi scambiati attraverso le tabelle di frontiera tra i sistemi di Repository di Insiel e LegalCare

4. STORICO REFERTI

Natura del documento	Referti di Laboratorio e Analisi firmati digitalmente dai medici refertanti....vedi commento sopra per parte di radiologia e referti specialistici prodotti dalla cartella informatizzata
Data di decorrenza del processo di conservazione elettronica	2013
Modalità di versamento	I documenti vengono inviati al sistema di conservazione tramite messaggi scambiati attraverso le tabelle di frontiera tra i sistemi di Repository di Insiel e LegalCare

5. FATTURA ELETTRONICA PA ATTIVA

Natura del documento	Fatture XML
Data di decorrenza del processo di conservazione elettronica	Marzo 2015
Modalità di versamento	I documenti vengono inviati al sistema di conservazione tramite

	chiamate HL7 scambiati tra i sistemi di Dedalus e il connettore LegalCare, dopo che le fatture sono state create all'interno del sistema di contabilità e inviate al Sistema di Interscambio.
--	---

6. FATTURA ELETTRONICA PA PASSIVA

<i>Natura del documento</i>	Fatture XML
<i>Data di decorrenza del processo di conservazione elettronica</i>	Marzo 2015
<i>Modalità di versamento</i>	I documenti vengono inviati al sistema di conservazione tramite chiamate HL7 scambiati tra i sistemi di Dedalus e il connettore LegalCare, dopo che le fatture sono state ricevute su PEC dedicata e liquidate nel gestionale Dedalus.

7. NOTIFICHE FATTURAZIONE ELETTRONICA PA ATTIVA

<i>Natura del documento</i>	Notifiche SDI
<i>Data di decorrenza del processo di conservazione elettronica</i>	2016
<i>Modalità di versamento</i>	I documenti vengono inviati al sistema di conservazione tramite chiamate HL7 scambiati tra i sistemi di Dedalus e il connettore LegalCare, dopo che le fatture sono state create all'interno del sistema di contabilità e inviate al Sistema di Interscambio.

8. NOTIFICHE FATTURAZIONE ELETTRONICA PA PASSIVA

<i>Natura del documento</i>	Notifiche SDI
<i>Data di decorrenza del processo di conservazione elettronica</i>	2016
<i>Modalità di versamento</i>	I documenti vengono inviati al sistema di conservazione tramite chiamate HL7 scambiati tra i sistemi di Dedalus e il connettore LegalCare, dopo che le fatture sono state ricevute su PEC dedicata e liquidate nel gestionale Dedalus.

7. Il processo di conservazione

Il processo di conservazione prevede l'accettazione di un pacchetto di versamento, formato dal documento da conservare e dai metadati ad esso associati e la conservazione di un pacchetto di archiviazione: il documento, ricevuto nei Data Center di InfoCert in formato digitale statico non modificabile, viene conservato a norma, corredato dall'Indice del Pacchetto di Archiviazione (Indice di Conservazione) generato dal sistema, che contiene i metadati in formato UNI SINCRO e le informazioni di conservazione del documento ed è firmato digitalmente e marcato temporalmente dal Responsabile del servizio di InfoCert.

Il sistema di conservazione, quindi, integra il sistema di gestione dell'ULSS e ne estende i servizi con funzionalità di stoccaggio digitale (archivio di deposito).

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

7.1. Tabella di Responsabilità

<i>Attività</i>	<i>ULSS</i>	<i>LegalCare</i>	<i>LegalDoc</i>	<i>Responsabile del servizio della Conservazione</i>
1. Formazione del documento	R - E			
2. Indicizzazione e archiviazione	R - E			
3. Acquisizione documento e creazione del file Indice di conservazione	V	R - E		
4. Invio al sistema di conservazione		R - E		
5. Verifica e accettazione del documento			E - V	
6. Creazione del file di Indice			E	R - V* - A
7. 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 del servizio della Conservazione sono garantite anche dal servizio di auditing InfoCert.

