MANUALE dei PROCESSI per la CONSERVAZIONE DIGITALE A NORMA

(Allegato del Manuale della Conservazione di InfoCert)

Master Training srl Reg. Imp. di RE - P.I. e C.F. 01932770355
Sede legale: Via Timolini 18 – 42015 Correggio (RE)
Sede operativa: Via San Martino, 11 – 42015 Correggio (RE) – Tel: 0522-268059 Fax: 0522-331673
www.mastertraining.it - e-mail info@mastertraining.it

INDICE

1 Introduzione al documento 4
1.1 Gestione versioni documento 4
1.2 Scopo e campo di applicazione del documento 4
1.3 Principi di redazione 5
1.4 Termini e definizioni 5
1.5 Acronimi 10
2 Normativa e standard di riferimento 11
2.1 Normativa di riferimento 11
2.2 Standard di riferimento 12
3 Nomine e individuazione dei compiti 13
3.1 Cliente/Soggetto Produttore: 13
3.2 Referenti di processo 13
3.3 Responsabile della Conservazione 13
3.4 InfoCert SPA 14
4 La conservazione dei documenti 15
4.1 Il Responsabile della Conservazione 15
5 Il sistema di creazione e gestione dei documenti 17
5.1 Controlli 17
5.2 Servizi di sottoscrizione 17
5.3 Indicizzazione dei documenti (metadati) 17
5.4 Gestione delle anomalie 17
5.5 Formato dei documenti elettronici 18
6 Il sistema di conservazione documentale 19
6.1 Descrizione generale del servizio 19
6.2 Definizione di documento 19
6.3 Configurazione dei sistemi 20
6.3.1 Modalità di erogazione 20
6.4 Componenti 20
6.4.1 Marca temporale 20
6.4.2 Firma digitale con dispositivo HSM 21
6.4.3 Supporti di conservazione 21
6.5 Controlli 21
6.5.1 Controlli di processo 21
6.5.2 Controlli periodici 21
6.5.3 Ispezione del sistema da parte delle autorità competenti 22
6.5.4 Incident management 22
7 Le tipologie documentali 23
DDT 23
Libri contabili 23
Fatture PA 23
Contratti 23
Registri di protocollo 23
Documenti Protocollati 23
Documenti didattici 24
7.2 Fasi del processo per i versamenti da MasterCom 2 24
8 Il processo di conservazione 26
8.1 Processi di front-end 26

8.2 Processi di back-end 26
8.3 Tabella di Responsabilità 27
8.5 Fasi del processo di conservazione: dettaglio 27
Formazione del documento 27
Indicizzazione e archiviazione 29
Acquisizione documento e creazione del file delle direttive 29
Verifica, accettazione e invio della ricevuta di accettazione del documento 29
Creazione del file di controllo 30
Memorizzazione, creazione copia di sicurezza e chiusura della conservazione 30
9 Procedure di ricerca ed esibizione 32
9.2 Procedura di esibizione: dettaglio 32
Ricerca del documento da esibire 32
Invio della richiesta a LegalDoc 32
Ricerca del documento nel sistema ed esibizione 33
Verifica del documento 33
Verifica del documento 33
9.3 Requisiti software 34
10 Modifica dei documenti posti in conservazione 35
11 Misure di sicurezza 36
11.1 Scuola xyz 36
11.2 InfoCert 36
11.2.1 Sicurezza fisica 36
11.2.2 Gruppi di continuità 36
11.2.3 Connessione a Internet 36
11.2.4 Sicurezza delle reti: protezione da intrusioni 37
12 Note conclusive 38
12.1 Protezione dei dati personali 38
13 Allegati 39
13.1 Documentazione contrattuale di riferimento 39

1 INTRODUZIONE AL DOCUMENTO

1.1 Gestione versioni documento

Versione:	01	Data Versione:	agosto 2016
Descrizione modifiche:	Nessuna		

1.2 Scopo e campo di applicazione del documento

Il presente documento è il Manuale dei processi documentali per la conservazione di InfoCert S.p.A., ai sensi del DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 pubblicato in GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20) e del Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014.

Come richiesto dal DPCM del 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 della Conservazione, integrato con il presente Manuale dei processi documentali per la conservazione, permette un agevole svolgimento di tutte le attività di controllo.

