

Allegato A

**Manuale dei processi per la
conservazione documentale
digitale
I.O.V.**



SOMMARIO

	SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO	3 -
	GLOSSARIO.....	4 -
	NORMATIVA DI RIFERIMENTO	9 -
	RUOLI E RESPONSABILITÀ	11 -
1	OGGETTI SOTTOPOSTI ALLA CONSERVAZIONE	14 -
2	PROCESSI DI FORMAZIONE E GESTIONE PER TIPOLOGIA DOCUMENTALE	14 -
3	DESCRIZIONE DEL SERVIZIO	16 -
4	RESPONSABILITÀ	17 -
5	CONFIGURAZIONE DEI SISTEMI	17 -
6	LEGALCARE.....	18 -
	LEGALDOC WEB	19 -
	MARCA TEMPORALE DEI PACCHETTI DI ARCHIVIAZIONE	20 -
	FIRMA DIGITALE CON DISPOSITIVO HSM DEI PACCHETTI DI ARCHIVIAZIONE.....	20 -
	SUPPORTI DI CONSERVAZIONE.....	20 -
	CONTROLLI DI PROCESSO.....	21 -
	ANALISI DEGLI ERRORI	21 -
	PROCEDURE DI RICERCA ED ESIBIZIONE IN LEGALDOC WEB.....	22 -
	PROCEDURE DI RICERCA ED ESIBIZIONE NELLA BROKERCONSOLE LEGALCARE	25 -
	PROCEDURA DI ESIBIZIONE LEGALCARE: DETTAGLIO	26 -
	RICERCA DEL DOCUMENTO DA ESIBIRE	26 -
	INVIO DELLA RICHIESTA A LEGALDOC	27 -
7	RICERCA DEL DOCUMENTO NEL SISTEMA ED ESIBIZIONE.....	27 -
	VERIFICA DEL DOCUMENTO TRAMITE ESIBITORE	27 -
	DOWNLOAD DEL DOCUMENTO TRAMITE L-CARE.....	28 -
	SICUREZZA E PROTEZIONE DEI DATI	29 -
	CED ISTITUTO	29 -
8	INFOCERT	29 -
	NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI, AI SENSI DEL REGOLAMENTO UE N. 679/2016.....	30 -
	POLICY PRIVACY BY DESIGN E BY DEFAULT	30 -
	DOCUMENTAZIONE RICHIAMATA E AGLI ATTI.....	31 -



SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO

1

Il presente documento è il Manuale dei processi documentali per la conservazione dell'**Istituto Oncologico Veneto**, 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), del Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 e delle Linee Guida di AgID su formazione, gestione e conservazione documentale.

Come richiesto dal DPCM del 2013 all'art. 8, il presente documento **“illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione”**.

In caso di ispezione da parte delle autorità di vigilanza preposte, il Manuale dei processi documentali per la conservazione, permette un agevole svolgimento di tutte le attività di controllo.

GLOSSARIO

2

ACCESSO	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
ACCREDITAMENTO	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione.
AFFIDABILITA'	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
ARCHIVIAZIONE	Processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.
AGID	Agenzia per l'Italia Digitale.
ARCHIVIO	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un Soggetto Produttore durante lo svolgimento dell'attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
ASP	Application Service Provider.
AUTENTICITA'	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
CA	Certification Authority.
CAD	Codice Amministrazione Digitale D.lgs. 82 del 7 marzo 2005 e successive modifiche.
CONSERVATORE ACCREDITATO	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
CODICE ESEGUIBILE	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.

CONSERVAZIONE	La conservazione dei documenti e dei fascicoli informatici, disciplinata dal DPCM 3 dicembre 2013, è l'attività volta a proteggere e mantenere nel tempo gli archivi di documenti e dati informatici. Il suo obiettivo primario è di impedire la perdita o la distruzione non autorizzata dei documenti e di mantenere nel tempo le loro caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.
COPIA ANALOGICA DI UN DOCUMENTO INFORMATICO	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
COPIA DI SICUREZZA	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 del DPCM del 3 dicembre 2013.
D. LGS	Decreto Legislativo.
DPCM	Decreto della Presidenza del Consiglio dei Ministri.
DPR	Decreto del Presidente della Repubblica.
DOCUMENTO ANALOGICO	Rappresentazione analogica di atti, fatti o dati giuridicamente rilevanti.
DOCUMENTO INFORMATICO	Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
ESIBIZIONE	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
EVIDENZA INFORMATICA	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
EXTENSIBLE MARKUP LANGUAGE	Linguaggio derivato dall'SGML (Standard Generalized Markup Language), metalinguaggio che permette di creare altri linguaggi. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags).
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).
FORMATO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
GU	Gazzetta Ufficiale della Repubblica Italiana.