7.2. Fasi del processo di conservazione della documentazione amministrativa e sanitaria

Formazione del documento

<i>INPUT</i>	<i>Documento da generare</i>	
ULSS	1.1	ULSS genera i documenti statici e non modificabili, secondo le procedure descritte precedentemente
<i>OUTPUT</i>	<i>Documento generato</i>	

Indicizzazione e archiviazione

<i>INPUT</i>	<i>Documento da archiviare</i>	
ULSS	1.1	L'ULSS provvede all'indicizzazione dei documenti utilizzando le funzioni messe a disposizione dai sistemi di creazione e gestione dei documenti sopra elencati secondo le specifiche di metadattazione contenute nella Scheda dati Tecnici per l'attivazione, allegata al presente Manuale.
<i>OUTPUT</i>	<i>Documento indicizzato e archiviato</i>	

Acquisizione documento e creazione del file delle direttive

<i>INPUT</i>	<i>File delle direttive da predisporre</i>	
L- Care	2.1	L- Care acquisisce i documenti informatici condivisi nel gestore documentale del ULSS e li prepara alla conservazione
	2.2	Il servizio L- Care 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
<i>OUTPUT</i>	<i>File delle direttive predisposto</i>	

Invio al sistema di conservazione

INPUT	<i>Documento da inviare a LegalDoc</i>	
L- Care	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	Presa 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	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.
	4.8	Generazione del file di ricevuta a partire dal file delle direttive.
	4.9	Generazione di un identificativo univoco per il documento (token LegalDoc) e firma elettronica sul file di ricevuta.
	4.10	Invio a L-Care del file di ricevuta di presa in carico della richiesta di conservazione.
L- Care	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. Restituisce il token tramite messaggi HL7 a E-Repository
OUTPUT	<i>Documento verificato</i>	

Creazione del file di controllo

INPUT	<i>Documento da conservare</i>	
LegalDoc	5.1	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.
	5.2	Apposizione della firma digitale del Responsabile del servizio della

	Conservazione sul file di controllo e sul file di indice.
OUTPUT	<i>Documento inserito in conservazione</i>

Memorizzazione, creazione copia di sicurezza e chiusura della conservazione

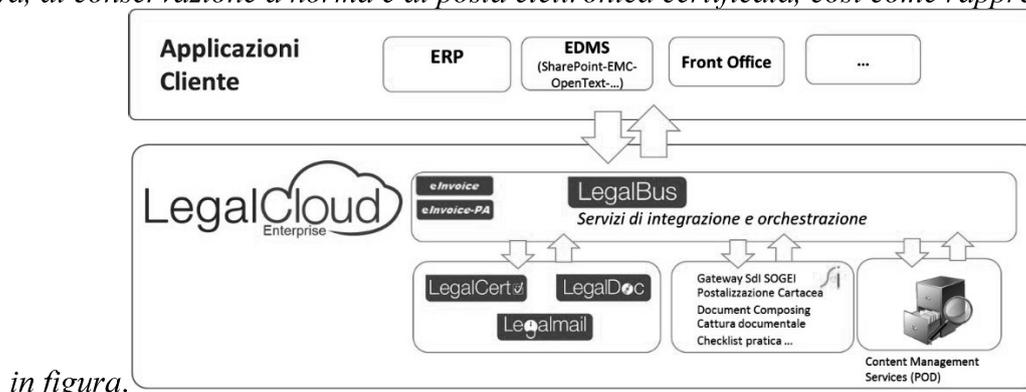
INPUT	<i>Documenti da memorizzare</i>	
LegalDoc	8.1	Memorizzazione del file su supporto magnetico.
	8.2	Creazione delle copie di sicurezza.
	8.3	Termine della procedura di conservazione.
OUTPUT	<i>Documenti conservati</i>	

7.3. Fasi del processo di conservazione delle Fatture PA

Le componenti applicative interessate nel processo di gestione delle fatture PA sono le seguenti:

1. *LegalCare, installata presso la ULSS per la gestione del flusso di conservazione dei documenti XML di fatturazione e di notifica prodotti; LegalCare è composto da una componente locale (L-Care), installata presso l'ULSS, che si occupa del recupero dei documenti dai sistemi nativi e monitora i flussi documentali verso la componente remota (LegalDoc) che invece si occupa della conservazione digitale a norma.*

2. *LegalBus, un middleware applicativo, facilmente integrabile, capace di orchestrare i vari servizi InfoCert. Di base integra, espone e richiama i servizi di firma digitale automatica massiva, di conservazione a norma e di posta elettronica certificata, così come rappresentato*



in figura.