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

https://www.infocert.it/

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

Il Manuale è organizzato per sezioni:

1. la prima sezione (capitoli 1-4) fornisce il profilo della Scuola, il profilo di InfoCert e dettaglia la configurazione dei sistemi utilizzati per l'erogazione;
2. la seconda sezione (capitoli 5-10) descrive il servizio LegalDoc, il Responsabile del servizio della conservazione, descrive i macro-flussi operativi definiti per la gestione della documentazione elettronica. Inoltre, è dettagliato il procedimento di conservazione posto sotto la responsabilità di InfoCert in virtù della delega allo svolgimento delle attività di competenza del Responsabile del servizio della Conservazione, sottolineando input, output e responsabilità di ogni fase. Infine, vengono descritti i controlli effettuati e i processi di ricerca e esibizione a norma dei documenti conservati.
3. la terza sezione (capitoli 11-13) riporta le misure fisiche e logiche di sicurezza adottate, i riferimenti alla normativa e alla policy sulla protezione dei dati personali e gli allegati al Manuale.

1.3 Principi di redazione

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

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

1.4 Termini e definizioni

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.
AGGREGAZIONE DOCUMENTALE INFORMATICA	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
ARCHIVIAZIONE	è il processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.
AGID	Agenzia per l'Italia Digitale
ARCHIVIO	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un Soggetto Produttore durante lo svolgimento dell'attività.
ARCHIVIO INFORMATICO	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
AREA ORGANIZZATIVA OMOGENEA	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.
ASP	Application Service Provider.
ATTESTAZIONE DI CONFORMITA' DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITA'	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.

BASE DATI	collezione di dati registrati e correlati tra loro.
CA	Certification Authority.
CAD	Codice dell'Amministrazione Digitale.
CAS	Content Addressed Storage.
CERTIFICATORE ACCREDITATO	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
CICLO DI GESTIONE	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
CLASSIFICAZIONE	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici parametri.
CODICE (DELL'AMMINISTRAZIONE DIGITALE)	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
CODICE ESEGUIBILE	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
CONSERVATORE ACCREDITATO	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale.
CONSERVAZIONE	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, descritto nel presente manuale di conservazione e che risponde a quanto stabilito nel DPCM 03/12/2013.
COPIA ANALOGICA DI UN DOCUMENTO INFORMATICO	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
COPIA DI SICUREZZA	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 del DPCM del 3 dicembre 2013.
DOCUMENTO ANALOGICO	Rappresentazione analogica di atti, fatti o dati giuridicamente rilevanti.
DOCUMENTO INFORMATICO	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
DATI SENSIBILI	ai sensi dell'articolo 4, comma 1, lettera d) del Decreto Legislativo 30 giugno 2003, n.196 e la seguente deliberazione del Consiglio dei Ministri del 25 maggio 2012, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
DLGS	Decreto Legislativo.
DPCM	Decreto della Presidenza del Consiglio dei Ministri.
DPR	Decreto del Presidente della Repubblica.
ESIBIZIONE	operazione che consente di visualizzare un documento conservato e di ottenerne copia.

EVIDENZA INFORMATICA	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
EXTENSIBLE MARKUP LANGUAGE	linguaggio derivato dall'SGML (Standard Generalized Markup Language), metalinguaggio che permette di creare altri linguaggi. Mentre l'HTML è un'istanza specifica dell'SGML, XML costituisce a sua volta un metalinguaggio, più semplice dell'SGML, largamente utilizzato per la descrizione di documenti sul Web. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags). Diversamente dall'HTML, l'XML consente all'utente di definire marcatori personalizzati, dandogli il controllo completo sulla struttura di un documento. Si possono definire liberamente anche gli attributi dei singoli marcatori.
FASCICOLO INFORMATICO	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
FIRMA DIGITALE	un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1 comma 1 lettera s) Decreto Legislativo del 7 marzo 2005 n. 82).
FIRMA ELETTRONICA	l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art. 1 comma 1 lettera q) Decreto Legislativo del 7 marzo 2005 n. 82).
FIRMA ELETTRONICA QUALIFICATA	un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1 comma 1 lettera r) Decreto Legislativo del 7 marzo 2005 n. 82).
FIRMA ELETTRONICA AVANZATA	insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1 comma 1 lettera q-bis) Decreto Legislativo del 7 marzo 2005 n. 82). Si vedano anche le regole tecniche, pubblicate nella G.U. il 21 maggio 2013.
FORMATO	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
GU	Gazzetta Ufficiale della Repubblica Italiana.
HSM	Hardware Security Module.
IDENTIFICATIVO UNIVOCO (di seguito detto Token)	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione. Detto anche token LegalDoc.