HSM	Hardware Security Module.
IDENTIFICATIVO UNIVOCO (di seguito detto Token)	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione. Detto anche token LegalDoc.
IMMODIFICABILITA'	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
INTEGRITA'	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
INTEROPERABILITA'	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
LEGGIBILITA'	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
MARCA TEMPORALE	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (art. 1, lettera m del DPCM 22 febbraio 2013). La marca temporale emessa in conformità con quanto previsto dal DPCM 22 febbraio 2013, titolo IV è opponibile ai terzi ai sensi dell'art. 41 dello stesso decreto.
MEF	Ministero dell'Economia e delle Finanze.
METADATI	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM del 3 dicembre 2013.
NTP	Network Time Protocol.
OAIS	Open Archival Information System: è lo standard ISO 14721:2003 e definisce concetti, modelli e funzionalità inerenti agli archivi digitali e gli aspetti di digital preservation.
PACCHETTO INFORMATIVO	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni

	documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
PORTABLE DOCUMENT FORMAT	<p>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.</p> <p>PDF è uno standard aperto; recentemente la versione PDF/A (PDF Reference Version 1.4) è stata riconosciuta dall'International Organization for Standardization (ISO) con la norma ISO 19005:2005.</p>
PRESA IN CARICO	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
PRODUTTORE	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
PA	Pubblica Amministrazione.
PEC	Posta Elettronica Certificata.
PU	Pubblico Ufficiale.
RAPPORTO DI VERSAMENTO	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
REST	Representational State Transfer.
RESPONSABILE DELLA CONSERVAZIONE	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 del DPCM del 3 dicembre 2013.
RIFERIMENTO TEMPORALE	Evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art. 1, lettera m del DPCM 22 febbraio 2013).
SaaS	Software as a Service.
SCARTO	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e/o di interesse storico culturale.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Nell'ambito della Pubblica Amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati

	è il sistema che consente la tenuta di un documento informatico.
STATICITA'	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.
TSA	Time Stamping Authority.
TSS	Time Stamping Service.
TU	Testo Unico.
URL	Universal Resource Locator.
UTC	Universal Coordinated Time
UTENTE	Persona fisica, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO AGLI ARCHIVI DI STATO	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata.

NORMATIVA DI RIFERIMENTO

L'Archivio è il complesso dei documenti (analogici e digitali) prodotti o comunque acquisiti da un ente durante lo svolgimento della propria attività. I documenti che compongono l'archivio sono pertanto collegati tra loro da un nesso logico e necessario detto 'vincolo archivistico' e sono suddivisibili in tre 'fasi di vita':

3

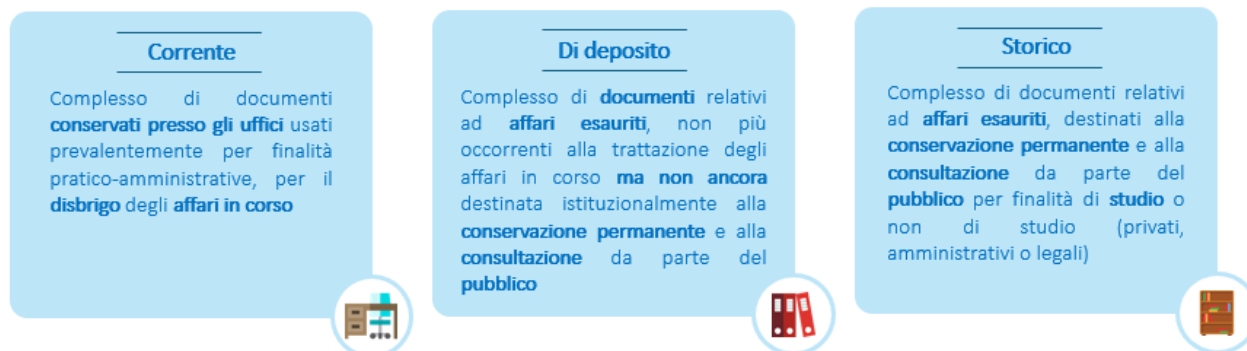


FIGURA 1 FASI D'ARCHIVIO

La fase corrente è oggi in parte sostituita dall'archiviazione digitale, cioè la memorizzazione di un documento su un Sistema Documentale, Protocollo informatico, CD, server, Repository. È un processo per sua natura 'statico', non normato e soggetto a obsolescenza nel tempo.

La fase di deposito è oggi in parte sostituita dalla conservazione digitale, servizio normato e accreditato, in cui il documento mantiene intatto nel tempo il suo valore legale e le caratteristiche di integrità, immutabilità, leggibilità e autenticità che un giudice valuta in sede di contenzioso.

Di seguito l'elenco dei principali riferimenti normativi italiani in materia:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e ss.mm.ii. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss.mm.ii – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai



sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;

- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri del 3 aprile 2013 n. 55, linee guida per la gestione dei processi di fatturazione elettronica verso la Pubblica Amministrazione.
- Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- eIDAS (electronic IDentification Authentication and Signature) EU Regulation 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market.
- GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Linee guida sulla formazione, gestione e conservazione di documenti digitali.

In ambito specificatamente sanitario:

- Decreto del Presidente del Consiglio dei Ministri del 14 novembre 2015 - prescrizioni farmaceutiche in formato digitale.
- Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015, n. 178 Regolamento in materia di fascicolo sanitario elettronico.
- 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.
- Decreto - legge n. 78/2010 - Dematerializzazione della ricetta medica cartacea.
- Autorità Garante della Privacy, Linee guida in tema di referti on-line – 19/11/2009.

