

Manuale della conservazione documentale digitale

I.F.O.

Istituti Fisioterapici Ospitalieri



SOMMARIO

1	SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO	4
2	GLOSSARIO.....	5
3	PREMESSA ARCHIVISTICA	11
4	NORMATIVA DI RIFERIMENTO	13
5	RUOLI E RESPONSABILITÀ	16
6	OGGETTI SOTTOPOSTI ALLA CONSERVAZIONE	19
	PROCESSI DI FORMAZIONE E GESTIONE PER TIPOLOGIA DOCUMENTALE	19
7	DESCRIZIONE DEL SERVIZIO	27
	RESPONSABILITÀ	28
	CONFIGURAZIONE DEI SISTEMI	29
	LEGALCARE.....	29
	FIRMA DIGITALE CON DISPOSITIVO HSM DEI PACCHETTI DI ARCHIVIAZIONE.....	31
	MARCA TEMPORALE DEI PACCHETTI DI ARCHIVIAZIONE	31
	SUPPORTI DI CONSERVAZIONE.....	31
	CONTROLLI DI PROCESSO	31
	ANALISI DEGLI ERRORI	31
	PROCEDURE DI RICERCA ED ESIBIZIONE NELLA BROKERCONSOLE LEGALCARE	32
	PROCEDURA DI ESIBIZIONE LEGALCARE: DETTAGLIO	35
	RICERCA DEL DOCUMENTO DA ESIBIRE	35
	INVIO DELLA RICHIESTA A LEGALDOC	35
	RICERCA DEL DOCUMENTO NEL SISTEMA ED ESIBIZIONE.....	35
	VERIFICA DEL DOCUMENTO TRAMITE ESIBITORE.....	36
	DOWNLOAD DEL DOCUMENTO TRAMITE L-CARE	36
	PROCEDURE DI RICERCA ED ESIBIZIONE NELLA PRECEDENTE VERSIONE DI LEGALDOC	36
8	SICUREZZA E PROTEZIONE DEI DATI	37
	CED IFO	37
	INFOCERT	37
	NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI, AI SENSI DEL REGOLAMENTO UE N. 679/2016.....	38
	POLICY PRIVACY BY DESIGN E BY DEFAULT	38
9	DOCUMENTAZIONE RICHIAMATA E AGLI ATTI.....	40

Versione/Release n°	1.0	Data Versione/Release	08/05/2023
Descrizione Modifiche	Aggiornamento normativo Linee guida AgID e descrizione tipologie documentali conservate		
Motivazioni	Prima emissione		

1 SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO

Il presente documento è il Manuale della conservazione degli **Istituti Fisioterapici Ospitalieri (IFO)**, ai sensi delle *Linee guida AgID su formazione, gestione e conservazione dei documenti informatici* (da ora in poi *Linee guida AgID*) in vigore dal 1 gennaio 2022, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 e del Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014.

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

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

2 GLOSSARIO

TERMINE	DEFINIZIONE
ACCESSO	Operazione che consente di prendere visione dei documenti informatici.
AFFIDABILITÀ	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
AGGREGAZIONE DOCUMENTALE INFORMATICA	Insieme di documenti informatici o insieme 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.
ARCHIVIO	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
AREA ORGANIZZATIVA OMOGENEA	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
ATTESTAZIONE DI CONFORMITÀ DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITÀ	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
CERTIFICAZIONE	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
CLASSIFICAZIONE	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
CLOUD DELLA PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
CODEC	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un <i>wrapper</i> (codifica), così come di estrarli da esso (decodifica).
CONSERVATORE	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
CONSERVAZIONE	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le

	caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
CONVENZIONI DI DENOMINAZIONE DEL FILE	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
COORDINATORE DELLA GESTIONE DOCUMENTALE	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
DESTINATARIO	Soggetto o sistema al quale il documento informatico è indirizzato.
DIGEST	Vedi Impronta crittografica.
DOCUMENTO AMMINISTRATIVO INFORMATICO	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
DOCUMENTO ELETTRONICO	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
DOCUMENTO INFORMATICO	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
DUPLICATO INFORMATICO	Vedi art. 1, comma 1, lett) i quinquies del CAD.
ESEAL	Vedi sigillo elettronico.
ESIBIZIONE	operazione che consente di visualizzare un documento conservato
ESIGNATURE	Vedi firma elettronica.
ESTRATTO DI DOCUMENTO INFORMATICO	Parte del documento tratto dal documento originale
ESTRATTO PER RIASSUNTO DI DOCUMENTO INFORMATICO	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
ESTRAZIONE STATICA DEI DATI	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
EVIDENZA INFORMATICA	Sequenza finita di <i>bit</i> che può essere elaborata da una procedura informatica.
FASCICOLO INFORMATICO	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
FILE	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
FILE CONTAINER	Vedi Formato contenitore.
FILE WRAPPER	Vedi Formato contenitore.
FILE-MANIFESTO	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
FILESYSTEM	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
FIRMA ELETTRONICA	Vedi articolo 3 del Regolamento eIDAS.
FIRMA ELETTRONICA AVANZATA	Vedi articoli 3 e 26 del Regolamento eIDAS.
FIRMA ELETTRONICA QUALIFICATA	Vedi articolo 3 del Regolamento eIDAS.
FLUSSO (BINARIO)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
FORMATO CONTENITORE	Formato di file progettato per consentire l'inclusione ("imbustamento" o <i>wrapping</i>), in uno stesso file, di una o più evidenze informatiche

	soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
FORMATO DEL DOCUMENTO INFORMATICO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
FORMATO "DEPRECATO"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
FUNZIONI AGGIUNTIVE DEL PROTOCOLLO INFORMATICO	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
FUNZIONI MINIME DEL PROTOCOLLO INFORMATICO	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
FUNZIONE DI HASH CRITTOGRAFICA	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o <i>digest</i> (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
GESTIONE DOCUMENTALE	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
HASH	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o " <i>digest</i> " (vedi).
IDENTIFICATIVO UNIVOCO	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
IMPRONTA CRITTOGRAFICA	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di <i>hash</i> crittografica a un'evidenza informatica.
INTEGRITÀ	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
INTEROPERABILITÀ	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
LEGGIBILITÀ	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
MANUALE DI CONSERVAZIONE	Documento informatico che descrive il sistema di conservazione e 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.
MANUALE DI GESTIONE	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

METADATI	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
NAMING CONVENTION	Vedi Convenzioni di denominazione
OGGETTO DI CONSERVAZIONE	Oggetto digitale versato in un sistema di conservazione.
OGGETTO DIGITALE	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
PACCHETTO DI ARCHIVIAZIONE	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
PACCHETTO DI DISTRIBUZIONE	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
PACCHETTO DI FILE (FILE PACKAGE)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
PACCHETTO DI VERSAMENTO	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
PACCHETTO INFORMATIVO	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
PATH	Percorso (<i>vedi</i>).
PATHNAME	Concatenazione ordinata del percorso di un file e del suo nome.
PERCORSO	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
PIANO DELLA SICUREZZA DEL SISTEMA DI CONSERVAZIONE	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
PIANO DELLA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
PIANO DI CLASSIFICAZIONE (TITOLARIO)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
PIANO DI CONSERVAZIONE	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
PIANO DI ORGANIZZAZIONE DELLE AGGREGAZIONI DOCUMENTALI	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
PIANO GENERALE DELLA SICUREZZA	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.

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 e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
PROCESSO	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
PRODUTTORE DEI PDV	Persona fisica, 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 il responsabile della gestione documentale.
QSEAL	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
QSIGNATURE	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
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.
REGISTRO DI PROTOCOLLO	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
REGISTRO PARTICOLARE	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
REGOLAMENTO EIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
REPERTORIO	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
RESPONSABILE DEI SISTEMI INFORMATIVI PER LA CONSERVAZIONE	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLA CONSERVAZIONE	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLA GESTIONE DOCUMENTALE	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.
RESPONSABILE DELLA PROTEZIONE DEI DATI	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
RESPONSABILE DELLA SICUREZZA DEI SISTEMI DI CONSERVAZIONE	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID

RESPONSABILE DELLO SVILUPPO E DELLA MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RIFERIMENTO TEMPORALE	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
RIVERSAMENTO	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
SCARTO	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
SERIE	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
SIDECAR (FILE)	File-manifesto (<i>vedi</i>).
SIGILLO ELETTRONICO	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
SISTEMA DI CONSERVAZIONE	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
TIMELINE	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di <i>timeline</i> un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
TITOLARE DELL'OGGETTO DI CONSERVAZIONE	Soggetto produttore degli oggetti di conservazione.
TRASFERIMENTO	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
UFFICIO	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
UTENTE ABILITATO	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce 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.

3 PREMESSA ARCHIVISTICA

L'Archivio è il complesso dei documenti (analogici e digitali) prodotti o comunque acquisiti da un ente, una persona, una famiglia, 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 per la disciplina archivistica l'unitarietà dell'archivio è garantita dalla sua gestione operativa in tre 'fasi di vita':



FIGURA 1 FASI D'ARCHIVIO

La fase corrente è oggi prevalentemente condotta mediante archiviazione digitale, cioè la memorizzazione di un documento su un Sistema di Gestione Documentale (nel quale possono confluire, ad esempio, le registrazioni effettuate negli applicativi di gestione della contabilità o nel sistema di protocollo informatico, ove presente) principalmente su server/repository o su altri supporti di memorizzazione. È l'archivio che è attualmente in uso ed è in continuo accrescimento. È un processo soggetto a obsolescenza nel tempo.