IMMODIFICABILITA'	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
I.N.RI.M	Istituto Nazionale di Ricerca Metrologica.
INSIEME MINIMO DI METADATI DEL DOCUMENTO INFORMATICO	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM del 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
INTEGRITA'	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
INTEROPERABILITA'	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
LEGALDOC	Servizio di conservazione digitale a norma di InfoCert.
LEGGIBILITA'	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
MARCA TEMPORALE	il riferimento temporale che consente la validazione temporale, così come definita all'art. 1 comma 1 lettera i) DPCM del 30 marzo 2009. La marca temporale è opponibile ai terzi, definita anche nel DPCM 22 febbraio 2013, titolo IV.
MEF	Ministero dell'Economia e delle Finanze.
METADATI	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM del 3 dicembre 2013.
NTP	Network Time Protocol.
OAIS	Open Archival Information System: è lo standard ISO 14721:2003 e definisce concetti, modelli e funzionalità inerenti agli archivi digitali e gli aspetti di digital preservation.
PACCHETTO INFORMATIVO	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
PORTABLE DOCUMENT FORMAT	formato di file creato da Adobe Systems nel 1993 per lo scambio di documenti. Il PDF è un formato a schema fisso basato su un linguaggio di descrizione di pagina che permette di rappresentare documenti in modo indipendente dall'hardware, dal software e dal sistema operativo; ogni PDF incapsula una descrizione completa del documento, che include testo, caratteri, immagini e grafica. PDF è uno standard aperto; recentemente la versione PDF/A (PDF Reference Version 1.4) è stata riconosciuta dall'International Organization for Standardization (ISO) con la norma ISO 19005:2005.
POSTA ELETTRONICA CERTIFICATA	sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici.

PRESA IN CARICO	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
PRODUTTORE	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
PA	Pubblica Amministrazione.
PEC	Posta Elettronica Certificata.
PU	Pubblico Ufficiale.
RAPPORTO DI VERSAMENTO	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore; in LegalDoc è l'insieme degli Indici del Pacchetto di Archiviazione associati ad ogni documento inviato in conservazione in un'unica sessione, che fanno parte del pacchetto di versamento.
REST	Representational State Transfer.
RESPONSABILE DELLA CONSERVAZIONE	il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione ottica conformemente a quanto previsto all'art. 7 del DPCM 03/12/2013.
RIFERIMENTO TEMPORALE	informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici, così come definito all'art. 1 comma 1 lettera m) DPCM del 30 marzo 2009, definito anche nel DPCM 22 febbraio 2013.
SCARTO	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
STATICITA'	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.
UTENTE	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO AGLI ARCHIVI DI STATO	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

1.5 Acronimi

CA	Certification Authority
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione, successivamente DigitPA ora Agenzia per l'Italia Digitale
D. LGS	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
GU	Gazzetta Ufficiale della Repubblica Italiana
HSM	Hardware Security Module
PDF	Portable Document Format
PEC	Posta Elettronica Certificata

SG	Sistema di Gestione
SGD	Sistema di Gestione Documentale
SSL	Secure Socket Layer
TSA	Time Stamping Authority
TSS	Time Stamping Service
TU	Testo Unico
URL	Uniform Resource Locator
XML	Extensible Markup Language

2 NORMATIVA E STANDARD DI RIFERIMENTO

2.1 Normativa di riferimento

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

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, 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 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

2.2 Standard di riferimento

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

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques – Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- ISO 14001:2013 Sistema di Gestione Ambientale;
- UNI EN ISO 20000- 1: 2011 Gestione dei Servizi Informatici;
- UNI EN ISO 9001:2008 Sistemi di gestione per la qualità.

3 NOMINE E INDIVIDUAZIONE DEI COMPITI

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

3.1 Cliente/Soggetto Produttore:

Scuola	I.S.I.S. "Daniele Crespi"
Sede Amministrativa	Via Carducci 4, 21052 – Busto Arsizio (VA)
Recapiti	Tel. 0331633256
Sito web	www.liceocrespi.gov.it
Partita Iva/Codice Fiscale	81009350125

3.2 Referenti di processo

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

Responsabile della conservazione interno	Prof.ssa Cristina Boracchi
Ente/Società	I.S.I.S. "Daniele Crespi" – Busto Arsizio
Data inizio incarico	7 dicembre 2017
Data termine incarico	31/08/2018

3.3 Responsabile della Conservazione

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

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

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

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

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

3.4 InfoCert SPA

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

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

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

InfoCert S.p.A. è un Conservatore accreditato presso l'Agenzia per l'Italia Digitale.

