Manuale di Conservazione

Indice

1 Introduzione

1.1 Scopo e campo di applicazione del documento

Il presente documento è il Manuale della 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.

Il Manuale risponde alla necessità di documentare il processo di conservazione di documenti informatici, effettuato con le modalità di cui al citato DPCM, nonché le procedure di sicurezza e di tracciabilità dei documenti conservati e le procedure da rispettare per l'apposizione del riferimento temporale. La conservazione dei documenti con rilevanza tributaria è effettuata seguendo le ulteriori regole contenute nel Decreto MEF del 17 giugno 2014.

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.

InfoCert eroga il servizio di conservazione in base ad accordi contrattuali che normalmente prevedono forme di servizio limitate nel tempo. Eventuali gestioni, che eccedono i limiti contrattuali, dovranno essere perfezionate con specifici accordi tra le parti.

2 Novità introdotte rispetto alla precedente emissione

Versione/Release n° :	1	***Data Versione/Release :***	luglio 2014
Descrizione Modifiche:	Revisione normativa e di processo		
Motivazioni:	Pubblicazione DPCM del 3 dicembre 2013. Pubblicazione DMEF del 17 giugno 2014. Produzione del Nuovo LegalDoc .		

3 Glossario

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.
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.
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.
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.
CODICE	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.
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.
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.
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.
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.
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.
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.
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.
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.

3.1 Acronimi

AgID	Agenzia per l'Italia Digitale (subentrato a DigitPA dal 2012)
AIPA	Agenzia per l'Informatica nella Pubblica Amministrazione
ASP	Application Service Provider
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005 n. 82 e successive modifiche)
CAS	Content-Addressed Storage
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione (subentrato all'AIPA)
DigitPA	Organismo governativo che dal 2009 al 2012 ha preso il posto del CNIPA
D.LGS	Decreto legislativo
DM	Decreto Ministeriale
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
GU	Gazzetta Ufficiale della Repubblica Italiana
HSM	Hardware Security Module
i.n.ri.m	Istituto Nazionale di Ricerca Metrologica

MEF	Ministero dell'Economia e delle Finanze
NTP	Network Time Protocol
PA	Pubblica Amministrazione
PEC	Posta Elettronica Certificata
PU	Pubblico Ufficiale
REST	Representational State Transfer
SaaS	Service as a Service
TSA	Time Stamping Authority
TSS	Time Stamping Service
TU	Testo Unico
URL	Universal Resource Locator
UTC	Universal Coordinated Time – Tempo Universale Coordinato
WORM	Write Once Read Many
PDF - PDF/A	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. E' stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Nell'attuale versione gestisce varie tipologie di informazioni quali: testo formattato, immagini, grafica vettoriale 2D e 3D, filmati. Un documento PDF può essere firmato digitalmente in modalità nativa attraverso il formato ETSI PAdES. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A (rif. Allegato 2 – DPCM. 3 dicembre 2013).
TIFF	Di questo formato immagine raster, in versione non compressa o compressa senza perdita di informazione. Di questo formato vi sono parecchie versioni, alcune delle quali proprietarie (che ai fini della conservazione nel lungo periodo sarebbe bene evitare). In genere le specifiche sono pubbliche e non soggette ad alcuna forma di limitazione. Questo è un formato utilizzato per la conversione in digitale di documenti cartacei. Il suo impiego va valutato attentamente in funzione del tipo di documento da conservare in considerazione dei livelli di compressione e relativa perdita dei dati. Esistono, infine, alcuni formati ISO basati sulla specifica TIFF 6.0 di Adobe (che è quella "ufficiale" del TIFF). Si tratta del formato ISO 12639, altrimenti noto come TIFF/IT, rivolto particolarmente al mondo del publishing e della stampa e dell'ISO 12234, altrimenti detto TIFF/EP, più orientato alla fotografia digitale.
JPG	Il formato JPEG può comportare una perdita di qualità dell'immagine originale. Anche in questo caso, come nel caso dei TIFF, avendo una grossa diffusione, può essere preso in considerazione, ma il suo impiego, correlato ad un opportuno livello di compressione va valutato attentamente in funzione del tipo di documento da conservare.JPG è il formato più

	utilizzato per la memorizzazione di fotografie ed è quello più comune su World Wide Web. Lo stesso gruppo che ha ideato il JPG ha prodotto il JPEG 2000 con estensione .jp2 (ISO/IEC 15444-1) che può utilizzare la compressione senza perdita di informazione. Il formato JPEG 2000 consente, inoltre, di associare metadati ad un'immagine. Nonostante queste caratteristiche la sua diffusione è tutt'oggi relativa.
XML	Comunemente abbreviato in OOXML, è un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database. Open XML è adottato dalla versione 2007 della suite Office di Microsoft. Lo standard prevede, oltre alle indicazioni fondamentali (strict), alcune norme transitorie (transitional) introdotte per ammettere, anche se solo temporaneamente, alcune funzionalità presenti nelle vecchie versioni del formato e la cui rimozione avrebbe potuto danneggiare gli utenti, facendogli perdere funzionalità. Per quanto riguarda il supporto di Microsoft Office allo standard ISO/IEC 29500:2008: - MS Office 2007 legge e scrive file conformi a ECMA-376 Edition 1. - MS Office 2010 legge e scrive file conformi a ISO/IEC 29500:2008 transitional e legge file conformi a ISO/IEC 29500:2008 strict . Documenti conformi ad ISO/IEC 29500:2008 strict sono supportati da diversi prodotti informatici disponibili sul mercato. Il formato Office Open XML dispone di alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML. I metadati associabili ad un documento che adotta tale formato sono previsti dallo standard ISO 29500:2008.
Open Document Format	ODF (Open Document Format, spesso referenziato con il termine OpenDocument) è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni. Secondo questo formato, un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione. Lo standard ISO/IEC IS 26300:2006 è ampiamente usato come standard documentale nativo, oltre che da OpenOffice.org, da una ampia serie di altri prodotti disponibili sulle principali piattaforme: Windows, Linux. Mac. È stato adottato come standard di riferimento da moltissime organizzazioni governative e da diversi governi ed ha una "penetrazione" di mercato che cresce giorno per giorno.
Formati Messaggi di posta elettronica	Ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, lo standard a cui fare riferimento è RFC 2822/MIME per la gestione degli allegati ci si riferisce ai precedenti formati descritti e approfonditi nell'allegato 2 del DPCM 3 dicembre 2013.

4 Profilo di InfoCert

Denominazione sociale	InfoCert S.p.A.
Sede Legale:	Piazza Sallustio, 9, 00187 Roma Tel.+39 06 836691 Fax +39 06 44285255
Sedi Operative:	Via Franco Russoli 5, 20143 Milano Tel: +39 02 872.867.00
	Corso Stati Uniti 14bis, 35127 Padova Tel. +39 04982881 Fax +39 049 0978406
	Via Marco e Marcelliano 45, 00147 Roma Tel. +39 06 836691 Fax +39 06 44285255
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. si pone sul mercato come un Partner altamente specializzato nei servizi di Certificazione Digitale e Gestione dei documenti in modalità elettronica, in grado di garantire ai propri clienti la piena innovazione nei processi di gestione del patrimonio documentale. InfoCert S.p.A., con un capitale sociale di oltre 17 M€, 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 Posta Elettronica Certificata.

InfoCert progetta e sviluppa soluzioni informatiche ad alto valore tecnologico di dematerializzazione dei processi documentali, attraverso componenti di Gestione Documentale, Conservazione, Firma Digitale e Posta Elettronica Certificata. I clienti vengono accompagnati nella scelta di servizi e soluzioni pienamente rispondenti alle esigenze organizzative, ai vincoli normativi generali e specifici di settore.

Professionisti aggiornati, con esperienza nelle più moderne tecnologie, ed esperti di Project Management, specializzati nella personalizzazione ed implementazione dei processi di gestione digitale dei documenti, consentono ad InfoCert di realizzare progetti e soluzioni complesse di dematerializzazione che conferiscono un vantaggio competitivo a chi li sceglie: piena comprensione delle esigenze del cliente e progettazione di soluzioni personalizzate garantiscono, infatti, al cliente

il raggiungimento di obiettivi di eccellenza, con servizi e soluzioni pienamente rispondenti alle esigenze organizzative e a vincoli normativi generali e specifici di settore.

InfoCert, inoltre, nello svolgimento delle proprie attività, ha conseguito le seguenti certificazioni:

- 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);
- UNI EN ISO 27001:2006 (Sistemi di gestione della sicurezza delle informazioni)

Modello di organizzazione e controllo sulla Responsabilità Amministrativa delle Imprese ai sensi del D.lgs. 231/01.

InfoCert ha adottato il modello di organizzazione e controllo [M231/01] di cui al D.lgs. del 08 giugno 2001 n.231 allo scopo di prevenire i reati per i quali la legge in questione prescrive la responsabilità amministrativa dell'impresa.

Il Modello adottato da InfoCert rappresenta un'ulteriore garanzia dell'azienda in termini rigore, trasparenza e senso di responsabilità nella gestione dei processi interni e nei rapporti con il mondo esterno.

Il modello prevede l'istituzione di un Organismo di Vigilanza, la gestione di un processo formativo/informativo, la adozione di un Codice Etico e la definizione di un Sistema Sanzionatorio.

InfoCert si è dotata di un Integrated Management System per la gestione dei processi e delle responsabilità aziendali. Il documento in allegato [5] "Processo MG115/TB02_Processi e Responsabilità_Integrated Management System" descrive la mappatura dei processi aziendali in termini di:

- Ambito di processo
- Processo
- Procedura
- Struttura Responsabile (owner di processo)

In particolare per quanto riguarda l'ambito di processo si individuano le seguenti aree funzionali:

- Modelli di gestione
- Sistema gestione qualità
- Pianificazione aziendale
- Risorse Umane
- Produzione
- Commerciale
- Progettazione
- Approvvigionamenti
- Produzione ed erogazione

- Controllo e analisi (miglioramento)
- Sistema di gestione sicurezza informatica
- Processi governance (M231/01 d.Lgs231)
- Controllo di gestione
- Sistema gestione sicurezza sul lavoro

In relazione allo specifico servizio di conservazione dei documenti informatici, InfoCert ha adottato i seguenti standard internazionali:

· ISO 14721:2002 OAIS (Open Archival Information System), Sistema informativo aperto per
· l'archiviazione.
· ETSI TS 101 533-1 V1.1.1 (2011-05) 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 V1.1.1 (2011-05) 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.
· UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel
· Recupero degli Oggetti digitali.
· ISO 15836:2003 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

5 Manuale di conservazione

Il presente manuale di conservazione 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.

L'ordine di esposizione degli argomenti trattati è definito dall'Articolo 8 del DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione a cui il presente manuale si attiene fedelmente, mentre i contenuti relativi alla sicurezza sono trattati separatamente secondo le indicazioni previste nell'articolo 12 del medesimo DPCM.

5.1 Responsabile del servizio di conservazione (art. 8 comma 2)

Di seguito vengono riportati i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa.

Nell'allegato [5] "Processo MG115/TB02_Processi e Responsabilità_Integrated Management System"Integrated Management System per la gestione dei processi e delle responsabilità aziendali, le procedure che descrivono il Modello della gestione del presente capitolo sono formalizzate in:

- MG435 (Gestire risorse umane InfoCert)
- MG434 (Gestire la motivazione e lo sviluppo del personale InfoCert)

- MG115 (Modello di Gestione del Sistema Qualità; Organigramma e Mission InfoCert]

5.1.1 Responsabile del servizio di Conservazione in carica (Articolo 8 comma 2 lettera a)

Nominativo	Antonio dal Borgo
Data di inizio dell'incarico	15.07.2008 [[rif. lettera di nomina di A. Dal Borgo]
Data di termine dell'incarico	
Struttura organizzativa di competenza	Sviluppo e Gestione Servizi
Certificato rilasciato da	InfoCert Firma Qualificata
Note	Dal 01-07-2007 al 15-07-2008 A. Dal Borgo ha ricoperto la funzione di Responsabile della struttura tecnica preposta allo sviluppo e alla gestione di tutti i servizi compresi quelli predisposti per la gestione dei sistemi di conservazione; in questo ruolo ha collaborato con il responsabile del servizio della conservazione [P. Barban] .

Il responsabile riceve e sottoscrive un documento di nomina nel quale sono esplicitati gli incarichi e la durate degli stessi.

5.1.2 Storia dei Responsabili del servizio della Conservazione (Articolo 8 comma 2 lettera a)

Nominativo	Pio Barban
Data di inizio dell'incarico	01.07.2007
Data di termine dell'incarico	15.07.2008
Struttura organizzativa di competenza	Certificazione Digitale e Sistemi
Certificato rilasciato da	InfoCamere Firma Qualificata
Note	Prima della scissione di ramo di azienda che ha portato alla nascita di InfoCert, Pio Barban ricopriva l'analogo ruolo in InfoCamere S.c.p.a.

5.1.3 La struttura organizzativa nel processo di conservazione (Articolo 8 comma 2 lettera b)

5.1.3.1 Struttura organizzativa

I Soggetti Produttori affidano in outsourcing il servizio di conservazione a InfoCert S.p.A., che assume le responsabilità della conservazione in accordo con quanto previsto dal contratto, dagli allegati contrattuali e dall'articolo 5 comma 2 lettera b) del DPCM del 3 dicembre 2013.

InfoCert S.p.A. provvede ad affidare l'incarico di Responsabile del servizio della conservazione ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dagli allegati contrattuali.