RUOLI E RESPONSABILITÀ

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

4

Al Responsabile della Conservazione sono attribuiti compiti di seguito elencati, riguardanti le funzioni, gli adempimenti, le attività e le responsabilità. Il Responsabile della Conservazione è tenuto a gestire il processo in coerenza con quanto stabilito dalla normativa in vigore.

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

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

- 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.

Ente	I.O.V. Istituto Oncologico Veneto - IRCCS
Sede Amministrativa	Via Gattamelata, 64 - 35128 Padova
Recapiti	049 821 1111
Sito web	https://www.ioveneto.it/
C.F. - Partita IVA	04074560287
Ruolo	Direttore Generale/ legale rappresentante <i>pro tempore</i>

Il Responsabile interno della conservazione designato contestualmente all'approvazione e all'adozione della deliberazione del presente Manuale è di seguito individuato:

Nome e Cognome	Andrea Longo
Ruolo	Dirigente UOS Sistemi Informativi
Data inizio incarico	Deliberazione di Adozione del Manuale di conservazione
Data termine incarico	Fino a diversa determinazione

L'ISTITUTO, avvalendosi della facoltà prevista dall'art. 5, comma 1, b) del DPCM 03/12/2013 ha affidato il servizio di conservazione a InfoCert S.p.A, la quale riveste il ruolo di **Responsabile esterno del servizio di conservazione ed** esegue i compiti definiti nel DPCM 03.12.2013 e garantisce lo svolgimento delle attività suddette.

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 Via Carlo Bo, 11, 20143 Milano • Via Marco e Marcelliano, 45, 00147 Roma <p>Tel: +39 06836691</p>
Sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
Codice Fiscale / Partita IVA	07945211006
Numero REA	RM – 1064345
Data inizio incarico	23.09.2019
Data termine incarico	

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

agid.gov.it (sezione Conservatori Accreditati)

infocert.it (sezione Conservazione)

Più concretamente si rimanda per i capitoli dedicati a:

- Struttura organizzativa e Ruoli di responsabilità del Conservatore
- Dettaglio tecnico del sistema di conservazione e trattazione dei pacchetti di archiviazione
- Monitoraggio e controlli del Conservatore.

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.

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

Per "**pacchetto di versamento**" si intende l'insieme di documenti che il Soggetto Produttore invia al sistema di conservazione in un'unica sessione.

Per "**pacchetto di archiviazione**" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center del Conservatore. Ad ogni documento il Sistema di conservazione associa un file XLM, detto Indice del Pacchetto di Archiviazione.

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 dall'ISTITUTO tramite interfaccia disponibile, che porta all'esibizione del documento conservato.

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.

PROCESSI DI FORMAZIONE E GESTIONE PER TIPOLOGIA DOCUMENTALE

Si rimanda al **Manuale di Gestione del Protocollo informatico, dei flussi documentali e degli Archivi** per la descrizione funzionale ed operativa del sistema di gestione informatica dei documenti adottato dall'ISTITUTO, con particolare riferimento alle fasi di creazione, ricezione e smistamento.

Nella seguente tabella sono riportate le principali fasi di processo per ciascuna tipologia documentale.

Tipologia documentale	Processo di formazione, versamento ed esibizione	Data di decorrenza (comprensiva del pregresso)
Documentazione clinica Ambiente AO Padova (B139)	<p>La documentazione clinica viene creata attraverso gli applicativi software in uso presso l'Istituto Oncologico Veneto-IRCCS, firmata digitalmente, e raccolta all'interno dell'applicativo Galileo e successivamente viene versata in conservazione attraverso il connettore LegalCare</p> <p>Questa tipologia documentale è in parte conservata nella precedente versione di LegalDoc.</p>	2015

Documentazione clinica non raccolta in Galileo	La documentazione clinica prodotta attraverso gli applicativi aziendali in uso presso l'Istituto Oncologico Veneto-IRCCS e <u>non</u> raccolta all'interno di Galileo può essere versata in conservazione sostitutiva attraverso il caricamento manuale da LegalDocWEB dal personale medico e sanitario dello IOV.	
Contratti e convenzioni	I contratti e le convenzioni stipulati in forma digitale e firmati digitalmente dal Provveditorato e dagli Affari Generali vengono versati in conservazione attraverso il caricamento manuale da LegalDoc WEB.	2020
Registri delle attività di trattamento GDPR	Il Registro delle attività di trattamento e gli altri Registri connessi alla protezione dei dati personali vengono periodicamente versati in conservazione attraverso il caricamento manuale da LegalDoc WEB.	2021
Libri e registri contabili (inventario, mastro, giornale, cespiti)	I registri sono creati, gestiti e firmati digitalmente dall'UOS Bilancio e Contabilità. Periodicamente (entro tre mesi dalla rispettiva dichiarazione dei redditi) vengono versati in conservazione attraverso il caricamento manuale da LegalDoc WEB.	2020
Documento protocollato	Il documento protocollato viene versato in conservazione sostitutiva in maniera automatica	2021
Registro giornaliero di protocollo	Il Registro giornaliero di protocollo viene versato in conservazione sostitutiva in maniera automatica	2021
Fatture elettroniche attive	Le fatture elettroniche attive sono versate automaticamente in conservazione sostitutiva	2021
Fatture elettroniche passive	Le fatture elettroniche passive sono versate automaticamente in conservazione sostitutiva	2021
Mandati di pagamento e reversali	I mandati di pagamento e i reversali sono versate in conservazione sostitutiva attraverso il caricamento automatico	2021