LA CONSERVAZIONE DEI DOCUMENTI

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

Di seguito si richiamano i principali strumenti ed elementi:

- ***Documento informatico***: è una realtà immateriale e il tipo di supporto fisico sul quale esso è registrato è irrilevante per la natura del documento stesso.
  Del documento informatico, a differenza di quello cartaceo, è possibile avere molteplici esemplari, tutti giuridicamente rilevanti e aventi identico valore legale. Per le sue caratteristiche, il documento informatico necessita di strumenti di validazione informatica efficaci e sicuri affinché ne siano garantite, in particolare, l'integrità e l'autenticità. Esemplificando, la gestione di un documento informatico non può prescindere dalla disponibilità di un elaboratore e dei relativi programmi necessari sia per "formare" il documento che per "leggerlo" e verificarne autenticità, integrità e paternità.
- ***Documento analogico***: in generale, è quello che per la sua formazione utilizza una grandezza fisica che assume valori continui come, ad esempio, le tracce continue su carta per il documento cartaceo o le immagini continue per il film. Il supporto fisico su cui si può formare il documento analogico non è necessariamente quello cartaceo, ma può essere film, lastra o pellicola radiologica, microfilm, nastro audio e video. Il documento analogico può essere originale, a sua volta distinto in originale unico e non unico, o copia.
- ***Firma digitale***: è l'elemento principale che interviene nella gestione elettronica del documento informatico dalla formazione, alla trasmissione, fino alla conservazione, poiché conferisce piena validità legale al documento cui è apposta, assicurando autenticità, integrità, non ripudiabilità.
- ***Attestazione temporale***: per stabilire il momento temporale in cui un documento informatico è stato formato è necessario attribuirgli una "validazione temporale", definita come il risultato di una procedura informatica in grado di offrire un riferimento temporale opponibile ai terzi. Lo strumento per ottenere questo risultato è la marca temporale, una particolare firma elettronica che contiene l'ora e la data in cui è stata generata ed è opponibile ai terzi.

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

Per effettuare la riproduzione e la conservazione dei documenti su supporti digitali è necessario rispettare le regole tecniche previste dal Ministero dell'Economia e delle Finanze con il Decreto del 17 giugno 2014, dai Decreti del Presidente del Consiglio dei Ministri del 3 dicembre 2013 e del 13 novembre 2014, ai sensi del Codice dell'Amministrazione Digitale.

4.1 Il Responsabile della Conservazione

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

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

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

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

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;

d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;

e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;

j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

l) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;

m) 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.

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

5 IL SISTEMA DI CREAZIONE E GESTIONE DEI DOCUMENTI

Si rimanda al Manuale di Gestione del Protocollo e degli Archivi (e/o a qualsiasi regolamento interno condiviso sulla gestione documentale) della Scuola, nonché alle funzioni di Segreteria Digitale del software MasterCom2, per la descrizione funzionale ed operativa del sistema di gestione informatica dei documenti adottato da esso, con particolare riferimento alle modalità di utilizzo dello stesso.

5.1 Controlli

Ai sensi di legge, l' I.S.I.S. "Daniele Crespi"assicura che i documenti inviati in conservazione sono statici e non modificabili, ovvero redatti in modo tale per cui il contenuto non possa essere alterabile durante le fasi di conservazione ed accesso ed è immutabile nel tempo.

5.2 Servizi di sottoscrizione

La Scuola ha fornito firme digitali al Dirigente Scolastico prof.ssa Cristina Boracchi e al DSGA Sig, Antonio Colangelo.

Inoltre l'applicativo di Master Training si avvale del servizio di firma automatica di InfoCert, Certification Authority accreditata.

Le Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, del DPCM del 22 febbraio 2013, 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 del Codice dell'Amministrazione Digitale all'art. 5 specificano che se il soggetto appone la sua firma elettronica qualificata o firma digitale per mezzo di una procedura automatica ai sensi dell'art. 35, comma 3 del Codice, deve utilizzare una coppia di chiavi destinata a tale scopo, diversa da tutte le altre in suo possesso.

L'utilizzo di tale procedura deve essere indicato esplicitamente nel certificato qualificato.

Di seguito il dettaglio delle tipologie documentali interessate:

TIPOLOGIA DOCUMENTALE	APPLICATIVO	FIGURA PROFESSIONALE FIRMATARIA	DESCRIZIONE
	MasterCom2		

...

5.3 Indicizzazione dei documenti (metadati)

La Scuola provvede all'indicizzazione dei documenti (metadati) utilizzando le funzioni di gestione documentale previste dalla segreteria digitale MasterCom 2, come da accordi contrattuali. Il dettaglio dei metadati concordati per tipologia documentale è allegato al presente Manuale.