La fase di deposito vede la presenza di documenti ancora utili per finalità amministrative o giuridiche (ad esempio per accertamenti fiscali), ma non più indispensabili per il disbrigo degli affari in corso. Si tratta della fase intermedia del ciclo di vita degli archivi, tra quella dell'archivio corrente e quella dell'archivio storico. È una fase dinamica e prevede che gli insiemi di documenti archivistici conservati possano essere trasferiti all'archivio storico oppure destinati alla distruzione/scarto (se non più giuridicamente attivi). È la fase di decantazione della documentazione archivistica, dove viene svolta una funzione di intermediazione prima di destinare la documentazione alla conservazione permanente. È in questa fase che vengono identificate le aggregazioni documentali che definiscono la struttura dell'archivio e che vengono configurati i criteri che guideranno la selezione ai fini di scarto o conservazione permanente.

Nelle *Linee guida AgID* viene sottolineato che il processo conservativo può essere avviato sia precocemente a partire dall'archivio corrente, che nella fase di archivio di deposito: in quest'ultimo caso riguarderebbe aggregazioni informatiche (fascicoli e serie archivistiche). In considerazione dei rischi dovuti all'obsolescenza tecnologica, viene previsto che il soggetto produttore dell'archivio possa "sulla base di specifiche esigenze" trasferire al sistema di conservazione anche i documenti relativi a fascicoli e serie ancora aperte, ribadendo quanto previsto dall'art. 44 comma 1 bis del CAD.

Il servizio di conservazione digitale a norma, di cui questo Manuale descrive il processo, risponde invece prevalentemente all'esigenza di assicurare l'efficacia probatoria dei documenti informatici, soprattutto quelli sottoscritti con firma digitale, in modo da estenderne l'efficacia oltre il periodo di validità tecnologica: è un servizio normato e qualificato, finalizzato al mantenimento nel tempo delle caratteristiche di integrità, immodificabilità, leggibilità e autenticità del documento, che può essere oggetto di esibizione a norma per permettere al giudice di valutarne il valore legale in sede di contenzioso.

Secondo il modello delle tre fasi di vita dell'archivio previsto dalla normativa italiana, si distinguono quindi le finalità di una conservazione a norma destinata principalmente a proteggere l'integrità e l'efficacia probatoria dei documenti e le finalità che devono guidare la conservazione illimitata a fini storici e di ricerca (archivio storico), dove prevale la dimensione storico-culturale della documentazione sebbene esse possa ancora essere utile a fini pratici.

Nella fase di archivio storico andranno previste soluzioni tecnologiche compatibili con i tempi, le responsabilità, le condizioni di qualità e completezza dei servizi di fruizione indispensabili per la conservazione permanente. L'archivio, durante il suo ciclo di vita, ha quindi sia un valore pratico-giuridico, che un valore storico-culturale: nella fase iniziale, prevale il primo valore che, man mano, si ridimensiona lasciando posto alla preminente dimensione storico-culturale; in molti casi però, anche dopo molti anni, la valenza giuridica dell'archivio e la sua utilità pratica non scompaiono del tutto.

È importante in ogni caso porre attenzione al profilo conservativo fin dal momento della formazione della documentazione, al fine di garantirne la tenuta all'interno del sistema di gestione informatica dei documenti e dell'eventuale conservazione a lungo termine all'interno di sistemi dedicati.

4 NORMATIVA DI RIFERIMENTO

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

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e ss.mm.ii. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss.mm.ii – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) – Codice dell'amministrazione digitale (CAD) e ss.mm.ii.;
- 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 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 [parzialmente abrogate dalle Linee Guida AgID a partire da gennaio 2022];
- 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;
- 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 AgID sulla formazione, gestione e conservazione dei documenti informatici*, pubblicate a settembre 2020, aggiornate nel maggio 2021 e pienamente applicabili dal 1° gennaio 2022.

- Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici di dicembre 2021 (MarketPlace), composto di due allegati tecnici, emanato secondo quanto previsto dall'articolo 34, comma 1-bis del decreto legislativo n. 82/2005, come integrato e modificato dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020 e entrato in vigore il 1° gennaio 2022.

In ambito specificatamente sanitario:

- Decreto MEF 4 agosto 2017 - Modalità tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE) di cui all'art. 12, comma 15-ter del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.
- 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.
- *Linee guida per la dematerializzazione in diagnostica per immagini* (Intesa Conferenza Stato Regioni 81 2012 del 4 aprile 2012)
- 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.