DESCRIZIONE DEL SERVIZIO

6 Il servizio LegalDoc di InfoCert è fruibile con modalità **automatica**, attraverso connettore LegalCare (descritto in seguito), oppure **manualmente**, attraverso il portale LegalDoc WEB, utilizzabile sia per il versamento manuale di singoli documenti non ricompresi nei processi automatici, sia per la ricerca e l'esibizione di tutti i documenti conservati.

Il servizio è erogato in modalità SaaS (Software as a Service) 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.

Principali funzionalità:

- **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 dall' ISTITUTO e ne estende i servizi con funzionalità di archivio di deposito 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 ISTITUTO sceglie di conservare.

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.

RESPONSABILITÀ

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

Attività	ISTITUTO	LegalCare	LegalDoc	Responsabile del servizio della Conservazione di InfoCert
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	V	R - E		
5. Verifica e accettazione del documento e produzione del rapporto di versamento			E - V	
6. Sottoscrizione del rapporto di versamento			E	R - V* - A
7. Marca temporale del rapporto di versamento			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.

CONFIGURAZIONE DEI SISTEMI

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

ID bucket: B149

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

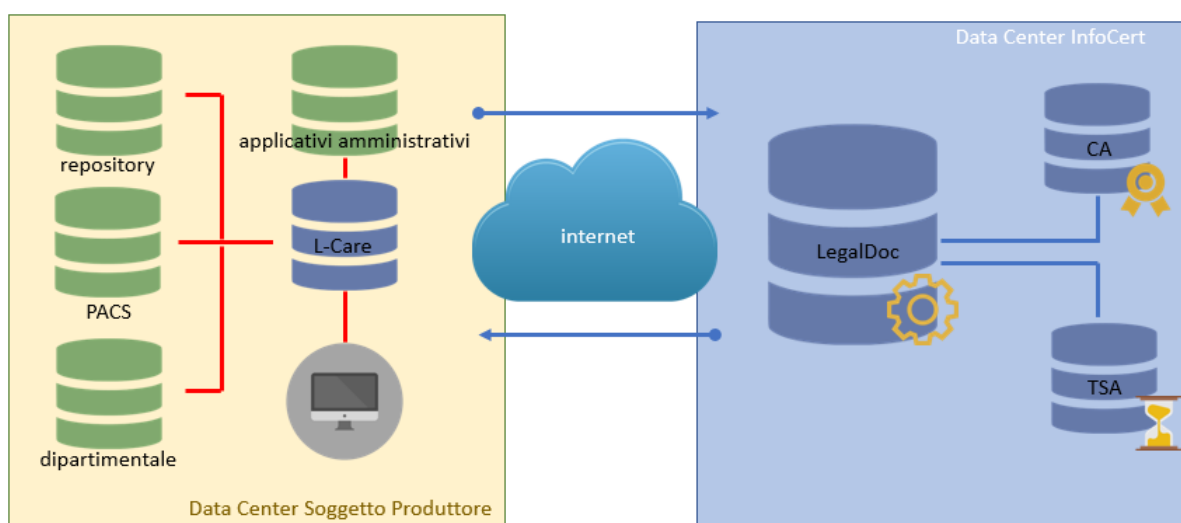


FIGURA 2 INFRASTRUTTURA TECNOLOGICA LEGALCARE

LEGALCARE

La componente locale L-Care si configura come il punto di consolidamento prima delle operazioni di conservazione a norma in ISTITUTO. 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'ISTITUTO.

Il sistema di conservazione LegalDoc è configurato per accettare solo documenti in formati prestabiliti e concordati con il cliente. 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'ISTITUTO tramite la consolle di amministrazione, accessibile mediante autenticazione.