5.4 Gestione delle anomalie

Il sistema di conservazione LegalDoc è configurato per accettare solo documenti in formati prestabiliti. Al venir meno di questa condizione, data l'impossibilità per LegalDoc di accettare il documento, questo viene lasciato in attesa senza immetterlo nel sistema di conservazione e viene segnalata l'anomalia nell'interfaccia della segreteria digitale MasterCom 2.

5.5 *Formato dei documenti elettronici*

Le nuove Regole Tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20) elencano in modo specifico i formati documentali da adottare per la conservazione a lungo termine dei documenti, ovvero le modalità di organizzazione delle informazioni in un codice binario nel loro Allegato 2. Pertanto l' I.S.I.S. "Daniele Crespi" ha deciso l'invio in conservazione soltanto di formati:

- **pdf**
- **xml**
- **txt**
- **tiff**

Tutti eventualmente firmati digitalmente e/o marcati temporalmente.

Qualora in futuro sia necessario conservare documenti in formati diversi da quelli elencati, è necessario che la Scuola sottoscriva l'apposito Addendum al contratto stipulato con InfoCert.

6 IL SISTEMA DI CONSERVAZIONE DOCUMENTALE

6.1 Descrizione generale del servizio

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

LegalDoc consente le funzionalità di:

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

LegalDoc integra il sistema di gestione documentale Master Training in uso dalla Scuola e ne estende i servizi con funzionalità di stoccaggio digitale; il servizio consente di organizzare liberamente le fasi di creazione, utilizzo e archiviazione dei documenti, intervenendo solamente nella fase di conservazione e solamente per i documenti che la Scuola sceglie di conservare.

6.2 Definizione di documento

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

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

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

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

6.3 *Configurazione dei sistemi*

6.3.1 Modalità di erogazione

Il servizio di conservazione LegalDoc è implementato da una applicazione software appositamente sviluppata a tale scopo (applicazione Java in architettura distribuita, ossia costituita da molteplici componenti) e da una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, PEC).

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

Il servizio è accessibile dalla apposita URL di rete https://conservazione.infocert.it; la Scuola richiama i servizi di LegalDoc tramite la segreteria digitale MasterCom2, secondo le modalità indicate da InfoCert nella documentazione contrattuale.

La figura 1 offre uno schema esemplificativo del dialogo tra la segreteria digitale MasterCom2 e LegalDoc, distinguendo le parti che rimangono sotto la responsabilità della Scuola da quelle di competenza di InfoCert.

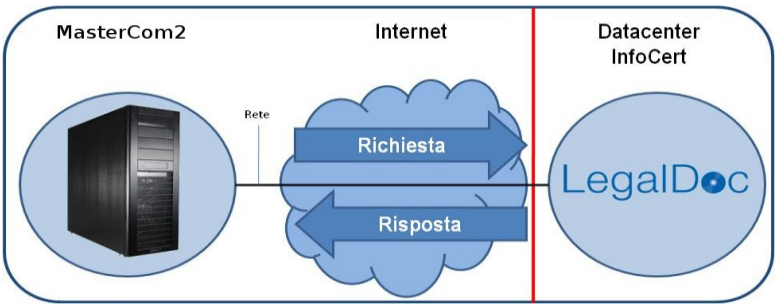

Figura 1 - Dialogo tra MasterCom2 e il sistema di conservazione documentale LegalDoc

6.4 *Componenti*

6.4.1 Marca temporale

Per l'emissione delle marche temporali LegalDoc si avvale del sistema di marcatura di InfoCert, Certification Authority accreditata. La marca temporale viene richiesta al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert.

Il TSS è sincronizzato via radio con l'I.N.RI.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.

6.4.2 Firma digitale con dispositivo HSM

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

6.4.3 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.

6.5 Controlli

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

I controlli effettuati possono essere distinti secondo le seguenti tipologie:

- controlli di processo;
- controlli periodici.

6.5.1 Controlli di processo

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

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

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

6.5.2 Controlli periodici

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

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

6.5.3 Ispezione del sistema da parte delle autorità competenti

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

Qualora dalle attività di ispezione e controllo emergessero punti critici o aree di miglioramento, è impegno di InfoCert l'attivazione delle strutture competenti per la tempestiva analisi della situazione e l'approntamento di tutte le misure necessarie al miglioramento del sistema e/o delle performance.