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

Le attività eventualmente affidate ai singoli soggetti sono definite nell'ordine di servizio che regolamenta il rapporto tra InfoCert e i dipendenti. Ogni dipendente svolge solamente le attività per le quali hanno raggiunto un comprovato livello di competenza e/o esperienza tali da consentire un adeguato livello di autonomia, pur sotto la costante supervisione del diretto superiore gerarchico e/o del dipendente responsabile del servizio della conservazione.

Il processo di conservazione è normalmente effettuato da procedure totalmente automatizzate, che non necessitano dell'intervento di altri soggetti o delegati.

5.1.3.2 I sistemi di gestione

InfoCert ha adottato i seguenti sistemi di gestione e organizzazione dei processi produttivi e garanzia della soddisfazione del cliente:

- SGA - Sistema gestione Ambientale
- SGSQ - Sistema Gestione Qualità InfoCert

• SGSI- Sistema Gestione Sicurezza della Informazioni InfoCert

• SMS – Service Management System InfoCert

• SGSL- Sistema Gestione Sicurezza sul Lavoro InfoCert

• M213- Modello di organizzazione e controllo D.lgs. 231/01 InfoCert

In ottica di ottimizzazione delle governance aziendale è stato adottato un approccio d'integrazione dei sistemi di gestione ed organizzazione finalizzato a promuove un sistema di processi integrati a sostegno degli obiettivi di business al fine di migliorare l'efficacia e l'efficienza dell'organizzazione.

5.1.3.3 I ruoli e le attività dei profili professionali di InfoCert nel processo di conservazione

Di seguito descritti i profili professionali che sono essere presenti nella struttura organizzativa di InfoCert.

ruoli	nominativo	attività di competenza	periodo nel ruolo
Responsabile del servizio di conservazione	Antonio Dal Borgo	Rif. Manuale capitolo 5.1.15.5 • Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; • Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; • Corretta erogazione del servizio di conservazione all'ente produttore; • Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione. • Definizione delle condizioni generali del contratto di servizio in coordinamento con la funzione Legale e la funzione commerciale e funzione marketing di InfoCert.	Vedi capitolo 5.1.1 Assunzione a tempo indeterminato
Responsabile Sicurezza dei sistemi per la conservazione	Alfredo Esposito	Rif. Manuale capitolo 6.1 • Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	01-01-2011 Assunzione a tempo indeterminato

Responsabile funzione archivistica di conservazione	Silvia Loffi	• Definizione e descrizione archivistica dei documenti e delle aggregazioni documentali per la fruizione del patrimonio documentario e informativo conservato; • definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; • Analisi archivistica per lo sviluppo di funzionalità del sistema di conservazione; • collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	Assunzione a tempo indeterminato.
Responsabile trattamento dati personali	Alfredo Esposito	Riferimento Manuale capitolo 6.2 • Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; • garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza	Assunzione a tempo indeterminato

Responsabile sistemi informativi per la conservazione	Massimo Biagi	• Presidio ed evoluzione dei sistemi informativi per la conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000 • Gestione dell'esercizio delle componenti hardware e software di base del sistema di conservazione; • monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore in collaborazione con Il Responsabile della manutenzione del sistema di conservazione; • segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; • pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; • controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione. • Coordinamento dello sviluppo e manutenzione delle componenti hardware e software di base del sistema di conservazione;	Assunzione a tempo indeterminato

Responsabile sviluppo e manutenzione del sistema di conservazione	Nicola Maccà	• Sviluppo e manutenzione del sistema di conservazione nel rispetto delle procedure ISO9001 ISO14000 ISO20000 ISO27000 • Coordinamento dello sviluppo e manutenzione delle componenti software del sistema di conservazione; • pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; • monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; • interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche in collaborazione con il Responsabile funzione archivistica di conservazione; • gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Assunzione a tempo indeterminato

Il responsabile riceve e sottoscrive un documento di nomina nel quale sono esplicitati gli incarichi e la durate degli stessi.

5.1.3.4 Le responsabilità nel processo di conservazione

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

Responsabilità **Attività**	**Responsabile del servizio della Conservazione**	**Responsabile della funzione archivistica**	**Responsabile del trattamento dei dati personali**	**Responsabile della sicurezza dei sistemi per la conservazione**	**Responsabile dei sistemi informativi per la conservazione**	**Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
1. Condizioni Generali di Contratto	**R**					
2. Richiesta di attivazione	**R**	**V**	**V**	**V**	**V**	**V-E**
3. Atto di affidamento	**R**					
4. Specifiche Tecniche di integrazione	**V**			**A**	**A**	**R-E**
5. Impegno alla riservatezza	**V**		**R**	**A**		
6. Acquisizione del documento da conservare	**R**				**E**	**V**
7. metadatazione ed archiviazione	**A**	**R**			**E**	**V**
8. Eventuale attestazione della conformità di quanto memorizzato nel documento d'origine da parte di un PU	**R**					
9. Creazione del pacchetto di versamento(*)						
10. Invio al sistema di conservazione del pacchetto di versamento(*)						

Responsabilità **Attività**	**Responsabile del servizio della Conservazione**	**Responsabile della funzione archivistica**	**Responsabile del trattamento dei dati personali**	**Responsabile della sicurezza dei sistemi per la conservazione**	**Responsabile dei sistemi informativi per la conservazione**	**Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
11. Validazione Del pacchetto di versamento	**R**				**E**	**V**
12. Generazione del pacchetto di archiviazione	**R**				**E**	**V**
13. Memorizzazione e creazione "copia di sicurezza"	**R**			**V**	**E**	**V**
14. Invio dell'IPdA al soggetto Produttore	**R**					

[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]

(*) Le Responsabilità sono in capo al soggetto produttore e definite nelle specifiche contrattuali.

Tutte le verifiche in carico al Responsabile del servizio della conservazione sono garantite anche dal servizio di auditing interno.

5.1.4 Oggetti sottoposti a conservazione e i formati (Articolo 8 comma 2 lettera c)

5.1.4.1 Descrizione delle tipologie degli oggetti sottoposti alla conservazione

Il Soggetto Produttore, al momento dell'invio in conservazione, associa ad ogni documento informatico (Rif. Allegato 5 Metadati al DPCM del 2013), un file dei parametri di conservazione e un file di indici entrambi di tipo XML. Al documento viene inoltre associato dal sistema di conservazione un file di ricevuta (file IPdA, ovvero un Indice del pacchetto di archiviazione) nonché un identificativo univoco generato dal sistema stesso, definito token.

Il file IPdA, firmato dal Responsabile del servizio della conservazione e marcato temporalmente, attesta la correttezza del processo, e dà certezza al momento temporale. La struttura del file IPdA rispecchia quanto richiesto nell'Allegato 4 del DPCM del 2013; per una sua completa descrizione si rimanda all'Allegato [1].

Il documento rappresenta l'unità minima di elaborazione nel senso che viene memorizzato ed esibito come un tutt'uno; non è possibile estrarre dal sistema parti di un documento. Un documento conservato presso il sistema di conservazione, 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;

- è conservato insieme al file dei parametri di conservazione, al file di indici del documento e al file di ricevuta (file IPdA).

I documenti inviati nei formati standard, dettagliati nella documentazione contrattuale a disposizione del Soggetto Produttore, sono visualizzabili mediante i relativi software definiti e messi a disposizione da InfoCert e sono tutti quelli previsti dall'Allegato 2 del Decreto del 3 dicembre 2013. Il Soggetto Produttore che avesse necessità di inviare documenti con formato diverso può effettuare il caricamento degli appositi visualizzatori in LegalDoc utilizzando la funzionalità messa a disposizione dell'applicativo LegalDoc descritta in seguito.

Nel documento "Dati tecnici per l'attivazione", in cui il Soggetto Produttore fornisce tutte le informazioni necessarie all'integrazione dei sistemi di conservazione nel proprio sistema di gestione, sono definiti, insieme al Responsabile del servizio della conservazione, i metadati e le specifiche tecniche idonee per l'attivazione del servizio di conservazione (parte integrante della documentazione contrattuale).

Come stabilito dai già citati Decreti del 3 dicembre 2013 e del 17 giugno 2014, i documenti sono statici e non modificabili, ovvero sono redatti in modo tale per cui il contenuto non è alterabile durante le fasi di conservazione ed accesso, e sono immutabili nel tempo. In pratica, il documento non contiene macroistruzioni né codici eseguibili.

Le caratteristiche di staticità ed immodificabilità del documento inviato al sistema di conservazione digitale sono assicurate dal soggetto Produttore, che altresì verifica l'effettiva compatibilità del file con il visualizzatore definito.

5.1.4.2 Formati gestiti nel processo di conservazione

Nell'allegato[2] "NDOC-dati scheda tecnica di attivazione 1.0" allegato al contratto del servizio di conservazione sono esplicitati:

- I formati standard previsti nell'allegato 2 del DPCM 3 dicembre 2013
- I formati concordati
- I metadati delle tipologie documentali concordati

5.1.4.3 I processi di caricamento dei visualizzatori

I documenti informatici sono memorizzati sotto forma di evidenza informatica su adeguati supporti. Le evidenze informatiche dei documenti possono essere strutturate in diversi modi, detti formati informatici (o mime/type). Affinché sia possibile utilizzare queste informazioni sono necessari degli appositi programmi che permettano l'interpretazione di una evidenza informatica di un documento, visualizzandolo a terminale e/o stampandolo su supporto cartaceo. Tali programmi, detti visualizzatori (o viewer), devono essere mantenuti all'interno del sistema di conservazione.

Nel sistema LegalDoc i formati informatici dei documenti sono divisi in due categorie:

- formati predefiniti previsti dall'Allegato 2 al DPCM del 3 dicembre 2013. Per ognuno di questi InfoCert mette a disposizione un visualizzatore in grado di interpretare il relativo formato;
- altri formati: per ognuno di questi il visualizzatore deve essere fornito dal Soggetto Produttore e caricato a sistema nelle modalità descritte in questo capitolo.

I visualizzatori dei formati predefiniti da InfoCert richiesti dal Soggetto Produttore sono automaticamente assegnati all'atto della attivazione della propria area di conservazione, e verranno

forniti da InfoCert al Soggetto Produttore all'atto di attivazione del prodotto. Tutti i documenti inviati in conservazione saranno associati al visualizzatore configurato per il particolare formato.

I visualizzatori di formati aggiuntivi ai predefiniti devono essere inviati dal Soggetto Produttore **prima** di iniziare la conservazione dei documenti. Il sistema accetta i documenti in conservazione anche se il visualizzatore non è caricato, ma finché non viene caricato non è possibile effettuare l'esibizione dei documenti.

Il caricamento di un visualizzatore per un particolare mime/type va effettuato una sola volta. Ulteriori caricamenti per lo stesso mime/type verranno identificati come aggiornamenti di versione del visualizzatore nelle modalità descritte nell'allegato [1] del Manuale.

I formati aggiuntivi devono essere concordati tra il Soggetto Produttore e InfoCert in fase contrattuale in [1]. Non è possibile caricare visualizzatori per formati non preventivamente concordati e configurati nel sistema.

Il servizio di caricamento dei visualizzatori è richiamabile secondo le specifiche descritte in [1].

5.1.4.4 Responsabilità nel processo di caricamento dei visualizzatori

Di seguito è riporta la tabella di sintesi del processo di caricamento dei visualizzatori, inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema: input\dettaglio delle attività\output.

Responsabilità **Attività**	**Responsabile del servizio della Conservazione**	**Responsabile della funzione archivistica**	**Responsabile del trattamento dei dati personali**	**Responsabile della sicurezza dei sistemi per la conservazione**	**Responsabile dei sistemi informativi per la conservazione**	**Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
1. Creazione del file dei parametri di upload, del file della scheda tecnica e predisposizione dei file del visualizzatore (*).						
2. Invio della richiesta al sistema di conservazione(*).						
3. Validazione delle informazioni presenti nei file della richiesta	**R**				E	V
4. Caricamento del visualizzatore, creazione del file IPdA, marcatura temporale e firma digitale	**R**				**E**	**V**

Responsabilità **Attività**	**Responsabile del servizio della Conservazione**	**Responsabile della funzione archivistica**	**Responsabile del trattamento dei dati personali**	**Responsabile della sicurezza dei sistemi per la conservazione**	**Responsabile dei sistemi informativi per la conservazione**	**Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
dello stesso ed invio al soggetto Produttore.						

[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]

(*) Le Responsabilità sono in capo al soggetto produttore e definite nelle specifiche contrattuali.

ATT.1 Creazione del file dei parametri di upload, del file della scheda tecnica e predisposizione dei file del visualizzatore

INPUT	Predisposizione file	
		Predisposizione del file della scheda tecnica da associare al visualizzatore.
		Predisposizione del file del visualizzatore.
		Creazione del file dei parametri di upload secondo le specifiche in [1].
OUTPUT	File predisposti	

ATT.2 Invio della richiesta al sistema di conservazione

INPUT	*Richiesta di caricamento dei visualizzatori da preparare*	
		Invocazione del servizio di caricamento dei visualizzatori da parte del sistema di gestione, secondo le specifiche descritte in [1].
		Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di sessione (ldSessionId).
		Invio della richiesta al sistema di conservazione.
OUTPUT	*Richiesta di cancellazione preparata*	

ATT.3 Validazione delle informazioni presenti nei file della richiesta

INPUT	*Richiesta da validare*

	Ricezione della richiesta di caricamento dei visualizzatori.
	Verifica dei valori indicati nella richiesta.
OUTPUT	*Richiesta validata*

ATT.4 Caricamento del visualizzatore, creazione del file IPdA, marcatura temporale e firma digitale dello stesso ed invio al soggetto Produttore.