Si riportano di seguito gli standard di riferimento:

- UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- ISO/TR 18492 - Long-term preservation of electronic document-based information;
- ISO 20652 - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard;
- ISO 20104 - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS);
- ISO/CD TR 26102 - Requirements for long-term preservation of electronic records;
- Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de données pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018;
- METS - Metadata Encoding and Transmission Standard;
- PREMIS – PREservation Metadata: Implementation Strategies;

- EAD (3)/ISAD (G);
- EAC (CPF)/ISAAR (CPF)
- ISO 16363 - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories;
- ISO/IEC 27001 - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ETSI TS 101 533-1 V1.2.1 - Technical Specification, Electronic Signatures and Infrastructures; (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.2.1 - Technical Report, Electronic Signatures and Infrastructures; (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

5 RUOLI E RESPONSABILITÀ

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

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

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

Più in particolare, ai sensi del par. 4.5 delle *Linee guida AgID*, il responsabile della conservazione:

- a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c) genera e sottoscrive 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) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- 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) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;
- 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 le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali;
- m) predispone il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Ente	Istituti Fisioterapici Ospitalieri (IFO)
Sede Amministrativa	Via Chianesi 53 - 00144 Roma
Recapiti	Centralino +39 06 52661 PEC: aagg@cert.ifo.it
Sito web	ifo.it
C.F. - Partita IVA	01033011006

a garanzia del corretto svolgimento delle attività interne nomina:

Nome e Cognome	Umberto Santi
Ruolo	Posizione Organizzativa
Data inizio incarico	28 febbraio 2023
Data termine incarico	Decorrenza incarico

Istituti Fisioterapici Ospitalieri (IFO), avvalendosi della facoltà prevista dal par. 4.5 *delle Linee guida AgID* di delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti che abbiano specifiche competenze ed esperienze, ha affidato in full-outsourcing al conservatore esterno **InfoCert S.p.A.** parte delle attività suddette, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing dalle PA.

Denominazione sociale	InfoCert S.p.A.
Sede Legale:	<ul style="list-style-type: none"> • 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 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
Data inizio incarico	28/05/2014
Data termine incarico	Decorrenza incarico

In InfoCert è stato nominato un Responsabile del Servizio della conservazione, che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione.

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

[https://www.infocert.it/ sezione Conservazione > Documentazione](https://www.infocert.it/sezione%20Conservazione%20Documentazione)

Più concretamente si rimanda al Manuale standard di InfoCert per:

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

6 OGGETTI SOTTOPOSTI ALLA CONSERVAZIONE

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

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

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

Per “**pacchetto di archiviazione**” si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center 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 da IFO 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

Le tipologie documentali sanitarie conservate nell’ambiente di conservazione (**ID bucket B318 – Istituti fisioterapici ospitalieri**: data di attivazione 28/05/2014) sono le seguenti:

Tipologie documentali	Codice tipologia
1. REFERTI_ANATOMIA_PATOLOGICA E ISTOPATOLOGIA	referti_anatomia_patologica
2. REFERTI_RADIOLOGIA	referti_radiologia
3. REFERTI_MEDICINA_NUCLEARE	referti_medicina_nucleare
4. REFERTI_PATOLOGIA_CLINICA E MICROBIOLOGIA	referti_patologia_clinica
5. STUDI_DICOM_RADIOLOGIA E MEDICINA_NUCLEARE	studi_dicom_radiologia

La documentazione viene formata attraverso gli applicativi RIS/PACS di pertinenza, firmati digitalmente dal medico refertante e versati in conservazione direttamente dai repository dei corrispondenti sistemi RIS/PACS attraverso il connettore LegalCare.

Il *retention period* per i referti è illimitato, mentre per le immagini diagnostiche è di 10 anni (come da *Linee guida per la dematerializzazione in diagnostica per immagini – 2012*).

Di seguito vengono riportati i dettagli per ogni tipologia documentale conservata:

Tipologia	Referti ANATOMIA PATOLOGICA E ISTOPATOLOGIA (referti_anatomia_patologica)
Data di decorrenza del processo di conservazione	Dal 13/01/2015 fino al 24/07/2015
Modalità di formazione, gestione e versamento in conservazione	I referti di anatomia patologica e Istopatologia (prodotti sia da Istituto Regina Elena che da San Gallicano) sono redatti attraverso applicativo di Engineering – WINSAP, e firmati digitalmente dai medici refertanti in formato PDF. I referti vengono poi archiviati in un unico repository e versati in conservazione tramite connettore LegalCare. La ricerca e l'esibizione a norma avvengono tramite BrokerConsole LegalCare.
Formato	PDF firmato digitalmente (pdf.p7m)
Tempistica di versamento in conservazione	Giornalmente
Tempi di conservazione	Illimitato
Metadati	<ul style="list-style-type: none"> • Data documento • Classe documentale • Codice Fiscale paziente • Cognome Paziente • Nome Paziente • Codice Prestazione • ID Paziente • Data di Nascita paziente • Sesso • Data Presa in Carico • Data Prestazione • ID Ordine • ID Referto • ID Ricovero <p>È sempre possibile l'aggiunta di ulteriori metadati che consentano la ricerca/esibizione nel tempo.</p>