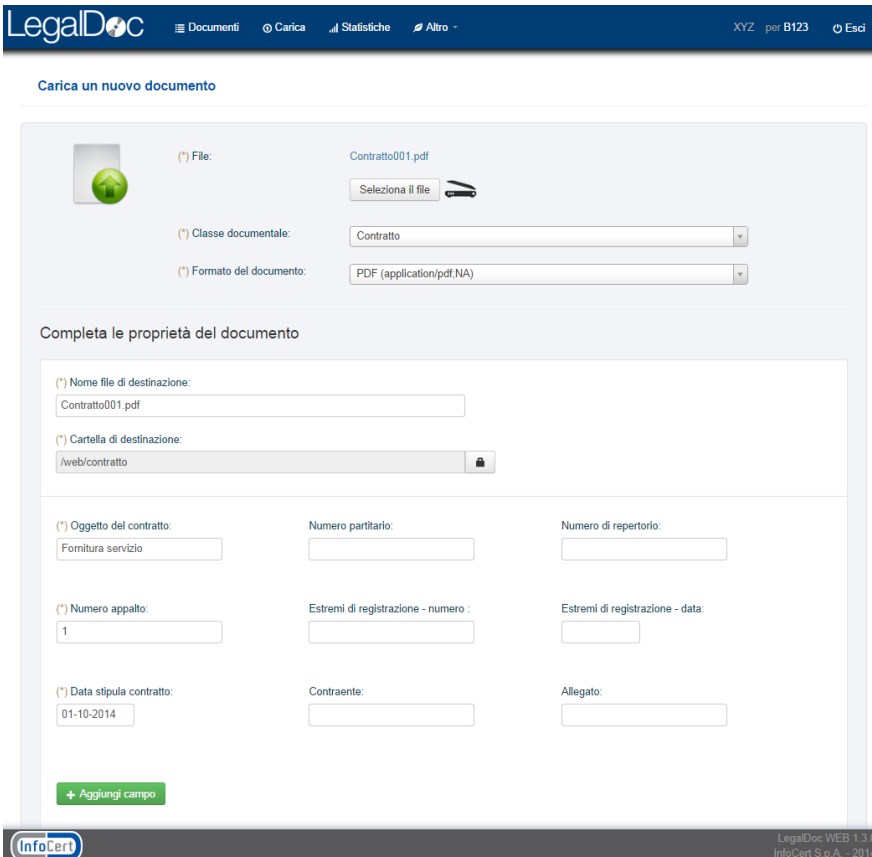
LEGALDOC WEB

Alcune tipologie documentali sono versate in **conservazione manualmente**, attraverso l'interfaccia di LegalDoc WEB.

Il portale è accessibile dall'URL <https://conservazioneasl.infocert.it/ui/> con apposite credenziali qui di seguito riportate:

UTENZA	NOME E COGNOME	INDIRIZZO MAIL	TIPOLOGIA DOCUMENTALE
NR9ND101 NR9ND102		ufficio.bilancio@iov.veneto.it	Libri e Registri contabili
NR9ND113 NR9ND114		privacy@iov.veneto.it	Registro e Consensi GDPR
NR9ND103 NR9ND104 NR9ND105 NR9ND106 NR9ND107 NR9ND108		amministrazione.ricerca@iov.veneto.it ufficioacquisti@iov.veneto.it	Contratti
NR9ND111 NR9ND112		idmo@iov.veneto.it	Referti

L'attività di caricamento prevede la scelta della tipologia documentale e la compilazione manuale dei metadati di riferimento.



LegalDocDoc Documenti Carica Statistiche Altro - XYZ per B123 Esci

Carica un nuovo documento

File: Contratto001.pdf
 Selezione il file

Classe documentale: Contratto

Formato del documento: PDF (application/pdf;NA)

Completa le proprietà del documento

Nome file di destinazione: Contratto001.pdf

Cartella di destinazione: /web/contratto

Oggetto del contratto: Fornitura servizio
 Numero partitario:
 Numero di repertorio:

Numero appalto: 1
 Estremi di registrazione - numero :
 Estremi di registrazione - data:

Data stipula contratto: 01-10-2014
 Contraente:
 Allegato:

+ Aggiungi campo

InfoCert LegalDoc WEB 1.3.0
 InfoCert S.p.A. - 2014

FIGURA 3 INTERFACCIA LEGALDOC WEB PER IL CARICAMENTO

MARCA TEMPORALE DEI 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.

FIRMA DIGITALE CON DISPOSITIVO HSM DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, il Responsabile del servizio della Conservazione di InfoCert appone la propria firma digitale su ogni pacchetto di archiviazione, mediante un sistema di firma automatica erogato dalla CA InfoCert, che si avvale di un dispositivo crittografico ad alte prestazioni HSM.

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 esterno del servizio della Conservazione per ogni indice di

conservazione su ogni file attesta la conservazione stessa.

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 controlli automatici, che richiedono l'intervento del Responsabile esterno del servizio della Conservazione solo al verificarsi di eventuali eventi anomali non gestibili in modo automatico. L'apposita procedura, detta "verificatore", esegue test di leggibilità binaria mediante il continuo calcolo delle impronte dei documenti conservati, con successivo confronto con l'hash del documento contenuto nel file delle direttive della conservazione versato: se la procedura non registra differenze tra i due hash, il documento è inalterato rispetto a quanto versato dall'ISTITUTO. In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile esterno del servizio della Conservazione e i suoi Responsabili incaricati sono dotati di apposita Console, con la quale procedono manualmente e periodicamente ad una verifica campionaria di leggibilità dell'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.

Tutti i controlli sono verbalizzati.