INPUT	*Visualizzatore da caricare*
	Caricamento del visualizzatore nel sistema di gestione .
	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.
	Creazione del file XML IPDA secondo le specifiche descritte in [1]
	Invio dell'esito e del file IPDA al soggetto Produttore
OUTPUT	*Visualizzatore caricato*

5.1.5 Definizione dei pacchetti (Articolo 8 comma 2 lettera d) operativamente

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 sulle specifiche descritte nell'allegato 1 SPT/NDOC- Specifiche tecniche per l'integrazione e all'allegato 2 AL/NDOC – Allegato Tecnico al Contratto LegalDoc.

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

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nell'allegato 1 SPT/NDOC- Specifiche tecniche per l'integrazione. Ad ogni documento il Sistema di conservazione associa un file XLM, detto Indice del Pacchetto di Archiviazione. L'insieme degli Indici del Pacchetto di Archiviazione associati ai file componenti un pacchetto è detto rapporto di versamento.

Per "pacchetto di distribuzione" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta, ovvero è la risposta alla ricerca effettuata dal Soggetto Produttore tramite interfaccia disponibile, che porta all'esibizione del documento

conservato. Il documento da esibire è accompagnato sempre dall'IPdA. Nel sistema il "pacchetto di distribuzione" coincide con il "pacchetto di archiviazione".

Eventuali specificità sono concordate con il soggetto Produttore e descritte nell'allegato 1 SPT/NDOC- Specifiche tecniche per l'integrazione e all'allegato 2 AL/NDOC – Allegato Tecnico al Contratto LegalDoc.

5.1.6 Presa in carico dei pacchetti di versamento (Articolo 8 comma 2 lettera d)

Di seguito è riporta la tabella "5.1.3.4Le responsabilità nel processo di conservazione", in particolare dalle attività 10 al 14. Inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema: input\dettaglio delle attività\output.

Responsabilità Attività	**Responsabile del servizio della Conservazione**	**Responsabile della funzione archivistica**	**Responsabile del trattamento dei dati personali**	**Responsabile della sicurezza dei sistemi per la conservazione**	**Responsabile dei sistemi informativi per la conservazione**	**Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
10.Invio al sistema di conservazione del pacchetto di versamento (*)						
11.Validazione del pacchetto di versamento	**R**				**E**	**V**
12. Generazione del pacchetto di archiviazione	**R**				**E**	**V**
13.Memorizzazione e creazione "copia di sicurezza"	**R**			V	**E**	**V**
14.Invio dell'IPdA al soggetto Produttore	**R**					

(*) Le Responsabilità sono in capo al soggetto produttore e definite nelle specifiche contrattuali.

ATT.10 Invio al sistema di conservazione del pacchetto di versamento

INPUT	*Documento da inviare al sistema di conservazione tramite il pacchetto di versamento*
	Invocazione del sistema di conservazione da parte del sistema di gestione, secondo lo standard descritto in [1].

		Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di sessione (ldSessionId)
		Trasmissione del pacchetto di versamento costituente il documento (file di dati, il file di indici del documento e il file dei parametri di conservazione) secondo le modalità di trasmissione descritte in [1].
OUTPUT	*pacchetto di versamento inviato*	

Per maggiori dettagli si rimanda al documento "SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc"(vedi elenco allegati al Manuale).

ATT.11 Validazione del pacchetto di versamento

INPUT	*Pacchetto di versamento*	
		Generazione dell'impronta di ogni file costituente il documento e confronto con la corrispondente impronta inviata dal soggetto Produttore, a garanzia dell'integrità del documento ricevuto. In caso di esito negativo delle verifiche, rigetto del documento con invio al sistema di gestione del Soggetto Produttore dell'errore intercorso. In questo caso, termine del flusso.
		Controllo dei valori indicati dal Soggetto Produttore nel file dei parametri di conservazione: verifica della policy dichiarata, verifica della congruenza dei tipi di file inviati (mimetype), verifica dell'univocità del file all'interno del path (cartella) indicato.
		Controllo dei valori indicati dal Soggetto Produttore nel file di indici del documento: validazione dei tracciati dei file di indice, verifica della correttezza della classe documentale, verifica della compatibilità fra policy dichiarate e policy configurate, verifica degli indici obbligatori (esistenza, valorizzazione, non duplicazione, correttezza del tipo di file, controllo numerico). I valori espressi nel file di indici vengono confrontati con la configurazione presente nelle apposite tabelle presenti nel database LegalDoc.
		Aggiornamento dei database del sistema con i dati relativi a il documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.
OUTPUT	*pacchetto di versamento verificato*	

5.1.6.1 Descrizione del rapporto di versamento

L'art. 7 comma c) del DPCM del 3 dicembre 2013 inserisce tra gli oneri del Responsabile del servizio della conservazione quello di generare il rapporto di versamento. Il rapporto di versamento

attesta l'avvenuta presa in carico da parte del sistema di conservazione del pacchetto di versamento inviato dal produttore ed è l'insieme degli Indici del Pacchetto di Archiviazione prodotti per ogni singolo documento oggetto di versamento (vedi allegato 1 SPT/NDOC- Specifiche tecniche per l'integrazione).

Il rifiuto dei pacchetti di versamento avviene nella modalità descritta nell'allegato 1 SPT/NDOC- Specifiche tecniche per l'integrazione e per le casistiche definite nell'allegato 4 SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc.

5.1.7 Descrizione del processo di conservazione (Articolo 8 comma 2 lettera e)

5.1.7.1 Descrizione generale del servizio

Il sistema di conservazione è erogato in modalità SaaS (Software as a Service) secondo uno schema di Business Process Outsourcing (BPO) e permette di mantenere e garantire nel tempo l'integrità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

Il sistema consente le funzionalità di:

- **accettazione del pacchetto di versamento**;
- **conservazione del pacchetto di archiviazione**: il documento, 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; la rettifica si applica al pacchetto di archiviazione;
- **scarto\cancellazione del pacchetto di archiviazione:** un documento inviato in conservazione può essere cancellato. Il sistema terrà comunque evidenza del documento all'interno dell'archivio a norma, nel rispetto del principio di tracciabilità; la cancellazione si applica al pacchetto di archiviazione, inoltre **lo scarto è l'operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.**
- **esibizione del pacchetto di distribuzione**: il documento richiesto via web viene richiamato direttamente dal sistema di conservazione digitale ed esibito, con garanzia della sua opponibilità a terzi;
- **ricerca dei documenti informatici indicizzati**: il Soggetto Produttore può eseguire una ricerca tra i documenti conservati trasversalmente sulle classi documentali;
- **visualizzazione delle statistiche di conservazione**;
- **caricamento dei visualizzatori**: è previsto il deposito dei visualizzatori da parte del Soggetto Produttore qualora la tipologia dei file conservati non sia quella standard, definita in fase di attivazione del sistema.

Il sistema di conservazione integra il sistema di gestione del Soggetto Produttore, sia esso un'azienda o un ente locale, e ne estende i servizi con funzionalità di stoccaggio digitale.

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

5.1.7.2 L'Indice del Pacchetto di Archiviazione e il rapporto di versamento

L'Indice del Pacchetto di Archiviazione è un file in formato XML, marcato temporalmente e firmato digitalmente dal responsabile del servizio della conservazione ione, generato dal sistema secondo le specifiche descritte in [1], che contiene le informazioni di conservazione del documento e viene con esso conservato.

In particolare nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA
- il token del documento
- l'operazione eseguita (conservazione, rettifica, scarto e cancellazione)
- il bucket (area di conservazione) associato al Soggetto Produttore e la policy utilizzata
- il nome dei file che compongono il documento, incluso il file dei parametri di conservazione ed il file di indici, e le rispettive impronte
- eventuali informazioni relative al documento rettificante e rettificato
- il tempo di creazione (timestamp) del file IPdA

L'insieme degli IPdA di un pacchetto formano il rapporto di versamento di cui all'art. 9, comma d) del DPCM del 3 dicembre 2013.

Il file IPdA è reso disponibile con il documento di riferimento ad ogni operazione di conservazione e richiesta esibizione.

ATT.12 Generazione del pacchetto di archiviazione

Le fasi previste sono la memorizzazione, la creazione del file IPDA e la marcatura temporale dello stesso.

INPUT	*Pacchetto di archiviazione*
	Eventuale apposizione della firma digitale sul file di dati (se prevista da accordi contrattuali)
	Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) secondo il formato descritto in [1] contenente: le informazioni sul processo di conservazione (in particolare sul software LegalDoc), le policy ed il bucket (area di conservazione) utilizzati, il nome e le impronte dei file costituenti il documento e l'identificativo (token) assegnato al documento,
	Marcatura e firma dal parte del Responsabile del servizio della conservazione del file IPdA. Copia del file sul supporto primario.
	Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.

OUTPUT	*pacchetto di archiviazione*

ATT.13 Memorizzazione e creazione copia di sicurezza

INPUT	*Pacchetto di archiviazione*
	Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali
	Inserimento nelle tabelle di interfaccia del sistema di archiviazione permanente delle informazioni di puntamento dei file, al fine di poter reperire gli stessi in seguito.
	La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
OUTPUT	*Documenti conservati*

ATT.14 Invio dell'IPdA al soggetto Produttore

INPUT	*File IPdA*
	Invio dell'esito e del file IPdA al soggetto Produttore.
OUTPUT	*Esito conservazione inviato*

5.1.8 Processo di esibizione e di esportazione (Articolo 8 comma 2 lettera f)

5.1.8.1 Il processo di esibizione di un pacchetto di distribuzione

Le procedure di esibizione permettono di estrarre dal sistema un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione, di rettifica o di cancellazione, utilizzando il relativo token. Insieme ai file costituenti il pacchetto di distribuzione, sono rese disponibili anche le informazioni che qualificano il processo di conservazione, ossia il file IPdA. Non è possibile esibire parti singole di documento.

L'esibizione può restituire il documento in due modalità differenti: in un unico pacchetto di distribuzione in formato zip, oppure un file alla volta. Quest'ultima modalità deve essere compatibile con il client di esibizione del soggetto Produttore.

5.1.8.2 Reperimento dei documenti e corretta esibizione

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione.

In particolare ogni documento inserito nel sistema di conservazione è identificato in maniera univoca mediante una stringa denominata token.

Il token consente il reperimento di ciascun documento e la sua corretta esibizione, nonché la fruizione dei servizi di rettifica, di ricerca e di cancellazione logica.

Le procedure del sistema mantengono e aggiornano ad ogni nuovo invio il database di tutti i token; il database viene interrogato ad ogni richiesta di rettifica, scarto e cancellazione, ricerca ed esibizione confrontando il token inviato con quelli memorizzati. La procedura assicura di agire solamente sul documento richiesto, e solamente se in possesso dei dovuti profili di autorizzazione.

5.1.8.3 Esibizione a norma

L'esibizione del pacchetto di distribuzione ottenuto tramite interrogazione al sistema di conservazione rappresenta un'esibizione completa, legalmente valida ai sensi del secondo comma dell'articolo 10 del DPCM 03/12/13 e dell'articolo 5 del DMEF 17/06/14.

Un apposito strumento di esibizione e verifica, anche detto “Esibitore a Norma”, permette di richiamare agevolmente un documento conservato e consente di ottenere in modo automatico sia la verifica delle firme digitali e delle marche temporali apposte che le verifiche di integrità dei documenti conservati e di tutti gli altri elementi conservati. Si rimanda a [11] per il dettaglio delle funzionalità di verifica del sistema.

Di seguito si descrivono le fasi della procedura di esibizione standard.

5.1.8.4 Responsabilità nel processo di esibizione dal sistema

Di seguito è riporta la tabella di sintesi del processo di esibizione dal sistema di conservazione, inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema: input\dettaglio delle attività\output.

Responsabilità **Attività**	**Responsabile del servizio della Conservazione**	**Responsabile della funzione archivistica**	**Responsabile del trattamento dei dati personali**	**Responsabile della sicurezza dei sistemi per la conservazione**	**Responsabile dei sistemi informativi per la conservazione**	**Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
1. Ricerca documento da esibire (*)						
2. Richiesta di esibizione del documento conservato (*)						
3. Accettazione della richiesta da parte del sistema di conservazione	**R**				E	V

Responsabilità **Attività**	**Responsabile del servizio della Conservazione**	**Responsabile della funzione archivistica**	**Responsabile del trattamento dei dati personali**	**Responsabile della sicurezza dei sistemi per la conservazione**	**Responsabile dei sistemi informativi per la conservazione**	**Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
4. Risposta del sistema di conservazione ed esibizione del documento	**R**				**E**	**V**

[**R**-responsabile; **E**-esegue; **V**- verifica; **A**-approva]

(*) Le Responsabilità sono in capo al soggetto produttore e definite nelle specifiche contrattuali.