Tipologia	REFERTI E IMMAGINI DI RADIOLOGIA (referti_radiologia)
Data di decorrenza del processo di conservazione	Dal 24/07/2015 – in corso
Modalità di formazione, gestione e versamento in conservazione	I referti (prodotti sia da Istituto Regina Elena che da San Gallicano) sono redatti attraverso applicativo RIS di Agfa – Elephant, firmati digitalmente dai medici refertanti in formato PDF. Le immagini DICOM sono prodotte dal PACS di AGFA Enterprise Imaging. I referti e le immagini vengono poi archiviati in un unico repository e versati in conservazione tramite connettore LegalCare. La ricerca e l'esibizione a norma avvengono tramite BrokerConsole LegalCare.
Formato	PDF firmato digitalmente (pdf.p7m)
Tempistica di versamento in conservazione	Giornalmente
Tempi di conservazione	Illimitato

Metadati

**[allineati alla normativa vigente - ex Allegato 5
Linee guida AgID]**

- Data documento
- Data Presa in Carico
- Data Prestazione
- Classe documentale
- ID Ordine
- ID Paziente
- ID Referto
- ID Ricovero
- Soggetto 1 (Tipo: PG/Ruolo: soggetto che effettua la registrazione /Denominazione "IRCCS Istituti Fisioterapici Ospitalieri")
- Soggetto 2 (Tipo: PF/Ruolo: autore/**Nome e Cognome medico refertante**)
- Codice Fiscale
- Cognome Paziente
- Nome Paziente
- Data di Nascita
- Sesso
- Tessera Sanitaria
- Codice Prestazione
- Allegati numero
- CDC erogante
- Data di registrazione
- Tipologia di flusso
- Tipo registro
- Numero documento
- Identificativo documento
- Modalità di formazione
- Impronta
- Algoritmo
- Nome file
- Oggetto
- Referto tipo
- Tipo documento
- Riservato
- Study instance UID
- Formato file
- Versione
- Sostituisce

È sempre possibile l'aggiunta di ulteriori metadati che consentano la ricerca/esibizione nel tempo.

Tipologia	REFERTI E IMMAGINI DI MEDICINA NUCLEARE (referti_medicina_nucleare)
Data di decorrenza del processo di conservazione	Dal 24/07/2015 – fino al 06/06/2018
Modalità di formazione, gestione e versamento in conservazione	<p>I referti sono redatti attraverso applicativo Elefante, firmati digitalmente dai medici refertanti in formato PDF. Le immagini sono prodotte dal PACS di AGFA Enterprise Imaging. Referti e immagini vengono poi archiviati in un unico repository e versati in conservazione tramite connettore L-Care.</p> <p>La ricerca e l'esibizione a norma avvengono tramite BrokerConsole LegalCare.</p>
Formato	PDF firmato digitalmente (pdf.p7m)
Tempistica di versamento in conservazione	Giornalmente
Tempi di conservazione	Illimitato
Metadati	<ul style="list-style-type: none"> • Data documento • Classe documentale • Codice Fiscale • Codice Prestazione • Cognome Paziente • Nome Paziente • Data di Nascita • Data Presa in Carico • Data Prestazione • ID Ordine • ID Paziente • ID Referto • ID Ricovero • Sesso • Tessera Sanitaria <p>È sempre possibile l'aggiunta di ulteriori metadati che consentano la ricerca/esibizione nel tempo.</p>

Tipologia	Referti PATOLOGIA CLINICA - MICROBIOLOGIA (referti_patologia_clinica)
Data di decorrenza del processo di conservazione	Dal 17/03/2016 fino al 07/06/2016 Attualmente in Regione Lazio
Modalità di formazione, gestione e versamento in conservazione	I referti sono redatti attraverso applicativo della società Dedalus THEMIS, firmati digitalmente dai biologi e medici refertanti in formato PDF. I referti vengono poi archiviati in un unico repository e versati in conservazione tramite connettore L-Care. La ricerca e l'esibizione a norma avvengono tramite BrokerConsole LegalCare.
Formato	PDF firmato digitalmente (pdf.p7m)
Tempistica di versamento in conservazione	Giornalmente
Tempi di conservazione	Illimitato
Metadati	<ul style="list-style-type: none"> • Data documento • Classe Documentale • Codice Fiscale paziente • Cognome Paziente • Nome Paziente • Data di Nascita paziente • Data Presa in Carico • Codice prestazione • Data Prestazione • ID Ordine • ID Paziente • ID Referto • ID Ricovero • Sesso <p>È sempre possibile l'aggiunta di ulteriori metadati che consentano la ricerca/esibizione nel tempo.</p>