Architettura di LegalBus

3. Servizio di Firma Digitale Automatica, che permette l'apposizione di firme digitali attraverso procedure automatiche, su un grande numero di documenti in breve tempo.

4. Servizio di conservazione a norma LegalDoc, già utilizzato dall'ULSS per la tenuta dei documenti sanitari (si rimanda al *Manuale dei processi di formazione e conservazione dei documenti elettronici* già in uso presso l'ULSS);

5. Servizio di Posta Elettronica Certificata Legalmail, impiegato per le comunicazioni con il Sistema di Interscambio tramite due caselle appositamente create.

7.3.1. Ciclo attivo

L'ULSS produce le FatturePA del suo ciclo attivo mediante il gestionale di contabilità e in formato XML, come previsto dalla normativa.

L'invio al Sistema di interscambio avviene mediante Legal-Care il middleware di integrazione precedentemente descritto.

Le FatturePA, quindi, generate dal sistema di contabilità in uso, vengono inviate a L-Care, tramite Network File System, e conseguentemente a LegalBus, che si occupa:

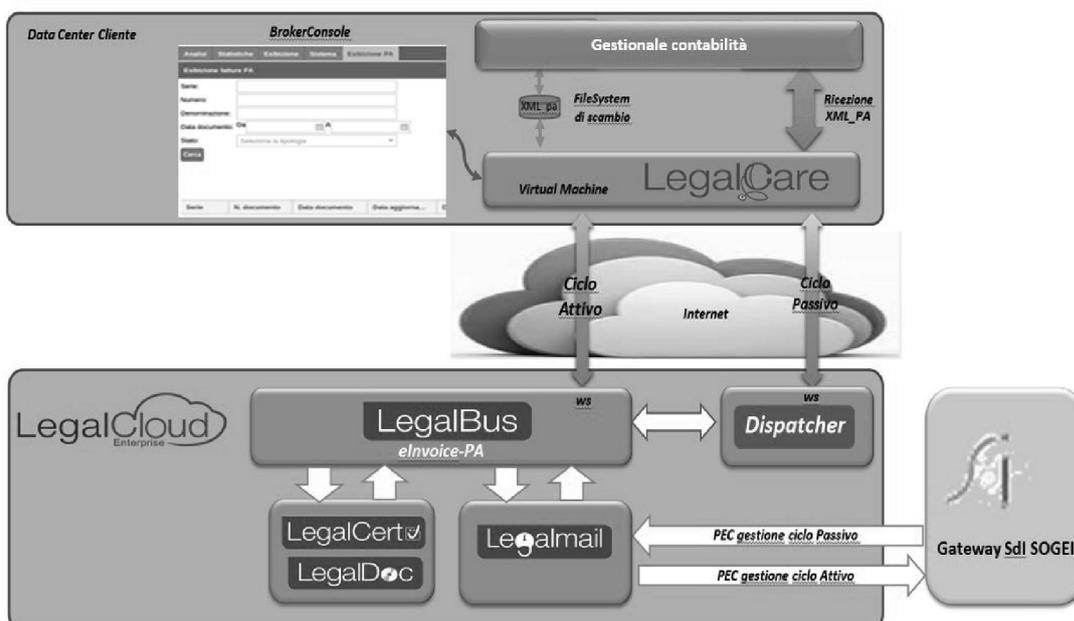
- dell'apposizione della firma digitale sulle fatture
- dell'invio tramite PEC dedicata al Sistema di Interscambio (di seguito SdI)
- della ricezione delle notifiche dal SdI
- dell'indicizzazione delle fatture e delle notifiche
- dell'invio in conservazione LegalDoc.

7.3.2. Ciclo passivo

L'ULSS riceve le FatturePA del suo ciclo passivo dal SdI in una PEC dedicata.

La componente LegalBus si occupa di colloquiare con il SdI di Sogei mediante l'utilizzo della casella PEC, ne sbusta il contenuto ed effettua le opportune verifiche di integrità e validità dei file XML firmati ricevuti in allegato alla PEC. LegalBus li rende disponibili al sistema LegalCare che, a sua volta, li trasmette al sistema di gestione documentale e contabile in uso presso l'ULSS.