ATT1.Ricerca del documento) da esibire

INPUT	*Lista di token archiviati dal sistema*	
		Ricerca negli archivi del sistema del token relativo al documento da esibire attraverso le procedure previste dai sistemi di gestione.
		Restituzione del token corretto.
OUTPUT	*Token relativo al documento da esibire*	

ATT2.Richiesta di esibizione del documento conservato

INPUT	*Richiesta di esibizione da eseguire*	
		Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di session (ldSessionId).
		Invocazione del servizio di esibizione del sistema di conservazione secondo le modalità descritte in [1]. In questa chiamata viene utilizzato il token ricavato in precedenza.
OUTPUT	*Richiesta di esibizione eseguita*	

ATT.3Accettazione della richiesta da parte del sistema di conservazione

INPUT	*Richiesta di esibizione*	
		Ricezione della richiesta di esibizione del documento.
		Controllo di corrispondenza tra il token inviato dal Soggetto Produttore e

	quelli dei documenti conservati.
OUTPUT	*Richiesta di esibizione presa in carico*

ATT.4Risposta del sistema di conservazione ed esibizione del documento

INPUT	*Richiesta di esibizione acquisita*
	Ricerca dei file costituenti il documento e dei file attestanti il processo di conservazione corrispondenti al token inviato e preparazione del pacchetto di file.
	Invio della risposta al sistema del Soggetto Produttore secondo le modalità previste in [1].
OUTPUT	*Documento esibito*

5.1.9 Componenti tecnologici del sistema di conservazione (Articolo 8 comma 2 lettera g)

5.1.9.1 Architettura generale del sistema

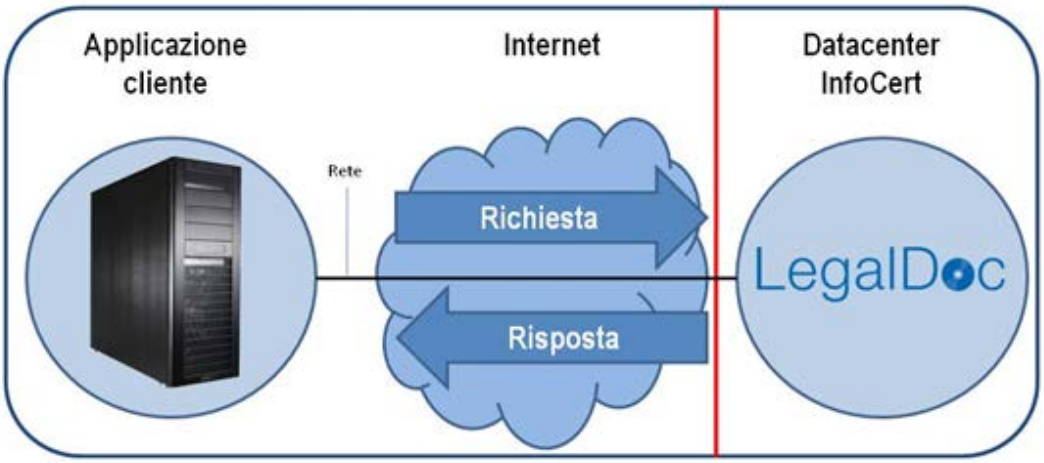
La descrizione puntuale dell'architettura generale del sistema di conservazione è presente nell'Allegato 16 – LDOC/Architettura logica e fisica del sistema di conservazione. I dettagli del sito primario sono descritti nel paragrafo 6.5.1. del presente Manuale.

Il sito secondario è dimensionato ad un terzo del sito primario, con l'esclusione della parte di storage che è dimensionata in modo equivalente.

Il sistema di conservazione è implementato da un'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). La gestione della configurazione dell'applicazione è dettagliata in [1], a cui si rimanda.

Il sistema è reso in modalità SaaS (Service as a Service) e consente al Soggetto Produttore di accedere ai sistemi 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 Condizioni Generali di Contratto e nella relativa documentazione tecnica da questo referenziata.

Il sistema è accessibile dalla apposita URL di rete; il Soggetto Produttore richiama il sistema di conservazione secondo le modalità indicate da InfoCert.



Dal punto di vista architetturale LegalDoc è realizzato utilizzando la tecnologia dei Web Services. I Web Services di LegalDoc sono implementati secondo architettura REST su protocollo HTTPS.

L'applicativo LegalDoc è dotato anche di un'interfaccia web con funzionalità in parte ad uso del Responsabile del servizio della conservazione, in parte per i soggetti Produttori.

Il sistema è protetto da firewall ed implementa un sistema di back-up dei dati memorizzati.

5.1.9.2 Firewall

I firewall assicurano la difesa del perimetro di sicurezza tra il sistema e il mondo esterno, nonché tra i sistemi dedicati all'erogazione del sistema ed i sistemi che interfacciano i dispositivi sicuri per la generazione della firma digitale.

I firewall sono configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile.

5.1.9.3 Servizi REST

Il prodotto LegalDoc è basato su servizi di tecnologia REST e svolge le operazioni di conservazione, esibizione, rettifica, cancellazione e ricerca. A sua volta utilizza componenti esterne e servizi esposti da altri prodotti InfoCert.

5.1.9.4 Back-up

L'intero sistema di conservazione viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria per la sicurezza del sistema.

5.1.9.5 Servizio di marcatura temporale

Per l'emissione delle marche temporali il sistema si avvale del servizio di marcatura di InfoCert, Certification Authority accreditata, le cui modalità di utilizzo sono descritte in [8], cui si rimanda. Il Piano per la Sicurezza del Certificatore è depositato presso AgID.

La marca temporale viene richiesta, utilizzando lo standard RFC3161, al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert. Il root-certificate della TSA è depositato presso AgID.

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.

5.1.9.6 Dispositivo HSM di firma digitale

Il sistema si avvale dei servizi di firma digitale forniti dalla CA InfoCert. In particolare, il servizio di firma automatica (firma massiva) permette di apporre automaticamente la firma digitale e la validazione temporale ad elevati volumi di documenti informatici, senza che sia necessaria la presenza del titolare nel momento preciso della firma.

I dispositivi utilizzati rispondono ai requisiti di sicurezza previsti per i dispositivi sicuri di firma.

5.1.9.7 Sistema Storage

Il sistema di conservazione di InfoCert utilizza storage magnetici ad alte performance come sistema primario e secondario per la memorizzazione dei dati. Tali storage, scelti tra i primari fornitori di tecnologie presenti sul mercato, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato.

L'allineamento tra il sito primario e il sito secondario avviene coerentemente con le politiche generali di Disaster Recovery definite in InfoCert che garantiscono RTO e RPO inferiori alle 48 ore.

Gli attuali fornitori del sistema di storage sono NetAPP e EMC2.

Tali storage rispondono all'esigenza di memorizzazione a lungo termine dei fixed content, ossia dei files che devono essere conservati con garanzia nel tempo di integrità e disponibilità del contenuto.

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni. Nel caso di documenti che contengono dati sensibili i dati vengono memorizzati cifrati con chiave in disponibilità al solo Responsabile del servizio della conservazione.

I sistemi di storage sono stati valutati da InfoCert sotto molteplici profili e, in virtù delle loro caratteristiche fisiche e architetturali, sono ritenuti idonei ad essere utilizzati nel sistema di conservazione.

Nell'ambito del sistema di conservazione, lo storage rappresenta il sia il supporto primario di conservazione posto fisicamente presso la sede InfoCert di Padova, sia il supporto secondario posto nel sito di disaster recovery di Modena. I due sistemi sono interconnessi mediante collegamenti ad alta velocità dedicati, completamente ridondati e protetti da misure di sicurezza. I collegamenti consentono la replicazione dei dati conservati eliminando il rischio di distruzione di tutte le copie delle informazioni in caso di danno irreparabile a livello di sito.

Questo secondo sistema funge anche da copia di sicurezza.

5.1.9.8 Posta Elettronica Certificata

Il sistema di conservazione si avvale del servizio di posta elettronica certificata di InfoCert: in sede di attivazione del sistema, viene definita per il Soggetto Produttore una casella di posta certificata (PEC) tramite la quale richiedere supporto alla casella di amministrazione del sistema.

La PEC configurata all'attivazione è utilizzata, inoltre, per ogni comunicazione al Soggetto Produttore che interessa il funzionamento del sistema.

5.1.9.9 Sincronizzazione dei sistemi

Tutti i server di InfoCert, attraverso il protocollo NTP (Network Time Protocol), sono sincronizzati sul “tempo campione” fornito dall’Istituto di Ricerca Metrologia – INRIM (già Istituto Elettrotecnico Nazionale “Galileo Ferraris”), abilitato a fornire il “tempo campione” ai sensi dell’articolo 2, comma 2, lettera b) del D.M. 30 novembre 1993, n. 591 “Regolamento concernente la determinazione dei campioni nazionali di talune unità di misura del Sistema internazionale (SI) in attuazione dell’art. 3 della L. 11 agosto 1991, n.273. La sincronizzazione è protetta da misure di sicurezza fisiche e logiche documentate per impedirne la manomissione.

Il meccanismo di allineamento temporale tra i sistemi fornisce la certezza della successione temporale degli avvenimenti nel sistema. La sincronizzazione delle macchine infatti, genera dei file di log temporalmente omogenei tra loro, che permettono di ricostruire con certezza l'ordine di accadimento degli eventi intervenuti a tutti i livelli del sistema, e di individuare la sequenza di svolgimento delle varie operazioni.

5.1.9.10 Definizione delle caratteristiche del sistema di conservazione

Il sistema di conservazione InfoCert e il processo da questi implementato rispondono interamente alle norme di legge che regolano la materia.

La progettazione e il continuo miglioramento del sistema di conservazione sono il frutto di una intensa opera di confronto tra le professionalità e le competenze delle diverse funzioni aziendali, al fine di giungere all'erogazione di un sistema pienamente conforme alle norme, architetturalmente stabile, affidabile, e che garantisca elevati livelli di servizio all'utente in condizioni di assoluta sicurezza, certezza degli accessi e tracciabilità delle operazioni.

Punto fondante del processo di progettazione è l'attenta disamina delle norme, al fine di definire puntualmente i requisiti legali che il sistema deve possedere per assicurare la corretta implementazione della conservazione.

Il rispetto dei requisiti di legge è la condizione imprescindibile per l'erogazione del servizio; oltre a questi sono definiti ulteriori requisiti funzionali, di architettura e di connettività e interoperabilità. I requisiti funzionali, individuati dal gruppo di competenza, rispondono all'obiettivo di offrire al Soggetto Produttore le funzionalità da questi richieste, mentre i requisiti di architettura e di interoperabilità rispondono alla necessità di sviluppare e mantenere un sistema stabile, in linea con le evoluzioni tecnologiche e capace di interfacciarsi con gli altri sistemi sviluppati dall'azienda, sfruttando le economie di scala e di conoscenza.

5.1.9.11 Criteri di organizzazione del contenuto

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi in cui i documenti sono corredati da tutta una serie di metadati. I documenti inviati al sistema di conservazione, infatti, vengono aggregati secondo criteri di omogeneità secondo le informazioni di configurazione definite in fase contrattuale. In particolare, vengono concordati i parametri fondamentali (bucket, policy, classi documentali) con i quali sono organizzati i documenti presi in carico, per consentire la maggiore interoperabilità possibile tra i sistemi di conservazione.

5.1.9.12 Organizzazione dei supporti

Come atto conclusivo della procedura di conservazione, i documenti vengono memorizzati nel sistema di storage. Nel sistema di storage, sono contenuti tutti i documenti inviati in conservazione e i relativi file IPdA in conformità alle regole AgID, OAIS e SInCRO.

.

5.1.9.13 Archivio dei viewer consegnati dal soggetto Produttore

InfoCert ha stabilito dei formati standard per i documenti da inviare in conservazione, dettagliati nella documentazione contrattuale a disposizione del Soggetto Produttore e nel DPCM del 3 dicembre 2013, per i quali l'azienda definisce e mette a disposizione dei Soggetti Produttori i relativi viewer, mantenendoli aggiornati. Al momento dell'attivazione del servizio, il Soggetto Produttore verifica che i documenti inviati siano nel formato standard e siano leggibili con il software definito da InfoCert.

Il sistema di conservazione InfoCert può conservare documenti informatici in un qualsiasi formato; se il Soggetto Produttore ha l'esigenza di inviare in conservazione documenti in formati differenti da quelli definiti standard, provvede a fornire ad InfoCert, tramite apposita funzionalità dell'applicativo LegalDoc descritta in precedenza, il relativo software di visualizzazione.

Se il Soggetto Produttore invia documenti in formato non standard senza depositare il relativo visualizzatore, oppure nel caso di invio di documenti in modalità cifrata, è sua cura la conservazione degli strumenti necessari per la decifratura e/o la visualizzazione di quanto conservato.

Il Responsabile del servizio della conservazione mantiene i programmi consegnati in un apposito database sottoposto a un periodico processo di back-up; in questo processo, il responsabile è supportato dalle apposite procedure automatiche del sistema.

5.1.9.14 Archivio dell'hardware e del software obsoleto

La tenuta di un archivio dell'hardware e dei sistemi operativi ormai obsoleti ma necessari alla visualizzazione dei documenti conservati non è esplicitamente prevista dalla norma, ma è un'attività che si desume dall'obbligo di tenuta dell'archivio dei software nelle eventuali diverse versioni, e a questo direttamente correlata e fa parte delle misure per combattere l'obsolescenza dei formati, citate all'art. 7 comma 1 lettera g) dal Decreto 2013.

Difatti, la normativa vigente prevede che i documenti informatici conservati devono poter essere perfettamente visualizzati durante l'intero periodo di conservazione, stabilito in almeno 10 anni per i documenti con rilevanza tributaria o fino a quando non si siano conclusi gli accertamenti relativi al periodo di imposta. Per le altre tipologie documentali i tempi di conservazione e le eventuali attività di scarto o di versamento in Archivi di Stato o nell'Archivio Centrale dello Stato saranno decisi caso per caso, analizzando i quadri normativi di riferimento e i massimari di selezione e scarto in uso presso i soggetti Produttori.

Il progresso tecnologico dei sistemi, tuttavia, può portare all'impossibilità di utilizzare i viewer definiti dal soggetto Produttore, se divenuti obsoleti, sulle macchine di ultima generazione, rendendo di fatto impossibile la presa di conoscenza del contenuto del documento e inficiandone così la validità legale nel tempo.