Tipologia	STUDI DICOM RADIOLOGIA (studi_dicom_radiologia)
Data di decorrenza del processo di conservazione	Dal 11/03/2015 – in corso
Modalità di formazione, gestione e versamento in conservazione	I referti sono prodotti attraverso l'applicativo Elefante di Agfa e le immagini DICOM sono prodotte dal PACS di AGFA: Enterprise Imaging. Entrambi vengono archiviati in un unico repository e versate in conservazione tramite connettore L-Care. La ricerca e l'esibizione a norma avvengono tramite BrokerConsole LegalCare.
Formato	PDF firmato digitalmente (pdf.p7m) e Immagini DICOM (ZIP)
Tempistica di versamento	Giornalmente
Tempi di conservazione in conservazione	10 anni

Metadati

**[allineati alla normativa vigente - ex Allegato 5
Linee guida AgID]**

- Data documento
- Accession Number
- Modalities in study
- Study description
- Data-Ora Esame
- Data Prestazione
- Classe documentale
- ID Ordine
- ID Paziente
- ID Referto
- ID Ricovero
- Soggetto 1 (Tipo: PG/Ruolo: soggetto che effettua la registrazione /Denominazione "IRCCS Istituti Fisioterapici Ospitalieri")
- Soggetto 2 (Tipo: PF/Ruolo: destinatario/**Nome e Cognome del paziente**)
- Allegati numero
- CDC erogante
- Data di registrazione
- Tipologia di flusso
- Tipo registro
- Numero documento
- Identificativo documento
- Modalità di formazione
- Impronta
- Algoritmo
- Nome file
- Oggetto
- Referto tipo
- Tipo documento
- Riservato
- Sostituisce
- Study instance UID
- Formato file
- Original size
- Versione

È sempre possibile l'aggiunta di ulteriori metadati che consentano la ricerca/esibizione nel tempo.

Per maggiori informazioni sulla configurazione dell'ambiente di conservazione e il dettaglio dei metadati (e relative obbligatorietà) per singola tipologia documentale si consulti il *File di configurazione* in allegato.

7 DESCRIZIONE DEL SERVIZIO

Il servizio LegalDoc di InfoCert è fruibile con modalità automatica, attraverso connettore LegalCare (descritto in seguito), 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 da IFO 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 IFO 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	IFO	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 IFO, che si occupa del recupero dei documenti dai sistemi nativi e monitorizza i flussi documentali verso la componente remota (LegalDoc, in IFO) 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: B318

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

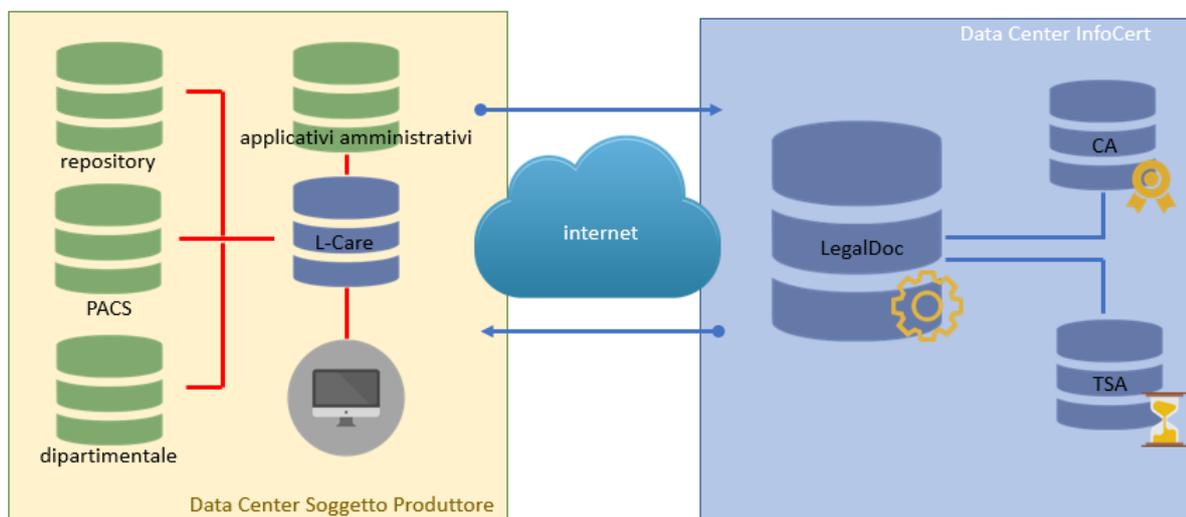


FIGURA 2 INFRASTRUTTURA TECNOLOGICA LEGALCARE

LEGALCARE

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

Il sistema di conservazione LegalDoc è configurato per accettare solo documenti in formati prestabiliti e concordate 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 a IFO tramite la **Broker Console**, accessibile mediante autenticazione.