ANALISI DEGLI ERRORI

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

- Formato dichiarato del documento da conservare (in coerenza con i 'Dati Tecnici di attivazione' e con la configurazione degli ambienti);
- Correttezza della struttura del file di Parametri (contenente le informazioni per la leggibilità nel tempo del documento da conservare);
- Correttezza della struttura del file di Indici (contenente i metadati del documento da conservare, alcuni dei quali obbligatori, in coerenza con i 'Dati Tecnici di attivazione');
- Presenza in conservazione sul medesimo path di un documento con lo stesso nome-file del documento da conservare;
- Abilitazione Utenza all'attività di versamento in quel dato ambiente (l'associazione tra utenza -username e password- e singola persona fisica è in capo all'ISTITUTO).
- Validità sessione in uso (di default della durata di un'ora tra login e logout);
- Dimensione massima del documento da conservare (di default 256 megabyte, variabile su richiesta);
- Validità del certificato qualificato di firma digitale con cui è sottoscritto il documento da conservare.

Se i pacchetti non superano i controlli, viene segnalato l'errore di versamento nell'apposita BrokerConsole.

Periodicamente tramite BrokerConsole il servizio Sistemi Informativi dell'ISTITUTO verifica i pacchetti di versamento contrassegnati come 'ERRORE' e, in base al tipo di errore e alla tipologia di documento viene coinvolto di volta in volta il relativo responsabile (o delegato).

Analisti Statistiche Esibizione PA Sistema Utenti									
Lista Documenti in errore									
SHA-1	Codice Documento	Dipartimentale	Errore	Data Firma	Data Arrivo	Stato	Nome	Valore	
<input type="checkbox"/>	f91f0d423a2f4c100e32656f1386b5...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 13:49	20/01/2015 9:2	In verifica	codute		
<input type="checkbox"/>	2c2a59ca6c5c42eda1a32859acc23...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 15:46	20/01/2015 9:2	In verifica	couite_variazione		
<input checked="" type="checkbox"/>	629aa03708392a062c32c63dea39...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 13:16	20/01/2015 9:2	In verifica	asl_comune_nascita		
<input type="checkbox"/>	2177a8cbaf06b91b2db0e192efaa8...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 13:25	20/01/2015 9:2	In verifica	doc_revisione		
<input type="checkbox"/>	65b37a888385f409fe20928deb162...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 15:0	20/01/2015 9:2	In verifica	ref_datafirma	19/01/2015 13:16:10	
<input type="checkbox"/>	a4afe82d72e3af3e2b916c70755cb...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 13:41	20/01/2015 9:2	In verifica	ref_tipo	6	
<input type="checkbox"/>	b68f217d1c444d27c776afa922c54...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 17:37	20/01/2015 9:2	In verifica	token		
<input type="checkbox"/>	29d263784795aadcb4b24d2b2c1b...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 11:27	20/01/2015 9:2	In verifica	ts	20/01/2015 09:02:22	
<input type="checkbox"/>	1b61af5c938aa80361d5d3946ec3...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 14:44	20/01/2015 9:2	In verifica	tsconserve		
<input type="checkbox"/>	fcdf29ee70a9f7c656be11e4f89b1c...	PRO	ERRORE: Certificato di CA non trovato	19/01/2015 17:32	20/01/2015 9:2	In verifica	reqid		

Page 1 of 859

Reset Visualizza Scarica Crea Report ReSubmit Conserva Cancella Verifica Documenti in hold Mostra Ignore Marca Ignore

Displaying 1 - 50 of 42926

FIGURA 4 ESEMPIO SEGNALAZIONE ERRORE DI VERSAMENTO

PROCEDURE DI RICERCA ED ESIBIZIONE IN LEGALDOC WEB

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, utilizzando il token o i metadati compilati in fase di versamento.

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.

Attraverso l'esibizione a norma diventa possibile:

- estrarre un documento e visualizzarlo a video;
- produrre copia cartacea o su altro supporto informatico del documento;
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione;
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione;
- verificare l'integrità del documento
- prendere visione dei file a corredo che qualificano il processo di conservazione attestandone il corretto svolgimento:
 - L'Indice di Conservazione UNI SINCR0, 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 (contente i metadati del documento conservato)
 - File di dati (documento conservato)
 - Attestazione di corretta conservazione.

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.

LegalDoc WEB è un portale accessibile dall'URL <https://conservazioneasl.infocert.it/ui/> e così configurato:

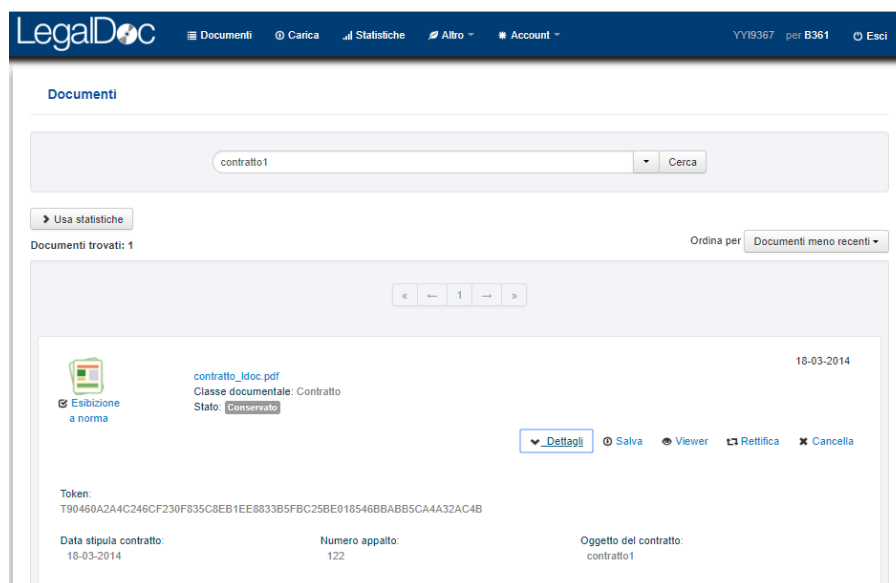


FIGURA 5 INTERFACCIA LEGALDOC WEB

La pagina “Documenti” consente di visualizzare i documenti conservati in LegalDoc e i metadati ad essi associati, di verificarne il processo di conservazione, di rettificarli e di scaricarne i visualizzatori necessari.

La pagina della visualizzazione dei documenti è composta di una barra per la ricerca comprensiva di un bottone per la ricerca avanzata, di un corpo centrale contenente i risultati della ricerca e di una spalla sinistra che permette di raffinare i risultati della ricerca mostrando alcuni.

Digitando il tasto “Cerca” il testo inserito nella barra viene cercato in tutti i metadati del documento (quali il token, il nome del documento, la classe documentale, gli indici indicati in fase di conservazione, etc.). I risultati vengono indicati sotto alla barra nel corpo centrale della pagina.

È inoltre possibile accedere alla ricerca “dettagliata”:

LegalDoc Documenti Carica Statistiche Altro Account YYI9367 per B361 Esci

Classe documentale:

Data stipula contratto:
Da: A:

Allegato:
 Qualsiasi Vero Falso

Contraente:

 Ricerca esatta

Estremi di registrazione - data:
Da: A:

Estremi di registrazione - numero :
Da: A:

Numero appalto:
Da: A:

Numero partitario:
Da: A:

Numero di repertorio:
Da: A:

Oggetto del contratto:

 Ricerca esatta

Codice fiscale:


 Ricerca esatta


FIGURA 6 RICERCA DETTAGLIATA LEGALDOC WEB

✔ Il documento è conservato correttamente




L'indice di conservazione (IDC UnISincro) è stato firmato digitalmente dal Responsabile del Servizio di Conservazione **Nicola Macca'** (codice fiscale **TINIT-MCCNCL72A22LB40M**) e marcato temporalmente in data **06-12-2018 08:34:16 (UTC)**

[▼ Dettagli](#) [📄 Salva](#)

	Firmatario	Nicola Macca'
	Ente certificatore	InfoCert Firma Qualificata 2
	Codice fiscale	TINIT-MCCNCL72A22LB40M
	Nome comune	Nicola Macca'
	Stato	IT
	Organizzazione	INFOCERT SPA
	Codice Identificativo	07945211006
	Certificato valido dal	18-06-2018 12:30:06 (UTC)
	Certificato valido al	18-06-2021 00:00:00 (UTC)
	Esito	✔ La firma è valida

	Ente certificatore	InfoCert Time Stamping Authority 2
	Marca temporale del	06-12-2018 08:34:16 (UTC)
	S/N	07945211006
	Esito	✔ La marcatura temporale è valida

L'indice di conservazione contiene i riferimenti ai seguenti file:

	Tipo: file dei parametri Nome: conserve.xml Mime-Type: text/xml;1.0	▼ Dettagli 📄 Salva
	Tipo: file di indici Nome: index.xml Mime-Type: text/xml;1.0	▼ Dettagli 📄 Salva
	Tipo: file dati Nome: report_B23058_1544085255766.pdf Mime-Type: application/pdf;NA	▼ Dettagli 📄 Salva 👁 Viewer

[📄 Scarica Attestato di Conservazione](#)

FIGURA 7 ESIBITORE LEGALDOC (PACCHETTO DI DISTRIBUZIONE)

Sono abilitati all'accesso e esibizione tramite LEGALDOC WEB i responsabili della conservazione e relativi responsabili.

PROCEDURE DI RICERCA ED ESIBIZIONE NELLA BROKERCONSOLE 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:

<http://10.1.2.168/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'IOV 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.