Per far fronte a questo rischio, il Responsabile del servizio della conservazione mantiene un archivio di tutte le componenti hardware e software non più compatibili con i programmi di visualizzazione garantiti e/o depositati dal soggetto Produttore, nel caso questi siano i soli strumenti che consentono di rendere leggibile i documenti conservati associati a tale viewer.

5.1.9.15 Service Management System – SMS InfoCert

InfoCert ha scelto di introdurre in azienda un Service Management System - SMS conforme alla **norma ISO/IEC 20000** [standard internazionale per l'IT Service Management] allo scopo di mantenere e migliorare l'allineamento e la qualità dei servizi di business e,rogati, attraverso un ciclo costante di monitoraggi, reporting e revisione degli SLA concordati.

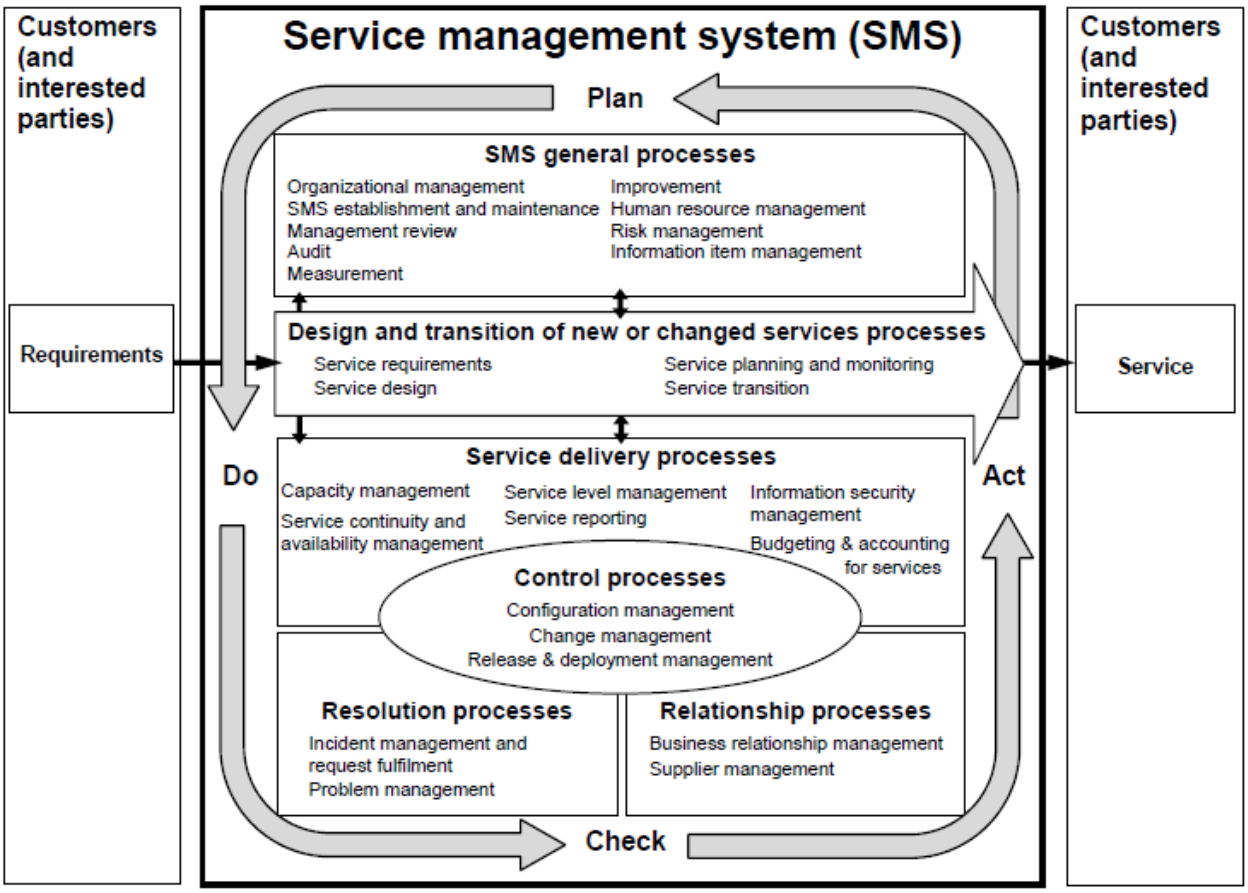
InfoCert ha individuato nella Certificazione ISO 20000 un obiettivo di qualificazione dell'offerta in grado di conferire **valore aggiunto ai servizi offerti e una maggiore garanzia dei livelli di servizio concordati** con i propri clienti.

L'adozione di un modello di Service Management System – SMS InfoCert ha permesso di :

- mappare ed integrare i Livelli di Servizio (SLA) garantiti ai clienti in relazione ai Livelli di servizio operativi garantiti internamente e quelli contrattuali garantiti dai fornitori;
- strutturare e governare la catena di composizione del valore dei servizi;
- ottimizzare la gestione dei processi aziendali integrando processi produttivi con processi di business fornendo un modello per la gestione sui servizi erogati;
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti evitando di assecondare aspettative cliente non erogabili;

- garantire un controllo dei fornitori che concorrono alla erogazione dei nostri servizi;
- migliorare la qualità dei servizi di business erogati

Di seguito lo schema rappresentativo del Modello adottato da InfoCert



Rappresentazione grafica processi della norma ISO/IEC 20000:11

Le attività di istituzione, attuazione, monitoraggio e sviluppo del Service Management System-SMS seguono il modello ciclico PDCA che si sviluppa nelle seguenti fasi:

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche e i requisiti per la gestione del servizi inerenti il campo di applicazione;
- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement dei servizi sulla base di quanto definito nel *service management plan;*
- azioni di monitoraggio e revisione del sistema-SMS (Check);
- attuazione di misure a miglioramento del sistema-SMS (Act) ove sono pianificate e attuate idonee azioni correttive sulla base dei risultati della fase precedente.

Il processo di gestione dei Livelli di Servizio [Service Level Management] è considerato un processo cardine del Service Management System in quanto ha effetto sui tre obiettivi principali quali:

- allineare i servizi di business con i bisogni correnti e futuri del cliente

- coordinare i requisiti del mercato sui servizi offerti con gli obbiettivi aziendali
- migliorare la qualità' dei servizi di business erogati
- fornire attraverso gli SLA una base per la determinazione del valore del servizio

Nello specifico InfoCert ha definito degli SLA baseline di riferimento in relazione ai seguenti KPI:

- Orario di servizio
- Disponibilità di servizio

Nell'allegato [5] "Processo MG115/TB02_Processi e Responsabilità_Integrated Management System", sono indicate le procedure che descrivono il Modello della gestione del presente capitolo; in sintesi:

- MGSMS (modello service management system)
- MGSLM (service Level management system)
- MGSLR (SLA reporting)

5.1.10 La descrizione delle procedure di monitoraggio (Articolo 8 comma 2 lettera h);

5.1.10.1 Monitoraggio dei sistemi

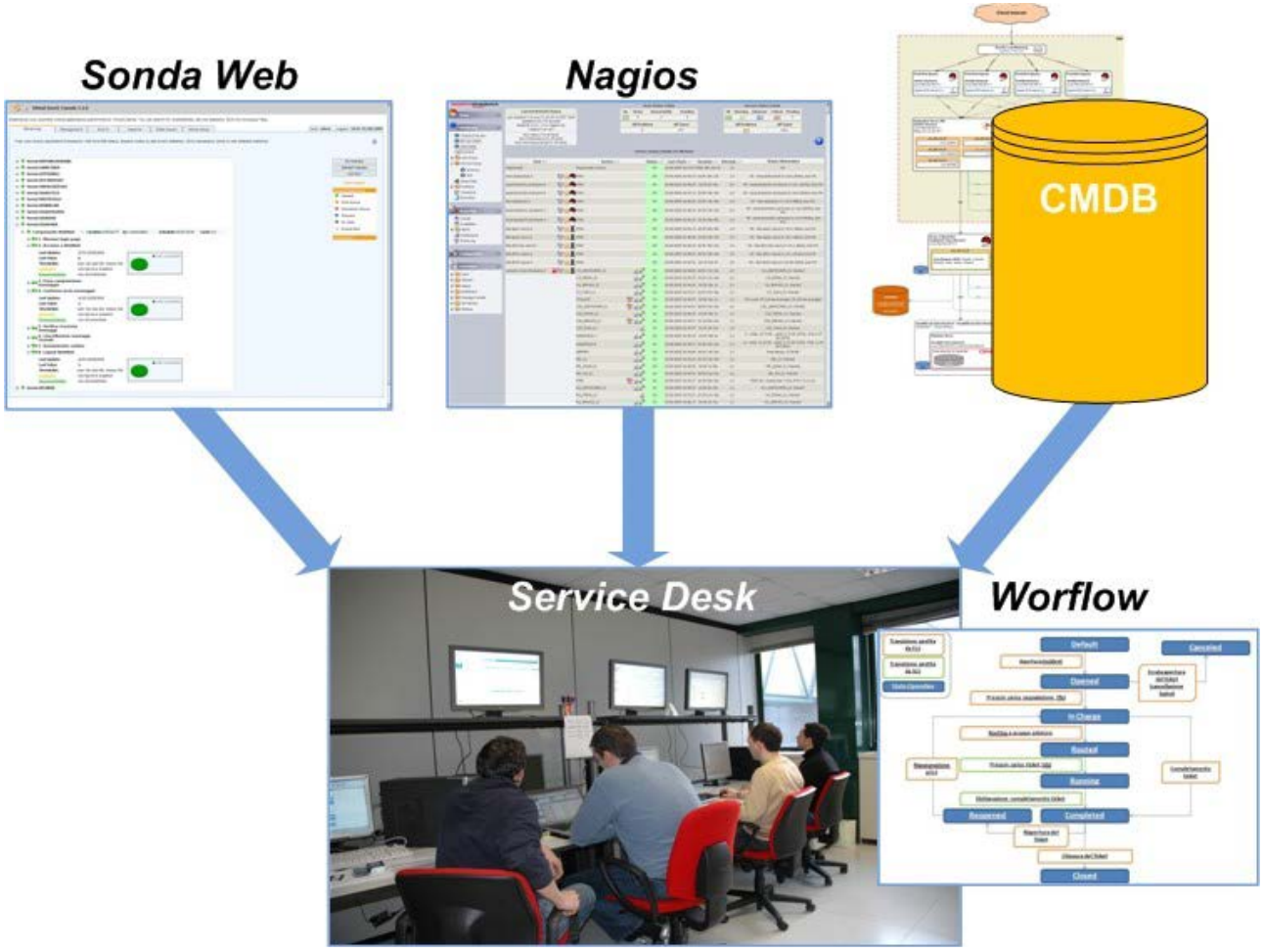
Il Data Center InfoCert è gestito seguendo le best practice suggerite dall'ITIL (Information Technology Infrastructure Library) implementato in conformità alla norma ISO 20000.

A livello organizzativo è presente una struttura di Service Desk la quale agisce come SPOC (Single Point Of Contact) per problemi relativi all'erogazione dei servizi. Le strumentazioni di controllo sono state implementate su progetti open source come il Nagios, tramite il quale si realizza il monitoraggio completo dei servizi di business offerti da InfoCert.

Nello specifico, InfoCert utilizza:

- il prodotto Net-eye di Wuerth Phoenix, basato su una logica di event management e finalizzato al monitoraggio e controllo di sistemi e servizi
- il prodotto S3 Virtual User, che implementa delle navigazioni automatiche sui servizi rilevando il corretto funzionamento dell'applicazione e lo SLA del servizio.

Il processo di Incident Management si avvale di una robusta infrastruttura di Event Management, nella quale i controlli Nagios sulle risorse vengono integrati e correlati con navigazioni web che testano il servizio in tutta la sua catena infrastrutturale. Gli eventi rilevati sono correlati alle mappe di servizio, registrate nel sistema di gestione della configurazione (CMDB – Configuration Management Database). Tramite queste fonti di informazione gli operatori del Service Desk sono in grado di operare con una soluzione di 1° livello, qualora l'evento sia già presente nel known error database, oppure di scalare la malfunzione verso il 2° livello inserendo tutte le informazioni necessarie ed attivando il corretto gruppo di supporto mediante un sistema di gestione del Workflow.



Le console operative del data center sono controllate dagli operatori durante l'orario di presidio. Sulle console operative vengono riportati, per ogni singolo server oggetto di controllo, tutte le informazioni raccolte dagli agenti e che richiedono l'attenzione degli operatori. Al di fuori di tali orari è previsto un servizio di reperibilità degli operatori del Service Desk che vengono avvisati in caso di anomalie dai sistemi di controllo automatici, tramite un sistema di notifica automatica SMS.

Il 2° livello di supporto è composto da un team di tecnici specializzati su tutti gli ambiti tecnologici (sistemi di base e storage, network, middleware e database).

5.1.10.2 Processi di monitoraggio del sistema di conservazione

Il monitoraggio del sistema di conservazione si esplica su due diversi livelli operativi:

- sistema di monitoring della disponibilità del sistema
- sistema di monitoring dell'integrità degli archivi

5.1.10.3 Monitoring della disponibilità del sistema

Tale operazione viene svolta coerentemente con le procedure di monitoring generali di InfoCert. In particolare tutte le componenti costituenti il sistema di conservazione, ovvero i servizi applicativi, i processi di elaborazione batch e le interfacce per l'utente finale sono inserite nel sistema di Sonde aziendale implementato con lo strumento S3 Virtual User.