Contemporaneamente LegalBus si occupa dell'invio al sistema di conservazione LegalDoc delle FatturePA e delle notifiche.



Architettura del processo

8. Procedure di ricerca ed esibizione

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

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.

Dal pulsante 'Esibizione a norma' è possibile accedere a:

- L'Indice di Conservazione UNI SINCRO, altrimenti detto Indice del Pacchetto di Archiviazione (firmato e marcato dal Responsabile del servizio di InfoCert)
- File di parametri (contante le informazioni per la leggibilità nel tempo)
- File di indici (contenente i metadati del documento conservato)
- File di dati (documento conservato).

L'esibizione del documento ottenuto tramite interrogazione al sistema LegalDoc rappresenta un'esibizione completa e legalmente valida ai sensi delle Regole Tecniche del DPCM 3 dicembre 2013.

8.1. Broker Console LegalCare

La BrokerConsole di LegalCare mette a disposizione un motore di ricerca che consente all'utente di effettuare delle ricerche per aprire l'esibitore LegalDoc direttamente sul documento di interesse.

Per accedere all'interfaccia di BrokerConsole occorre connettersi al sistema, mediante un browser web (Microsoft Internet Explorer 5.5 o superiori, Netscape 7.2, Mozilla 1.4 o superiori, Firefox 1.0 o superiori, Safari 1.2 o superiori, Opera 9.2 o superiori, Chrome.....), digitando come indirizzo il seguente:

<https://10.1.102.203/BrokerConsole/>

Ogni utente è configurato con delle specifiche regole di accesso che gli consentono solo alcune operazioni. La definizione degli utenti viene effettuata da InfoCert sulla base delle richieste espresse dall'ULSS in fase di attivazione del servizio.

La BrokerConsole è suddivisa in sezioni per:

- **Analisi:** consente la visione dello stato di elaborazione dei documenti (referti, immagini o studi, altri documenti). Permette di gestire anche l'estrazione dei documenti in errore e la gestione del recupero degli stessi.
- **Statistiche:** consente di avere una panoramica dell'andamento del processo di conservazione, esponendo graficamente il numero dei documenti ricevuti, conservati, in errore e bloccati in funzione di diversi intervalli temporali impostabili dall'utente.
- **Esibizione:** consente di ricercare un documento conservato e di attivare l'interfaccia di esibizione, come dettagliato in seguito.
- **Sistema:** consente di visualizzare lo stato di carico del sistema e la quantità di spazio utilizzato.
- **Utenti:** attiva solo per gli utenti configurati come amministratori, permette la gestione di tutti gli utenti registrati nel sistema e dei loro permessi.

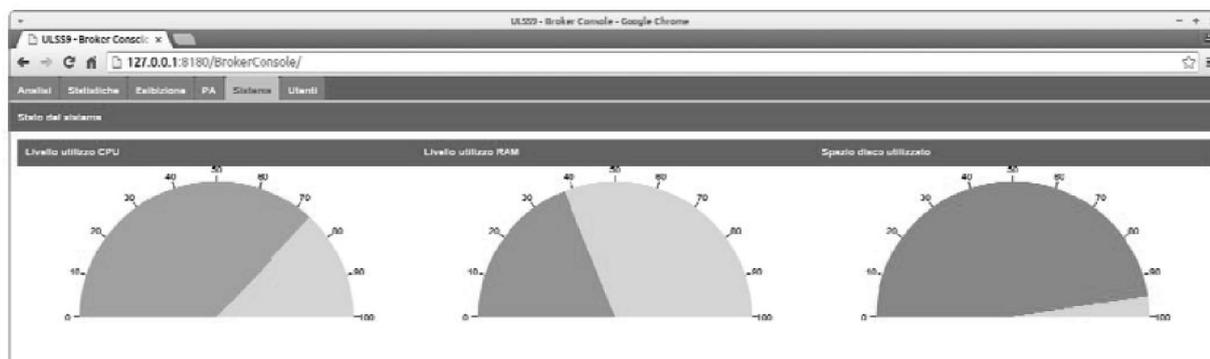


Figura 2 – Visibilità grafica dello stato del Sistema con BrokerConsole

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

8.2. Procedura di esibizione: dettaglio

Ricerca del documento da esibire

INPUT	<i>Lista di documenti</i>	
ULSS	1.1	Attraverso L-Care 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>	
L-Care	2.1	L-Care 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 dall'ULSS e quelli dei documenti conservati; effettuazione della copia dei file costituenti il documento e dei file attestanti il processo di conservazione.
	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 L-care
OUTPUT	<i>Documento passato all'Esibitore L-care</i>	