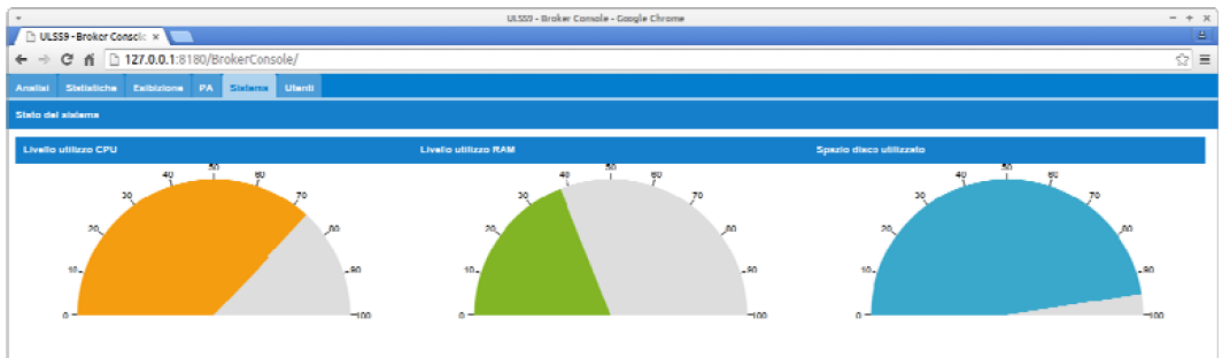


FIGURA 8 – VISIBILITÀ GRAFICA DELLO STATO DEL SISTEMA CON BROKERCONSOLE

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

PROCEDURA DI ESIBIZIONE LEGALCARE: DETTAGLIO

RICERCA DEL DOCUMENTO DA ESIBIRE

INPUT	<i>Lista di documenti</i>	
IOV	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'IOV 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 care	L-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 care	L-	5.1 Download del documento e memorizzazione dello stesso in locale
OUTPUT	<i>Documento salvato</i>	

SICUREZZA E PROTEZIONE DEI DATI

CED ISTITUTO

L'ISTITUTO si è dotata di un Regolamento interno per l'utilizzo degli strumenti informatici con deliberazione 839 del 28 dicembre 2018.

7 INFOCERT

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 di accesso. 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.

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.

La sede di Disaster Recovery è a Modena.

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.



NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI, AI SENSI DEL REGOLAMENTO UE N. 679/2016

Ai sensi dell'art. 6, DPCM 3.12.2013, InfoCert, quale soggetto esterno cui l'ISTITUTO ha affidato il servizio di conservazione, assume il ruolo di Responsabile del trattamento dei dati personali.

Il trattamento dei dati è effettuato:

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

In particolare, sono affidate le seguenti operazioni di trattamento, da effettuarsi con l'ausilio di strumenti elettronici e negli specifici limiti previsti dal DPCM e dal Contratto: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, selezione, estrazione, interconnessione, comunicazione, cancellazione e (eventuale) distruzione di dati.

POLICY PRIVACY BY DESIGN E BY DEFAULT

InfoCert ha aggiornato le proprie linee guida relative al trattamento sicuro delle informazioni, integrandole e adeguandole ai requisiti dettati dal GDPR, per le attività di progettazione e per le attività di sviluppo. L'applicazione di tali linee guida è parte integrante dei processi di progettazione e sviluppo di qualsiasi prodotto/servizio e sono tenute costantemente aggiornate affinché restino adeguate alle evoluzioni tecnologiche inerenti i servizi erogati.

Inoltre, tutte le richieste di dati formulate dai servizi InfoCert sono configurate per acquisire il set minimo indispensabile per l'erogazione del servizio e/o per il rispetto della normativa vigente nel caso di servizi normati.

Tutte le tempistiche, le tipologie di dati e la loro quantità sono definibili dall'ISTITUTO tramite Scheda Dati Tecnici di Attivazione del servizio di conservazione.

InfoCert si è dotata di apposita Procedura di scarto, hand-over e termination plan, tesa a minimizzare il più possibile il trattamento dei dati quantitativamente e qualitativamente.

Il servizio permette la cancellazione della documentazione conservata a due livelli: una, logica, sotto il controllo dell'ISTITUTO, l'altra, più profonda, allo scadere del retention period stabilito in fase di attivazione del servizio e/o su richiesta, tramite apposita procedura di scarto e previo nullaosta della Soprintendenza archivistica di competenza. L'hardware in dismissione viene trattato con tecniche elettroniche di alienazione, smantellamento, sovrascrittura profonda del disco.

L'accesso alla ricerca e all'esibizione dei documenti conservati avviene sulla base di credenziali concordate con l'ISTITUTO, protette da password (modificabile al primo accesso) e configurate con delle specifiche regole che consentono l'accesso solo ad alcune tipologie documentali, sulla base di quanto richiesto in fase di attivazione.

Tutte le comunicazioni avvengono tramite protocollo sicuro HTTPS e in fase di conservazione InfoCert adotta tecniche crittografiche di cifratura con algoritmo AES 256.

DOCUMENTAZIONE RICHIAMATA E AGLI ATTI

Elenco dei documenti contrattuali a cui il Manuale si riferisce:

8

1. Condizioni Generali di Contratto – Regola il rapporto tra InfoCert e l'ISTITUTO;
2. Atto di affidamento del procedimento di conservazione sostitutiva – formalizza l'affidamento ad InfoCert del processo di conservazione, delineandone l'ambito di applicazione;
3. Scheda Dati Tecnici di attivazione – descrive tipologie documentali, formati, metadati e utenze richieste;
4. File di Configurazione dell'ambiente di conservazione;
5. Manuale utente esibitore.