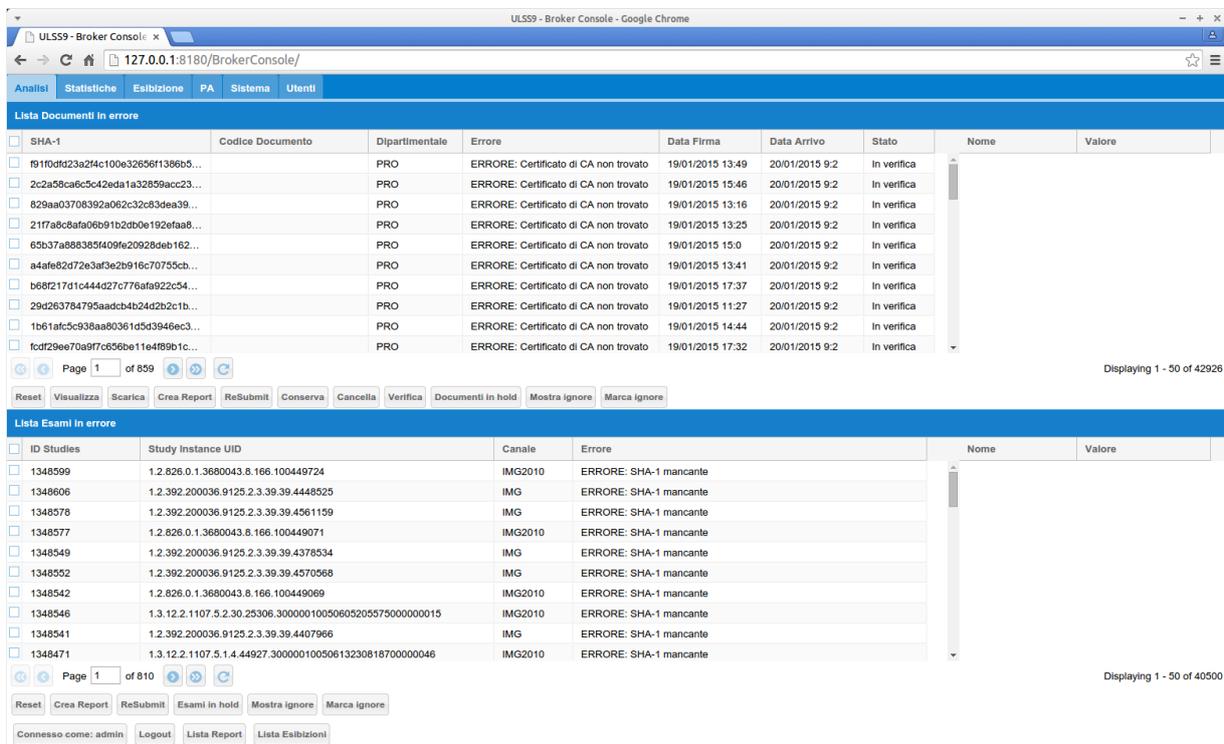


FIGURA 3 INTERFACCIA BROKER CONSOLE LEGALCARE

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 altre prestazioni HSM.

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.RI.M di Torino (Istituto Nazionale di Ricerca Metrologica, già Elettrotecnico Nazionale "Galileo Ferraris") ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

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.

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 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 da IFO. In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile 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 (utenza applicativa).
- 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 di versamento non superano i controlli, viene segnalato l'errore di versamento nell'apposita BrokerConsole e mediante **mail di notifica giornaliera** al referente IFO.

Analsi Statistiche Esibizione PA Sistema Utenti									
Lista Documenti in errore									
<input type="checkbox"/>	SHA-1	Codice Documento	Dipartimentale	Errore	Data Firma	Data Arrivo	Stato	Nome	Valore
<input type="checkbox"/>	f91f0df23a2f4c100e32656f1386b5...		PRO	ERRORE: Certificato di CA non trovato	19/01/2015 13:49	20/01/2015 9:2	In verifica	codute	
<input type="checkbox"/>	2c2a58ca6c5c42eda1a32859acc23...		PRO	ERRORE: Certificato di CA non trovato	19/01/2015 15:46	20/01/2015 9:2	In verifica	couta_variazione	
<input checked="" type="checkbox"/>	829aa03708392a062c32c83dea39...		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"/>	21f7a8c8afaf06b91b2db0e192efaa8...		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"/>	1b61afc5c938aa80361d5d394fec3...		PRO	ERRORE: Certificato di CA non trovato	19/01/2015 14:44	20/01/2015 9:2	In verifica	tsconserva	
<input type="checkbox"/>	fdcd29ee70a9f7c656be11e4f89b1c...		PRO	ERRORE: Certificato di CA non trovato	19/01/2015 17:32	20/01/2015 9:2	In verifica	reqid	

Page 1 of 89

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 NELLA BROKERCONSOLE LEGALCARE

La Broker Console 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 Broker Console 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, Crome.....), 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 da IFO in fase di attivazione del servizio.

La Broker Console 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.