6.5.4 Incident management

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

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

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

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

7 LE TIPOLOGIE DOCUMENTALI

DDT

Tipologia di documento	DDT emessi e ricevuti
Natura del documento	Originale digitale
Data di decorrenza del processo di conservazione elettronica	01 settembre 2017

Commento [1]: Comprensiva del pregresso

Libri contabili

Tipologia di documento	Libri giornale, mastro, cespiti, inventari
Natura del documento	cartaceo
Data di decorrenza del processo di conservazione elettronica	NO

Commento [2]: Gli obblighi di numerazione progressiva e di vidimazione previsti dalle disposizioni di legge o di regolamento per la tenuta dei libri, repertori e scritture sono assolti, in caso di tenuta con strumenti informatici, mediante apposizione, almeno una volta all'anno, della marcatura temporale e della firma digitale dell'imprenditore o di altro soggetto dal medesimo delegato (art.2215bis CC)

Fatture PA

Tipologia di documento	Fattura elettronica PA passiva con relativa Notifica SdI
Natura del documento	Originale digitale firmato digitalmente
Data di decorrenza del processo di conservazione elettronica	01ottobre 2017

Contratti

Tipologia di documento	Contratti

Natura del documento	Originale digitale firmato digitalmente
Data di decorrenza del processo di conservazione elettronica	02 gennaio 2018

Registri di protocollo

Tipologia di documento	Registri giornalieri di protocollo (DPCM 3 dicembre 2013)
Natura del documento	Originale digitale
Data di decorrenza del processo di conservazione elettronica	02 gennaio 2017

Documenti Protocollati

Tipologia di documento	Documenti in entrata, interni e in uscita
Natura del documento	Originale digitale o copia per immagine di originale analogico
Data di decorrenza del processo di conservazione elettronica	02 gennaio 2018

Documenti didattici

Tipologia di documento	Registri dei voti, Registri di classe, Registri docenti, Verbali dei consigli di classe
Natura del documento	Originale digitale firmato elettronicamente
Data di decorrenza del processo di conservazione elettronica	Data da definire

Di seguito l'analisi dettagliata del processo:

7.2 Fasi del processo per i versamenti da MasterCom 2

Fase / Attività	*Soggetti*	*Afferenza / Applicativi*	*Descrizione*
Redazione	Operatori Scuola	Sistema di gestione documentale della segreteria digitale MasterCom2 (MasterCom, Mail, Upload, Scanner, Fax)	Il documento viene ricevuto o redatto.

Estrazione CONNETTORE web service	Operatori Scuola	Segreteria digitale di MasterCom2	L'operatore incaricato seleziona i documenti da inviare in conservazione attraverso apposita funzione prevista all'interno della segreteria digitale MasterCom2. Il connettore, attraverso chiamate web service, provvede all'invio in conservazione dei documenti selezionati.
Completamento del processo di conservazione	InfoCert	LegalDoc	Il sistema di conservazione LegalDoc eroga il processo di conservazione dei documenti secondo quanto dettagliato al capitolo 7.
Custodia dei supporti	InfoCert	LegalDoc	La custodia dei supporti è demandata ad InfoCert come da accordi contrattuali

8 IL PROCESSO DI CONSERVAZIONE

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

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

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

8.1 Processi di front-end

I processi di front-end sono erogati in modalità sincrona dal sistema LegalDoc, e sono finalizzati a mettere in comunicazione la Scuola con i servizi di LegalDoc e sono richiamati in modalità on-line.

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

- invio di un documento informatico o di un documento analogico opportunamente digitalizzato in conservazione;
- rettifica o cancellazione per via telematica di un documento già conservato in modalità digitale;
- ricerca trasversale sulle classi documentali del documento da esibire;
- esibizione di un documento direttamente dal sistema LegalDoc;
- download del documento conservato con i relativi metadati contenuti nell'Indice di Conservazione;
- visualizzazione delle statistiche di conservazione da interfaccia web.

8.2 Processi di back-end

I processi di back-end sono eseguiti dal sistema LegalDoc in modalità differita e sono i processi che, a partire dai documenti caricati sul sistema LegalDoc dalla Scuola, implementano la conservazione in conformità alle regole tecniche contenute nel DPCM 03/12/2013.

Il processo di conservazione prevede l'elaborazione del singolo documento.

Il documento viene, quindi, corredato da un file di indice, firmato digitalmente dal Responsabile del servizio della Conservazione, contenente informazioni sensibili ai fini della conservazione (indice del documento, impronte dei file che lo costituiscono, classificazione anagrafica dei firmatari). Ogni indice di conservazione di ogni file ha la firma del Responsabile del servizio della Conservazione, a garanzia della sua integrità e immodificabilità.