Verifica del documento tramite esibitore

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

Download del documento tramite L-care

INPUT	<i>Documento esibito</i>	
Esibitore L-care	5.1	Download del documento e memorizzazione dello stesso in locale
OUTPUT	<i>Documento salvato</i>	

8.3. Approfondimento della precedente versione di LegalDoc

Il 12 aprile 2014 è entrato in vigore il citato DPCM del 3 dicembre 2013, recante le nuove Regole Tecniche in materia di Conservazione, lasciando agli enti che già avevano attivato un sistema di conservazione, come nel caso di questa ULSS, 36 mesi di tempo per l'adeguamento dei sistemi (aprile 2017).

L'ULSS ha conservato i propri documenti prima in un sistema di conservazione aderente alla Deliberazione CNIPA 11/2004 e successivamente, dall'autunno 2016, nel nuovo sistema di conservazione, aderente al DPCM del 3 dicembre 2013, entrambi sviluppati e gestiti da InfoCert.

Sebbene non vi siano modifiche nell'attività dell'ULSS ma solo nelle attività di LegalCare, che permette la ricerca/esibizione nei diversi ambienti, di seguito si riassumono le principali differenze tra i due sistemi:

	Precedente LegalDoc	Nuovo LegalDoc
<i>Normativa di riferimento</i>	Deliberazione CNIPA 11/2004	DPCM 3 dicembre 2013 e standard UniSincro
<i>Tempistiche di versamento</i>	Invio in conservazione asincrono di lotti di documenti omogenei	Invio in conservazione sincrono (immediato) di ogni singolo documento
<i>Tipologia di chiamate</i>	Soap	Rest
<i>Autenticazione</i>	Tramite p12 + chiave accesso attribuita all'SGD	Basic authentication tramite user/password
<i>Numero file dati in una richiesta di conservazione</i>	Da 1 a 50	1
<i>Restituzione del token (identificativo univoco)</i>	Il token è presente nel file ldmsg_conserve_result.xml 1 lungo 32 caratteri	Il token è presente nel file IdC (Indice di Conservazione) ed è di 64 caratteri
<i>Indicizzazione</i>	Facoltativa ed esterna	Obbligatoria
<i>Firma del Responsabile del Servizio di Conservazione</i>	La firma è apposta sul file di chiusura del lotto	La firma è apposta sul file IdC (Indice di Conservazione), associato ogni singolo documento
<i>Esibitore</i>	Rif. <i>Manuale utente esibitore LegalDoc</i>	Rif. <i>Manuale utente esibitore NDoc</i>

8.4. Requisiti software

Per la visualizzazione e la stampa del documento ottenuto con la procedura di esibizione da LegalDoc, l'ULSS 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.

Per la verifica del file di controllo del documento e del file di ricevuta si utilizza il prodotto Dike o un qualunque software di verifica presente in commercio.

9. Modifica e scarto dei documenti conservati

In caso di modifica dei documenti già posti in conservazione, l'ULSS provvede ad emanare ex novo un documento di rettifica che verrà a sua volta conservato a norma, senza cancellare il documento rettificato.

La riconducibilità del documento modificante a quello modificato è resa possibile grazie agli indici (metadati) predisposti dall'ULSS in fase di caricamento, che ne assicura la sistematicità e la coerenza.

Per il principio di tracciabilità informatica, il sistema tiene memoria sia del documento rettificante che del documento rettificato.

Per le procedure di scarto archivistico si rimanda al Manuale della Conservazione standard di InfoCert (cap.7.8).

10. Misure di sicurezza

10.1. 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.

10.1.1. Sicurezza fisica

I locali che ospitano il sistema LegalDoc sono in un immobile la cui zona di 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.

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

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

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

All'interno dei Sistemi Informativi è dotato 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.

10.1.2. 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.

10.1.3. 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.

10.1.4. 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.