A fronte di anomalie rilevate lo strumento invia delle segnalazioni al Service Desk InfoCert che le gestisce in conformità ai processi di Incident Management e, se necessario, Problem Management. Tali processi sono descritti nelle procedure che definiscono il Sistema di gestione integrato InfoCert.

5.1.10.4 Monitoring dell'integrità dell'archivio

Il sistema di memorizzazione utilizzato, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architetturale e alle procedure di memorizzazione permanente dei dati, garantisce l'immodificabilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione.

Il sistema mantiene traccia di tutte le operazioni effettuate sui documenti in appositi file di log; inoltre, è garantita la tracciatura di tutti i documenti richiamati dal Soggetto Produttore mediante interrogazione al sistema e conseguentemente esibiti, che rappresenta una ulteriore prova di leggibilità, effettuata direttamente dal soggetto Produttore.

Inoltre come descritto dall'art. 7 comma 1 lettera 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”, InfoCert, per rispondere a tali richieste, ha attivato sottosistemi di controllo automatico dedicati alla simulazione della navigazione nel sistema e delle operazioni che effettua l'utente, svolgendo controlli di coerenza dei dati e attività di ripristino da situazioni di errore.

In ogni occasione in cui il file viene copiato o spostato di posizione, funzionalità automatiche verificano che le sue dimensioni non siano mutate durante lo spostamento e che non siano intervenute alterazioni, che possono inficiare la visualizzazione.

In aggiunta alle procedure citate, il sistema implementa numerosi controlli automatici a garanzia dell'integrità e della coerenza dei dati movimentati; i controlli automatici richiedono l'intervento del Responsabile del servizio della conservazione solo al verificarsi di eventi anomali non gestibili in modo automatico. In particolare, è stata realizzata una procedura specifica denominata ‘verificatore’ descritta nel paragrafo successivo.

Inoltre, le procedure di gestione del sistema prevedono un elenco di controlli manuali effettuati direttamente dal Responsabile del servizio della conservazione o dai suoi incaricati.

5.1.10.5 La verifica di leggibilità

Il Responsabile del servizio della conservazione, come descritto nell'art. 7 comma 1 lettera f) “assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità” dei documenti conservati con procedure automatiche e manuali, al fine di prevenire il rischio che i documenti non possano essere visualizzabili, inficiando il mantenimento della loro validità legale nel tempo.

L’apposita procedura, detta verificatore, esegue il 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 inviato dal soggetto Produttore. Se la procedura non registra differenze tra i due hash, il documento è leggibile ed inalterato rispetto a quanto trasmesso dal Produttore.

Vengono eseguiti i seguenti passi operativi:

- verifica della validità della firma digitale e della marcatura temporale apposte all'atto della conservazione dal Responsabile del servizio della conservazione sul file IPdA se presenti, verifica della firma digitale e della marcatura temporale del file;
- calcolo dell'impronta del documento e confronto con quella contenuta all'interno del file IPdA,
- generazione di un report che viene automaticamente sottoposto alla conservazione nell'area dedicata al Responsabile del servizio della conservazione azione (quindi a sua volta firmato e marcato temporalmente dal Responsabile del servizio della conservazione stesso).

La procedura appena descritta viene applicata sia sul supporto primario sia su quello secondario. In caso di anomalie, se il documento risulta corrotto in uno dei due repository, il sistema tenta il ripristino automatico con il dato presente nel repository integro. Se invece ambedue le copie sono alterate, viene inviato un alert al Responsabile del servizio della conservazione, che tenterà il ripristino manuale partendo da un'altra sorgente (per esempio le copie di backup). Se nessuna sorgente è disponibile viene redatto un Verbale di Incidente, sottoscritto e conservato dal Responsabile del servizio della conservazione per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.

Periodicamente, il sistema produce dei report di sintesi dell'attività di verifica svolta.

In aggiunta, il Responsabile del servizio della conservazione e i suoi incaricati sono dotati di apposita strumentazione con credenziali di accesso dedicate che consentono l'accesso per la visualizzazione e la verifica di tutti i documenti conservati.

Oltre alla verifica dell'integrità binaria, il Responsabile del servizio della conservazione procede periodicamente ad una verifica campionaria di leggibilità del parco documentale conservato utilizzando uno specifico tool progettato allo scopo. Il tool sceglie casualmente un numero configurabile (tipicamente 20) di documenti presenti nel sistema di conservazione.

Il Responsabile del servizio della Conservazione estrare i documenti presenti in questa lista e, se necessario, i relativi visualizzatori e ne prende visione, verificandone pertanto il contenuto.

Viene redatto un verbale che attesta l'elenco dei documenti visualizzati. Tale verbale è successivamente sottoscritto e conservato dal Responsabile del servizio della Conservazione nell'area appositamente creata nel sistema di conservazione.

5.1.10.6 I Controlli

Oltre ai monitoraggi appena descritti, il sistema di conservazione implementa numerosi sotto-processi dediti al controllo del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al personale incaricato dell'amministratore del sistema.

I controlli effettuati si distinguono nelle due tipologie: controlli di processo e controlli periodici.

5.1.10.7 Controlli di processo di progettazione e sviluppo dei servizi

L'organizzazione garantisce che non vengano rilasciati prodotti/servizi per i quali non siano state completate le attività di controllo della qualità citate nelle relative procedure di rilascio.

5.1.10.8 Monitoraggio e registrazioni durante il ciclo produttivo

Lungo l'intero ciclo produttivo si effettuano i controlli al fine di verificare la conformità del prodotto e del processo a quanto previsto dalle procedure applicabili.

Nelle procedure “PR/235 Progettare e sviluppare un servizio informatico InfoCert” e “PR/225-Change Management InfoCert” sono indicate le fasi specifiche per i controlli, i test e le misurazioni del prodotto/servizio in termini di ciclo di vita, tecniche, metriche del SW, gestione dei controlli, dello “sforzo/effort”, tenuta in controllo dei costi e dei tempi di realizzazione, la definizione dei mezzi e delle risorse necessarie .

Il prodotto/servizio è oggetto di un processo progressivo di accettazione: le registrazioni documentano la conformità del prodotto ai criteri di accettazione e indicano la persona che autorizza il rilascio.

Il prodotto/servizio sarà predisposto per la consegna al cliente ad esito positivo delle prove, controlli e collaudi. I prodotti che non superano le prove, i controlli e i collaudi sono sottoposti alla procedura per il trattamento dei prodotti non conformi così come descritto nel relativo capitolo del presente manuale.

5.1.10.9 Monitoraggio e registrazioni per collaudo finale

Il prodotto/servizio corrispondente ai requisiti contrattuali è oggetto di un processo progressivo di accettazione che viene attivato in occasione di ogni consegna ufficiale al Cliente, o di una accettazione globale fatta alla fine del processo produttivo secondo quanto previsto dalla procedura PR/215 – Impostare e condurre attività progettuali InfoCert.

5.1.10.10 Controlli periodici

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

La struttura si avvale di un gruppo di lavoro trasversale all'azienda ed effettua la raccolta dei dati relativi al funzionamento dei servizi.

Il gruppo si riunisce con una periodicità mensile al fine di individuare le cause dei malfunzionamenti registrati nel periodo, analizzare le soluzioni contingenti adottate per il superamento del problema e sviluppare eventuali proposte per rimedi strutturali.

5.1.10.11 Riesame del sistema

Ad ogni semestre il Responsabile del servizio della conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).

Per ogni riunione è redatto un apposito verbale contenente i punti trattati e la sintesi della discussione; il verbale viene mandato in conservazione in un’apposita area di conservazione nella quale sono contenuti anche tutti gli eventuali verbali di incidente redatti nel corso del trimestre

oggetto di riesame. Inoltre, il verbale e il relativo token vengono archiviati nella Intranet aziendale secondo le procedure previste dal sistema di gestione della qualità

5.1.10.12 Auditing generale del sistema

Il Piano delle verifiche ispettive è definito annualmente dal gestore della qualità e approvato dal Rappresentante della direzione.

Le verifiche ispettive sono condotte all'interno della società sulla base della procedura "MG/325 Gestire Verifiche Ispettive InfoCert" volte a determinare se i processi aziendali ed i risultati ottenuti:

- sono orientati alle politiche per la qualità e al raggiungimento degli obiettivi
- sono in accordo con quanto previsto nei documenti di riferimento
- sono compliance alla normativa di riferimento
- sono compliance agli standard adottati dal sistema di conservazione
- sono attuate efficacemente
- sono idonee al conseguimento degli obiettivi della Qualità e miglioramento servizi

In ogni processo aziendale, le modalità di audit sono improntate alle indicazioni dello standard UNI EN ISO 19011 ed hanno per oggetto:

- strutture organizzative
- risorse utilizzate
- procedure
- processi
- prodotti e i risultati dell'attività
- documentazione
- addestramento
- le segnalazioni dei clienti e terze parti

Gli audit sono coordinati dall'Esecutivo Qualità ed eseguiti direttamente o da personale interno o esterno qualificato e debitamente addestrato.

Oltre alle verifiche ispettive sopra descritte indirizzate al Sistema gestione Qualità, sono pianificati e condotti Audit su tutti gli altri componenti del Sistema di Gestione Integrato (SGSI-ISO 27001, SMS-ISO 20000, SGA-ISO14001, Verifiche di interoperabilità condotte da Agid, Privacy, Sicurezza Fisica, M231/01 ecc.).

Relativamente al SGA-ISO14001 l'attività di audit comprende anche la verifica di conformità legislativa.

Il processo prevede inoltre la gestione controllata di tutti gli Audits esterni svolti dagli Enti istituzionali, relativi ai Sistemi di Gestione ed ai Prodotti/Servizi certificati.

A fronte di non conformità rilevate in sede di verifica ispettiva, il responsabile della Struttura Organizzativa valutata definisce un piano di attuazione delle Azioni Correttive o Migliorative richieste.

Il responsabile delle verifiche e ispezioni (auditing) pianifica e implementa processi di audit che coinvolgono aspetti di processo, organizzazione, tecnologici e logistici. L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto, alla documentazione generale del sistema, ai principi che ispirano il sistema qualità e al presente Manuale della Conservazione.

L'audit è un processo fondamentale per lo screening del sistema, in quanto consente l'individuazione delle aree critiche d'intervento e la pianificazione dei necessari interventi sul sistema, ragion per cui è svolto periodicamente.

5.1.10.13 Incident management

L'ambito completo del processo si applica alla gestione degli incidenti informatici che possono interessare uno o più servizi tecnologici eventualmente interconnessi ed è formalmente descritto dalla procedura PR455-Incident Management InfoCert. La procedura definisce anche la metodologia di assegnazione della gravità di un incidente e della relativa priorità di gestione in base alla matrice di analisi di impatto/urgenza effettuata utilizzando le informazioni sul servizio di riferimento e sui relativi SLA del servizio o nelle istruzioni /policy specifiche relative alla sicurezza informatica.

PRIORITA'			
Urgenza → / Impatto ↓	**ALTA**	**MEDIA**	**BASSA**
ALTO	critica	alta	media
MEDIO	alta	media	bassa
BASSO	media	bassa	molto bassa

L'impatto è definito in base alla BIA [Business Impact Analisys] del servizio.
L'urgenza è dettata dallo SLA di disponibilità del servizio.

Il processo di gestione degli incidenti, condotto secondo le raccomandazioni delle Best Practice ITIL e in conformità alle norme ISO 27001, si focalizza sulle modalità di gestione e di ripristino tempestivo degli incidenti informatici. La funzione InfoCert coinvolta in tale processo è il Service Desk che opera anche come interfaccia per gli altri processi, quali il Change Management, il Problem Management e il Configuration Management.

Il modello organizzativo prevede che il supporto specialistico sistemistico sia fornito dalla funzione di Service Desk InfoCert (SD) che gestisce il ciclo di vita dell'incidente con lo strumento per la tracciatura dell'evento e che si avvale della collaborazione di tutte le strutture aziendali coinvolte.

Il processo d'incident è supportato dall'attività di Problem Management (procedura PR456) che mira a ridurre gli impatti negativi a seguito di incidenti che possono essere provocati da errori/malfunzioni nelle infrastrutture IT e a prevenire il verificarsi e il ripetersi di tali errori.

A tale scopo il Problem Management cerca di individuare la causa degli incidenti e ne attua le opportune azioni preventive, correttive e/o migliorative.

La gestione dei problemi può essere sia reattiva che proattiva. Reattiva quando sono risolti problemi a seguito di uno o più incidenti. La gestione proattiva riguarda invece l'identificazione e la risoluzione di problemi prima che si verifichino degli incidenti.

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

Il Responsabile del servizio della conservazione mantiene il verbale degli incidenti e delle contromisure attuate, che divengono oggetto della successiva riunione di riesame e sono inviate al sistema di conservazione.

5.1.11 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

La conservazione avviene su supporto primario e su supporto secondario. Come descritto in altri punti del presente manuale, tali supporti sono magnetici ad alte capacità e performance, che garantiscono la ridondanza interna del dato. E' inoltre eseguito un backup periodico su tape magnetico.

Oltre a queste modalità, possono essere generati anche duplicati o copie su supporto ottico, su specifica richiesta del Cliente. Tali copie sono tipicamente inviate al Cliente, oppure mantenute da InfoCert.

Le copie possono essere generate automaticamente alla fine del processo di conservazione, oppure on-demand in qualsiasi momento. Nel secondo caso il Cliente inoltra la richiesta ai suoi riferimenti abituali (help desk o account) che poi provvedono alla veicolazione verso gli operatori interni.