8.3 Tabella di Responsabilità

Responsabilità Attività	*Scuola*	*Connettore MasterCom2*	*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 Indice di conservazione	**V**	**R - E**		
4. Invio al sistema di conservazione	**R – E**	**R – E**		
5. Verifica e accettazione del documento			**E - V**	
6. Creazione del file di Indice			**E**	**R - V* - A**
7. Attestazione di corretto procedimento			**E**	**R - V* - A**
8. Memorizzazione, creazione "copia di sicurezza" e chiusura del processo			**E**	**R - V* - A**
[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]				

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

8.5 Fasi del processo di conservazione: dettaglio

Formazione del documento

INPUT	*Documento da generare*	
Scuola	1.1	La Scuola genera i documenti statici e non modificabili attraverso le apposite funzioni di estrapolazione dei dati previste in MasterCom e MasterCom2, nonché programmi di elaborazione documenti secondo le procedure previste.
OUTPUT	*Documento generato*	

Indicizzazione e archiviazione

INPUT	*Documento da archiviare*

Scuola	1.1	I documenti vengono corredati da appositi metadati (indicizzazione) attraverso MasterCom2
Scuola	1.2	I documenti vengono inviati in modalità automatica al sistema di conservazione LegalDoc attraverso la Segreteria Digitale MasterCom2 (chiamate web service)
OUTPUT	*Documento indicizzato e archiviato*	

Acquisizione documento e creazione del file delle direttive

INPUT	*File delle direttive da predisporre*	
LegalDoc	2.1	Il sistema LegalDoc acquisisce i documenti informatici caricati e li prepara alla conservazione a lungo termine predisponendo i file XML di indice (Rapporto di versamento).
OUTPUT	*File di indice predisposto*	

Verifica, accettazione e invio della ricevuta di accettazione del documento

INPUT	*Documento da verificare*	
LegalDoc	4.2	Acquisizione del documento
	4.3	Sbustamento del messaggio e verifica della firma elettronica apposta sul file delle direttive di conservazione
	4.4	Presa in carico dei file costituenti il documento
	4.5	Esecuzione di una serie di verifiche sulla completezza e sulla correttezza delle informazioni contenute nel file delle direttive di conservazione
	4.6	Generazione dell'impronta di ogni file del documento
	4.7	Nel caso di esito negativo delle verifiche, il documento viene respinto con l'indicazione che descrive l'errore intercorso. In questo caso il flusso termina.
	4.8	Generazione del file di ricevuta a partire dal file delle direttive
	4.9	Generazione di un identificativo univoco per il documento (token LegalDoc) e firma elettronica sul file di ricevuta

	4.10	Invio a LegalDoc WEB del file di ricevuta di presa in carico della richiesta di conservazione
MasterCom2	4.11	Riceve il file di ricevuta di presa in carico della richiesta di conservazione, ne estrae il token LegalDoc e lo memorizza presso i propri archivi, in associazione con gli indici di ricerca
OUTPUT	*Documento verificato*	

Creazione del file di controllo

INPUT	*Documento da conservare*	
LegalDoc	5.1	Predisposizione del file di controllo del documento contenente l'indice del documento, le impronte dei file che lo costituiscono, la classificazione anagrafica del documento, gli estremi di identificazione del Responsabile del servizio della Conservazione.
	5.2	Apposizione della firma digitale del Responsabile del servizio della Conservazione sul file di controllo e sul file di indice.
OUTPUT	*Documento inserito in conservazione*	

Memorizzazione, creazione copia di sicurezza e chiusura della conservazione

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

9 PROCEDURE DI RICERCA ED ESIBIZIONE

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

L'esibitore è un'applicazione in tecnologia web, che permette ad un utente, precedentemente definito e in possesso delle debite autorizzazioni e credenziali, di accedere al sistema di conservazione LegalDoc da una qualsiasi stazione di lavoro (computer), purché collegata in rete e con disponibilità di un browser web.

Attraverso l'esibizione a norma diventa possibile:

- estrarre un documento e visualizzarlo a video
- produrre copia cartacea o su altro supporto informatico del documento
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione
- prendere visione dei file a corredo che qualificano il processo di conservazione attestandone il corretto svolgimento
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione
- verificare l'integrità del documento.

L'esibizione del documento ottenuto tramite interrogazione al sistema LegalDoc rappresenta un'esibizione completa, legalmente valida ai sensi delle Regole Tecniche del 03/12/2013.