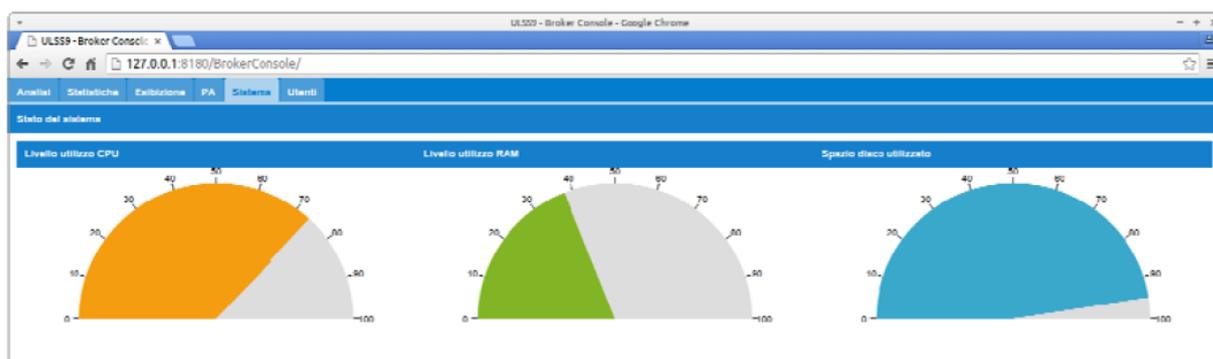


FIGURA 5 – VISIBILITÀ GRAFICA DELLO STATO DEL SISTEMA CON BROKERCONSOLE

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.

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 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 (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.

✔ 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	18-05-2018 12:30:05 (UTC)
	Certificato valido al	18-05-2021 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)
	SIN	07945211006
	Esito	✔ La marcatura temporale è valida

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

✔  Tipo: [file dei parametri](#)
Nome: conserva.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 6 ESIBITORE LEGALDOC (PACCHETTO DI DISTRIBUZIONE)

PROCEDURA DI ESIBIZIONE LEGALCARE: DETTAGLIO

RICERCA DEL DOCUMENTO DA ESIBIRE

INPUT	<i>Lista di documenti</i>	
IFO	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>	

PROCEDURE DI RICERCA ED ESIBIZIONE NELLA PRECEDENTE VERSIONE DI LEGALDOC

Il 1 gennaio 2022 sono entrate pienamente in vigore le Linee guida AgID (che abrogano il precedente DPCM del 3 dicembre 2013, recante le nuove Regole Tecniche in materia di Conservazione).

IFO ha conservato i propri documenti dal 2013 al febbraio 2017 in un sistema di conservazione e da febbraio 2017 in poi nel nuovo sistema di conservazione, entrambi sviluppati e gestiti da InfoCert.

La ricerca e l'esibizione sia sul nuovo che sul vecchio sistema avvengono mediante la BrokerConsole e LegalDoc WEB, come descritto precedentemente, e senza nessuna differenza tra i due sistemi.

8 SICUREZZA E PROTEZIONE DEI DATI

CED IFO

IFO si è dotata di un Disciplinare per l'utilizzo delle apparecchiature e degli strumenti informatici che definisce le regole e le condizioni per l'utilizzo degli strumenti informatici dell'Azienda da parte dei dipendenti e di tutti i soggetti esterni in possesso di un opportuno titolo autorizzativo (stagisti, prestatori di servizi, etc.) che possono accedere a strumenti informatici dell'Azienda.

Il Disciplinare implementa un insieme codificato di disposizioni, di carattere obbligatorio, finalizzato ad attuare un sistema generalizzato di sicurezza ICT, attraverso il ricorso a protocolli e metodologie standard e l'adozione di idonee misure organizzative, tecnologiche ed operative volte a prevenire il rischio di utilizzi impropri delle strumentazioni e a tutelare le informazioni gestite nel sistema informativo aziendale.

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 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.

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 del par.4.5 delle Linee guida AgID, InfoCert, quale soggetto esterno cui IFO 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 dei dati, da effettuarsi con l'ausilio di strumenti elettronici e negli specifici limiti previsti 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 da IFO 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 di IFO, 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, smagnetizzazione, sovrascrittura profonda del disco.

L'accesso alla ricerca e all'esibizione dei documenti conservati avviene sulla base di credenziali concordate con IFO, 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.

9 DOCUMENTAZIONE RICHIAMATA E AGLI ATTI

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

1. Condizioni Generali di Contratto – Regola il rapporto tra InfoCert e IFO;
2. Atto di affidamento del procedimento di conservazione – formalizza l'affidamento ad InfoCert del processo di conservazione, delineandone l'ambito di applicazione;
3. Scheda Dati Tecnici di attivazione – per la formulazione della richiesta di tipologie documentali, formati, metadati e utenze;
4. File di Configurazione dell'ambiente di conservazione (bucket ID B318) – riepiloga la configurazione dell'ambiente di conservazione dedicato;
5. Manuale utente Broker Console LegalCare.
6. Verbale di incident 2024 v.1