La creazione di copie in caso di adeguamento del formato rispetto all'evoluzione tecnologica sarà presa in carico dal Responsabile del servizio della conservazione e dalle figure professionali coinvolte nel processo di conservazione in base alle specifiche del formato in questione e al know-how tecnologico a disposizione. A fronte di questa analisi sarà progettata una soluzione di concerto con il soggetto Produttore del formato più idoneo per permettere la leggibilità del documento conservato.

InfoCert valuta anche la possibilità di generare supporti alternativi all'ottico per specifiche esigenze della clientela. Tali supporti sono esclusivamente generati e inviati al Cliente.

5.1.12 Gestione di rettifica, cancellazione e scarto

5.1.12.1 Rettifica e cancellazione di un pacchetto di archiviazione

Il sistema è configurato in modo da consentire la rettifica e cancellazione logica dei pacchetti di archiviazione dal database.

La rettifica e la cancellazione logica possono essere richieste solo dal Soggetto Produttore che, utilizzando le funzioni messe a disposizione dal sistema di gestione,; il Soggetto Produttore è identificato mediante certificato di autenticazione.

In risposta all'invocazione del sistema di rettifica/cancellazione si otterrà il file IPdA che attesta il momento dell'avvenuta rettifica/cancellazione del documento indicato.

5.1.12.2 Responsabilità nel processo di rettifica e cancellazione

Di seguito è riporta la tabella di sintesi del processo di rettifica e cancellazione dal sistema di conservazione, inoltre per ognuna delle attività elencate saranno descritte le attività di dettaglio, seguendo lo schema: input\dettaglio delle attività\output.

Responsabilità **Attività**	**Responsabile del servizio della Conservazione**	**Responsabile della funzione archivistica**	**Responsabile del trattamento dei dati personali**	**Responsabile della sicurezza dei sistemi per la conservazione**	**Responsabile dei sistemi informativi per la conservazione**	**Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
1. Ricerca del token relativo al documento da rettificare/cancellare (*)						
2. Creazione del file dei parametri di rettifica/cancellazione (*)						
3. Invio della richiesta di rettifica/cancellazione al sistema di conservazione (*)						
4. Validazione delle informazioni presenti nel file dei parametri di rettifica/ cancellazione	**R**					
5. Rettifica/cancellazione logici del file, creazione del file IPdA, marcatura temporale e firma digitale dello stesso	**R**					

(*) Le Responsabilità sono in capo al soggetto produttore e definite nelle specifiche contrattuali.

ATT.1 Ricerca del token del pacchetto di archiviazione da rettificare/cancellare

INPUT	Ricerca del token
	Ricerca negli archivi del sistema del token relativo al documento da rettificare/cancellare attraverso le procedure previste dai sistemi di gestione.
OUTPUT	*Token* trovato

ATT.2 Creazione del file dei parametri di rettifica/cancellazione

INPUT	*File dei parametri di rettifica e cancellazione da creare*
	Ricerca negli archivi del sistema del token relativo al documento originale da rettificare/cancellare
	Generazione del file XML dei parametri di rettifica e cancellazione secondo le specifiche contenute in [1].
OUTPUT	*File dei parametri di rettifica e cancellazione creato*

ATT.3 Invio della richiesta di rettifica e cancellazione al sistema di conservazione

INPUT	*Richiesta di rettifica e cancellazione da preparare*
	Invocazione del servizio di rettifica e cancellazione da parte del sistema di gestione, secondo le specifiche descritte in [1].
	Autenticazione al sistema LegalDoc mediante credenziali (username/password) e ottenimento dell'identificativo di sessione (ldSessionId)
	Invio della richiesta al Soggetto Produttore (comprensiva del file dei parametri di rettifica/cancellazione)
OUTPUT	*Richiesta di rettifica e cancellazione preparata*

ATT.4Validazione del file dei parametri di rettifica e cancellazione

INPUT	*Richiesta da validare*
	Ricezione della richiesta di rettifica e cancellazione
	Verifica dei valori indicati nella richiesta di rettifica e cancellazione

	Ricerca del documento da rettificare/cancellare con i parametri indicati nella richiesta
OUTPUT	*Richiesta validata*

ATT.5Rettifica e Cancellazione logico del file

La fase comprende la creazione del file IPdA, la marcatura temporale , la firma digitale dello stesso ed invio al soggetto Produttore

INPUT	*Documento da rettificare/cancellare*
	Modifica dello stato del documento rettificato da “conservato” a “rettificato/cancellato” nel database del sistema di conservazione.
	Creazione del file XML IPdA secondo le specifiche descritte in [1]
	Invio dell'esito e del file IPdA al soggetto Produttore
OUTPUT	*Documento rettificato/cancellato*

5.1.12.3 Versamento e scarto dei documenti

In ambito Pubblica Amministrazione, per determinare i tempi di conservazione e di scarto è obbligatorio l’adozione, da parte del Soggetto Produttore, gli strumenti del Massimario di scarto collegato con il Titolario o piano di classificazione, previsti nel Manuale di gestione dell’Ente.

Il Soggetto Produttore 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 (articoli 21, 40 e 41).

Lo scarto dei file avviene mediante cancellazione del documento conservato.

L’eliminazione del documento, che non permetterà di riottenere mai più lo stesso contenuto, è pilotata dalla lista dei documenti da cancellare fornita dal Soggetto Produttore debitamente firmata. La lista sarà essa stessa oggetto di conservazione.

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 della conservazione mantiene traccia delle richieste di scarto ricevute e correttamente evase, 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.

5.1.13 Processo di richiesta presenza di un pubblico ufficiale;

All'art. 7 comma 1 lettera j) del DPCM del 3 dicembre 2013 si sottolinea come il Responsabile del servizio della conservazione “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".

Inoltre nel Manuale della conservazione ai sensi dell'art. 8 comma 2 letta k) deve riportare "le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento".

I casi in cui è previsto il suo coinvolgimento sono descritti nel Codice dell'Amministrazione Digitale:

Art 22 "Copie informatiche di documenti analogici" D.lgs. 82 del 2005 e suoi successivi aggiornamenti

[..]

1. I documenti informatici contenenti copie di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata. La loro esibizione e produzione sostituiscono quella dell'originale.

2. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.

3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

4. Le copie formate ai sensi dei commi 1, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.

5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

6. Fino alla data di emanazione del decreto di cui al comma 5 per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

L'attività primaria richiesta l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico che si esplicita in una dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.

5.1.14 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

Nel caso il Soggetto Produttore decidesse di rescindere il contratto di affidamento del servizio di conservazione, ovvero siano scaduti i termini di legge che impongono la conservazione obbligatoria, il Responsabile del servizio della conservazione provvede a comunicare al Soggetto Produttore la lista dei documenti conservati.

Nel caso di rescissione del contratto di affidamento del servizio di conservazione, il Responsabile del servizio della conservazione provvede a consegnare al Soggetto Produttore i documenti conservati su adeguati supporti.

Gli archivi di conservazione generati dal sistema InfoCert sono conformi allo standard di interoperabilità UniSincRO L'interrogazione di tali archivi restituisce le informazioni secondo il suddetto standard.

L'adozione di tale standard permette l'interoperabilità e la trasferibilità dei dati in modo semplificato.

5.1.15 Le normative in vigore nei luoghi dove sono conservati i documenti.

5.1.15.1 Il quadro normativo

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

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

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

Nel frattempo, è stato completato il quadro normativo relativo al documento informatico, alla firma digitale e alla fattura elettronica (a titolo non esaustivo si cita il Testo Unico sulla documentazione amministrativa – TU 445/2000, il Decreto del Presidente del Consiglio dei Ministri 8/02/1999 poi sostituito dal Decreto del Presidente del Consiglio dei Ministri del 13/01/2004, le numerose deliberazioni AIPA – poi divenuta CNIPA, ora AgID, il Decreto Ministero Economia e

Finanze 23 gennaio 2004 e il Decreto Legislativo 52 del 20 febbraio 2004, relativi a specifiche tipologie di documenti).

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

Infine il DPCM 03/12/2013 (GU n. 59 del 12-03-2014) Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005, traccia le regole per la conservazione a norma, andando ad abrogare la Deliberazione CNIPA 11/2004. Si precisa che i sistemi di conservazione già esistenti alla data di entrata in vigore del presente decreto sono adeguati entro e non oltre 36 mesi dall'entrata in vigore del decreto 03/12/13 secondo un piano dettagliato. Fino al completamento di tale processo restano validi i sistemi di conservazione realizzati ai sensi della deliberazione CNIPA n. 11/2004. Il Responsabile della conservazione valuta l'opportunità di riversare nel nuovo sistema di conservazione gli archivi precedentemente formati o di mantenerli invariati fino al termine di scadenza di conservazione dei documenti in essi contenuti, così come previsto dall'Art. 14 del DPCM 03/12/13.

5.1.15.2 Principali riferimenti normativi

1) *Decreto del 17 giugno 2014 del Ministero dell'Economia e delle Finanze* – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto.
2) *Il Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 (GU n. 59 del 12-03-2014)* Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005, traccia le regole per la conservazione a norma, andando ad abrogare la Deliberazione CNIPA 11/2004.
3) *Decreto del Presidente del Consiglio dei Ministri* 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 *(GU n.117 del 21-5-2013).*
4) *Decreto Legislativo del 30 dicembre 2010* – Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.
5) *Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009* – Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.
6) *Decreto-Legge 29 novembre 2008, n. 185, coordinato con la legge di conversione 28 gennaio 2009, n. 2 – Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale* – Modifiche al CAD in materia di copie informatiche di documenti analogici, modifiche al Codice Civile in materia di documentazione informatica.

7) *Decreto Legislativo del 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale* – Testo che rappresenta la base per tutti i successivi interventi che verranno in tema di uso dei documenti digitali. In dettaglio si definiscono nuovamente i ruoli e le caratteristiche dei documenti informatici e se ne amplia l'utilizzo; in particolare, la PA vede imporre un uso delle tecnologie informatiche e la pressoché totale dematerializzazione dei documenti nei rapporti tra cittadini, imprese e pubblica amministrazione.
8) *Deliberazione CNIPA n. 11 del 19 febbraio 2004* – Regole tecniche per la riproduzione e conservazione su supporto ottico idoneo a garantire al conformità dei documenti agli originali.
9) *Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche* – Codice in materia di Protezione dei Dati Personali.
10) *Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445* – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. Testo coordinato con le modifiche apportate dal D.Lgs 23 gennaio 2002, n. 10 e dal DPR 7 aprile 2003, n. SQ01-00-02 Procedura per la gestione della documentazione. Questo DPR è stato per la maggior parte sostituito dal Codice dell'amministrazione digitale in vigore dal 1° gennaio 2006.

5.1.15.3 La conservazione digitale dei documenti

L'implementazione e la gestione del processo di conservazione digitale si avvale di numerosi strumenti ed elementi, regolati da discipline apposite che vanno raccordate alla disciplina generale della conservazione.

Di seguito si richiamano i principali strumenti ed elementi:

- ***Documento informatico***: è una realtà immateriale e il tipo di supporto fisico sul quale esso è registrato è irrilevante per la natura del documento stesso. Del documento informatico, a differenza di quello cartaceo, è possibile avere molteplici esemplari, tutti giuridicamente rilevanti e aventi identico valore legale (detti 'duplicati'). Per le sue caratteristiche, il documento informatico necessita di strumenti di validazione informatica efficaci e sicuri affinché ne siano assicurate, 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 amministrativo informatico***: ogni rappresentazione informatica di atti, anche interni formali, di pubbliche amministrazioni utilizzati ai fini di attività amministrative.
- ***Documento analogico***: in generale, è quello che per la sua formazione utilizza una grandezza fisica che assume valori continui, come, ad esempio, le tracce continue su carta per il documento cartaceo o le immagini continue per il film. Il supporto fisico su cui si può formare il documento analogico non è necessariamente quello cartaceo, ma può essere film, lastra o pellicola radiologica, microfiche e microfilm, nastri audio e video.
- ***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.

- ***Supporto di memorizzazione***: il supporto può essere ottico o non ottico, in quanto il documento esiste a prescindere dal supporto su cui è memorizzato. Già la deliberazione CNIPA 11/2004, secondo un'impostazione poi superata con il DPCM 3 dicembre 2013, autorizzava l'utilizzo di un qualsiasi tipo di supporto di memorizzazione che consenta la registrazione mediante tecnologia laser (dischi ottici WORM e CD-R, dischi magneto-ottici o DVD).
- ***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 ripudio.
- ***Validazione temporale***: per stabilire il momento temporale in cui un documento informatico è stato formato è necessario attribuirgli una "validazione temporale", ovvero 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.
- ***Pacchetto di archiviazione***: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3/12/2013 e secondo le modalità descritte in questo Manuale.
- ***Pacchetto di distribuzione***: pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
- ***Pacchetto di versamento***: pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e descritto in questo Manuale.

5.1.15.4 Dalla deliberazione CNIPA 11 del 19 febbraio 2004 alle Regole Tecniche di cui al DPCM 3 dicembre 2013

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

Il Decreto, che sostituisce integralmente la precedente Deliberazione 11 del 2004, aggiorna le regole tecniche per la riproduzione e conservazione dei documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali, come previsto all'articolo 6, commi 1 e 2, del TU delle disposizioni legislative e regolamentari in materia di documentazione amministrativa di cui al DPR 28 dicembre 2000, n. 445.

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

5.1.15.5 Il responsabile della conservazione

Come già per la deliberazione AIPA n. 42/2001, la deliberazione CNIPA n. 11/2004 (art. 5) e le Regole Tecniche del DPCM 03/12/2013 enfatizzano la figura del Responsabile del servizio 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 attributi 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.