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

9.2 Procedura di esibizione: dettaglio

Ricerca del documento da esibire

INPUT	*Lista di documenti*	
Scuola	1.1	Attraverso MasterCom2 utilizzando gli indici di metadati con cui è stato caricato, ricerca il documento da esibire
OUTPUT	*Token relativo al documento da esibire*	

Invio della richiesta a LegalDoc

INPUT	*Richiesta di esibizione da preparare*	
Master Training	2.1	MasterCom2 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	*Richiesta di esibizione presa in carico da LegalDoc*	

Ricerca del documento nel sistema ed esibizione

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

Verifica del documento

INPUT	*Documento ricevuto dal sistema di conservazione*	
Esibitore	4.1	Visualizzazione del pacchetto di file ed effettuazione di tutte le verifiche
OUTPUT	*Documento esibito*	

Verifica del documento

INPUT	*Documento esibito*	
Scuola	5.1	Download del documento e memorizzazione dello stesso in locale
OUTPUT	*Documento salvato*	

9.3 Requisiti software

Per la visualizzazione del documento ottenuto con la procedura di esibizione da LegalDoc, MasterCom2 utilizza, per ognuno dei file costituenti il documento, il relativo viewer definito da InfoCert per i formati standard o depositato presso il sistema di conservazione per le altre tipologie di file.

10 MODIFICA DEI DOCUMENTI POSTI IN CONSERVAZIONE

In caso di modifica dei documenti già posti in conservazione, la Scuola provvede ad emanare ex novo un documento di rettifica che verrà a sua volta conservato a norma; la riconducibilità del documento modificante a quello modificato è resa possibile grazie agli indici predisposti dalla Scuola in fase di caricamento, che ne assicura la sistematicità e la coerenza. LegalDoc terrà traccia sia del documento rettificante che del documento rettificato, nel rispetto del principio di tracciabilità.

La cancellazione fisica dei documenti conservati, cioè il così detto 'scarto' è espressamente richiesta dalla Scuola, mediante apposita lista debitamente firmata.

Per determinare i tempi di scarto si rimanda al Massimario di selezione e scarto, collegato con il Titolario o Piano di classificazione e alle informazioni contenute nel Manuale di gestione del protocollo e degli archivi adottato della Scuola ai sensi del DPCM del 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.

La Scuola avvierà l'iter di scarto autorizzato presso la Sovraintendenza Archivistica o la Commissione di sorveglianza di riferimento come sancito dal Codice dei Beni Culturali del 2004, articolo 21.

La distruzione degli eventuali supporti ottici rimovibili di back-up è effettuata mediante strumentazione adeguata e seguendo le procedure definite per lo smaltimento dei rifiuti prodotti.

Il Responsabile del servizio della Conservazione mantiene traccia delle richieste di scarto ricevute e correttamente eseguite, con l'indicazione a margine di eventuali errori occorsi durante lo svolgimento del processo, dei rimedi attuati e delle altre informazioni che ritiene meritevoli di annotazione.

11 MISURE DI SICUREZZA

11.1 I.S.I.S. "Daniele Crespi"- Busto Arsizio

Per le misure di sicurezza nel trattamento dei documenti della Scuola si rimanda all'apposito DPS

11.2 InfoCert

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

11.2.1 Sicurezza fisica

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

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

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

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

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

11.2.2 Gruppi di continuità

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

11.2.3 Connessione a Internet

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

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

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

11.2.4 Sicurezza delle reti: protezione da intrusioni

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

Le regole definite sui firewall vengono progettate in base a due principi: in primis il "default deny", ossia quanto non è espressamente permesso è vietato di default ed è, quindi, consentito solo quanto è strettamente necessario al corretto funzionamento dell'applicazione. Il secondo principio consiste nel "defense in depht", 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.

12 NOTE CONCLUSIVE

12.1 Protezione dei dati personali

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

Ai sensi dell'articolo 29 del Codice, la Scuola ha nominato InfoCert SpA Responsabile dei trattamenti dei dati necessari all'esecuzione del servizio (allegato [2]).

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

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

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

13 ALLEGATI

13.1 Documentazione contrattuale di riferimento

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

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

- Richiesta di Registrazione e Certificazione Ufficio di Registrazione di Mastertraining s.r.l (allegato A)
- Richiesta di attivazione con Condizioni Generali di Contratto – Regola il rapporto tra InfoCert e la Scuola; (Allegato B)
- Affidamento del procedimento di conservazione – formalizza l'affidamento ad InfoCert del processo di conservazione, delineandone l'ambito di applicazione; (Allegato C)
- Allegato Tecnico al contratto – descrive le modalità di fornitura del servizio e l'infrastruttura utilizzata per la sua erogazione; (Allegato D)
- Dati Tecnici contrattuali recanti i metadati associati alle tipologie documentali scelte per la Conservazione digitale. (Allegato D)