In merito al comma l) InfoCert si rende disponibile alla configurazione del servizio di versamento in base a specifici accordi contrattuali che saranno definiti tra le parti in base alla normativa vigente.

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

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

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

5.1.15.6 La conservazione digitale dei documenti rilevanti ai fini tributari: Il decreto del Ministro dell'Economia e delle Finanze del 17 giugno 2014

Il decreto del Ministro dell'Economia e delle Finanze 17 giugno 2014 interviene ad aggiornare e sostituire il precedente Decreto di riferimento –a distanza di oltre dieci anni- 23 gennaio 2004. Esso dispone le modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto e riprende le disposizioni in materia di documento informatico, firma elettronica e conservazione di cui al DPCM 22 febbraio 2013 e al DPCM 3 dicembre 2013.

Il Decreto all'art. 2 ribadisce che :

Ai fini tributari, la formazione, l'emissione, la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione, l'esibizione, la validazione temporale e la sottoscrizione dei documenti informatici, avvengono nel rispetto delle regole tecniche adottate ai sensi dell'art. 71 del decreto legislativo 7 marzo 2005, n. 82, e dell'art. 21, comma 3, del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633, in materia di fatturazione elettronica. I documenti informatici rilevanti ai fini tributari hanno le caratteristiche dell'immodificabilità dell'integrità, dell'autenticità e della leggibilità, e utilizzano i formati previsti dal decreto legislativo 7 marzo 2005, n. 82, dai decreti emanati ai sensi dell'art. 71 del predetto decreto legislativo ovvero utilizzano i formati scelti dal responsabile della conservazione, il quale ne motiva la scelta nel manuale di conservazione, atti a garantire l'integrità, l'accesso e la leggibilità nel tempo del documento informatico.

Per gli stessi documenti devono, inoltre, essere garantiti un minimo di parametri obbligatori che consentano le funzioni di ricerca ed estrazione delle informazioni (articolo 3, comma 1, lettera b)). in relazione a: nome, cognome, denominazione, codice fiscale, partita I.V.A., data e relative associazioni logiche. Nulla osta, dopo aver rispettato il nucleo minimo di chiavi previste per legge, di prevederne di ulteriori.

Per il pieno rispetto delle condizioni poste dal Decreto, è necessario produrre documenti che non contengano macroistruzioni o altro codice eseguibile, ossia che rientrino nella categoria di "documento statico non modificabile", adottando il formato più adeguato alle esigenze gestionali (ad esempio il formato PDF-A o il formato TXT).

Successivamente, si procede alla memorizzazione del documento su un idoneo supporto e si attua la procedura per la conservazione. La procedura termina con l'apposizione della firma digitale del Responsabile del servizio della conservazione, che attesta la correttezza del processo, e della marca temporale (in luogo del riferimento temporale previsto per i documenti senza valenza

tributaria), che dà certezza al momento temporale, sull'Indice del pacchetto di archiviazione (art. 3 comma 2).

La procedura è analoga nel caso di documenti analogici acquisiti dal sistema informatico, eccezion fatta per l'iniziale trasformazione del documento in formato digitale mediante uno scanner. Nel caso in cui il documento analogico fosse in origine un documento originale unico, ovvero un documento per il quale non sia possibile risalire al contenuto neppure attraverso altre scritture o documenti di cui sia obbligatoria la conservazione anche presso terzi, è richiesto l'ulteriore intervento da parte di un pubblico ufficiale o da un notaio.

La cadenza per la conservazione digitale dei documenti rilevanti ai fini tributari non prevede più una periodicità almeno quindicinale per le fatture, che sono conservate entro tre mesi dalla scadenza del termine per la presentazione delle dichiarazioni annuali, secondo il Decreto.

6 Sicurezza del sistema di conservazione (Articolo 12)

La sicurezza del sistema di conservazione è gestita il conformità al Sistema di Gestione della Sicurezza delle Informazioni InfoCert (SGSI) .

Nell'allegato "Processo MG115/TB02_Processi e Responsabilità_Integrated Management System" sono riportati i processi, le responsabilità aziendali e le procedure che descrivono il Modello SGSI :

- MG165 (Modello Gestione Sicurezza delle Informazioni)
- MG685 (Gestire la tutela dei dati personali)
- MG605 e relative policy (Gestire la sicurezza delle informazioni)

6.1 Gestione delle procedure di sicurezza e di tracciabilità

6.1.1 Sicurezza degli accessi

Il sistema di conservazione è protetto da firewall, che impedisce l'accesso agli utenti non autorizzati. I sistemi firewall sono configurati in alta affidabilità, ovvero sono formati da coppie di macchine indipendenti collegate tra loro e gestite, tramite apposito software, in modo che in caso di guasto di una delle macchine sia sempre disponibile una macchina di back-up.

Le regole definite sui firewall sono progettate in base ai principi di default deny (è consentito solo quanto è strettamente necessario al funzionamento dell'applicazione) e defense in depht (vengono organizzati livelli successivi di difesa, prima a livello di rete e poi a livello di sistema).

Il log del firewall registra tutti gli accessi e le connessioni che lo interessano, memorizzando in particolare gli IP di provenienza, la data e l'ora della connessione, il protocollo utilizzato, l'esito della richiesta.

6.1.2 Modalità di accesso al sistema

In fase di attivazione del sistema, la CA di InfoCert fornisce ad ogni Soggetto Produttore i relativi codici account (username/password) mediante i quali il Soggetto Produttore che accede al sistema è identificato univocamente.

Gli estremi dell'account sono inviati attraverso la casella di Posta Elettronica Certificata generata in fase di attivazione: la PEC fornisce certezza dell'invio, della ricezione, del mittente e del destinatario di informazioni così rilevanti per la sicurezza degli accessi.

6.1.3 Tracciabilità delle operazioni

Il sistema di conservazione è costituito da numerose componenti, ciascuna dotata di un proprio file di log applicativo nel quale sono tracciate tutte le operazioni eseguite dal componente e le altre informazioni che permettono di tenere traccia delle attività svolte e facilitare la diagnosi di eventuali comportamenti anomali del sistema.

Nell'ambito dei processi di LegalDoc per ogni richiesta sono disponibili le informazioni su tutti i passi procedurali effettuati tra cui in particolare le informazioni relative alla data/ora di elaborazione, alla tipologia della richiesta, all'identificativo del Produttore e della sessione (ldsessionid), al file costituente il documento e al suo identificativo (token).

Un apposito servizio centralizza i file di log di tutte le applicazioni; tutti i file di log e il database dei metadati di processo vengono sottoposti a periodici processi di back-up.

La sincronizzazione di tutti i sistemi sul tempo campione proveniente dalla fonte esterna prevista dalla legge consente la ricostruzione della corretta sequenzialità di accadimento delle operazioni registrate nei file di log.

6.2 La protezione dei dati personali

Ai sensi dell'articolo 29 del D. L.vo n. 196/2003 "*Codice in materia di protezione dei dati personali*", InfoCert S.p.A. è nominata Responsabile dei trattamenti dei dati necessari all'esecuzione del servizio.

In particolare, anche in considerazione del ruolo di Responsabile del servizio della conservazione ricoperto, i compiti affidati ad InfoCert S.p.A. 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 scarto 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. L.vo 196/2003 per i dati relativi al contratto è resa ai soggetti Produttori nell'atto di affidamento allegato al materiale contrattuale sottoscritto, ove viene altresì agli stessi consentito di esprimere il consenso per gli ulteriori trattamenti indicati.

6.3 Sicurezza fisica e logica del sistema

Il sistema di conservazione è protetto da un misure di sicurezza fisiche e logiche idonee a garantire la sicurezza dei sistemi, delle informazioni e dei documenti secondo tre parametri fondamentali:

- *integrità*: le informazioni sono protette contro il rischio di scarto o alterazione da parte di soggetti o procedure non autorizzate, o a causa di eventi accidentali;
- *riservatezza*: un utente non autorizzato non può, volontariamente o involontariamente, acquisire o dedurre dal sistema informazioni che non è autorizzato a conoscere;
- *disponibilità*: le informazioni sono accessibili solamente al soggetto autorizzato, nei modi e nei tempi previsti dalle policy.

L'azienda definisce la politica di sicurezza, che promuove e individua i criteri generali di sicurezza, definendo i ruoli, le responsabilità e le risorse assegnate. Le procedure operative attuano la politica di sicurezza, descrivendo le contromisure definite ed attuate per far fronte alle diverse classi di rischio individuate ed analizzate.

Alla base della politica e delle procedure sono posti i due principi fondamentali della *separazione dei ruoli* e del minimo privilegio.

Nel rispetto del primo principio è stabilita una netta separazione di ruolo tra i soggetti che definiscono e gestiscono il sistema di sicurezza e gli utenti operativi; inoltre, in ossequio al principio del *minimo privilegio*, agli utenti del sistema sono assegnati solamente i diritti necessari per portare a termine l'operazione per la quale sono abilitati.

Il sistema di sicurezza di InfoCert rispetta pienamente il principio di adozione di misure minime di sicurezza previsto dal Decreto Legislativo 30 giugno 2003 numero 196 “Codice in materia di protezione dei dati personali”; ove queste non fossero idonee a garantire una accettabile copertura dai rischi, sono adottate misure più stringenti ed adeguate.

L'azienda è impegnata nel costante aggiornamento del sistema in funzione dell'evoluzione delle minacce, del sistema, della normativa e della tecnologia disponibile sul mercato.

Misure specifiche di sicurezza sono definite ed implementate per la Certification Authority, di cui il sistema di conservazione richiama i servizi.

Si rimanda a [6], documento riservato ad uso interno, per la descrizione dettagliata delle misure fisiche, logistiche e logiche, dei processi attuati e della tecnologia utilizzata nelle diverse fasi di sviluppo, implementazione, gestione, audit e revisione del sistema di sicurezza InfoCert.

6.4 Caratteristiche del data center InfoCert

InfoCert nel proporre i propri servizi, sia architetturali sia di rete, ritiene di poter caratterizzare l'offerta attraverso una serie di elementi e modalità gestionali tecnico operative e livelli di sicurezza fisica ed informatica ai massimi livelli disponibili sul mercato.

Next Generation Data Center: il data center InfoCert, di recente realizzazione, è stato progettato seguendo alcuni principi fondamentali che permettono di erogare, con elevati standard di disponibilità e sicurezza i servizi di business:

- ampia adozione di tecnologie hardware contraddistinte da una scalabilità orizzontale (blade server); queste piattaforme server permettono di contenere i consumi energetici senza alcuna penalizzazione prestazionale;
- ampia adozione di tecnologie di virtualizzazione contraddistinte da elevati standard di disponibilità dei sistemi, flessibilità gestionale e da costi scalabili (dimensionamento dei server virtuali allineate alle necessità del business); le tecnologie di virtualizzazione sono abilitanti al "libero posizionamento" del servizio erogato in base a parametri di economicità di esercizio o di necessità prestazionali, addirittura variabili nel tempo;
- ampio utilizzo di componenti software open source caratterizzate da bassi impatti economici di investimento e da prestazioni in linea con quelle offerte da strumenti di mercato.

6.5 Ubicazione dei data center

6.5.1 Data Center primario

All'interno del Data Center di InfoCert sono collocati i sistemi e gli apparati elettronici di proprietà InfoCert e le apparecchiature dei Clienti che fruiscono dei servizi di Housing/Hosting.

Il Data Center InfoCert si trova presso la sede operativa di Padova, in Corso Stati Uniti 14.

6.5.2 Data Center secondario (DR)

Il sito di Disaster Recovery è ubicato a **Modena, Via F. Malavolti, 5**,ed è connesso al Data Center sopra citato tramite un collegamento dedicato MPLS 50 Mbit/s.

6.6 Disaster Recovery

Il processo di gestione della disponibilità dei servizi [MG745 – Availability Management InfoCert] definisce i parametri di riferimento per il controllo della capacita' di un servizio IT o di un componente di un servizio IT di esplicare le proprie funzioni in un determinato periodo di tempo.

Nello specifico si definiscono:

RTO	Recovery Time Objective, il massimo periodo di tempo entro il quale un processo/servizio deve essere ripristinato

RPO	Recovery Point Objective, il periodo di tempo massimo che può intercorrere tra l'ultimo salvataggio dei dati di un processo/servizio ed il verificarsi dell'evento che causa l'arresto dello stesso

I valori di RTO e RPO sono definiti in funzione della Business Impact Analysis (BIA) InfoCert determina l'impatto sul business conseguente alla indisponibilità delle risorse aziendali (infrastrutture, persone, sistemi informativi, ecc.) .

Per il sistema di Conservazione Sostitutiva InfoCert gli SLA definiti sono:

METRICHE	VALORE
RTO – Tempo Massimo di Ripristino	48h
RPO – Tempo Massimo di Anzianità dei dati	24h
Esecuzione dei Test	1 Test/Anno

6.7 Crisis Management

Il processo di gestione della crisi è inserito nel processo di Avalability Management e definisce tutte le prime fasi della gestione di una crisi partendo dalla dichiarazione di un'emergenza fino all'intera gestione della crisi.

Nello specifico nella procedura MG745 – Availability Management InfoCert è definita l'organizzazione di riferimento, i componenti e i ruoli e le attività che questi devono ricoprire durante il periodo di emergenza; la crisi viene gestita dal Gruppo Coordinamento Emergenza [GCE] che interviene a fronte degli eventi disastrosi succitati o di altri, derivanti dall'escalation di incidenti di sicurezza.

6.8 Contingency Plan

Il documento di "Contingency Plan" riporta le procedure dettagliate da seguire nella fase di Recovery; costituisce il vero e proprio "Red Book" o manuale delle procedure di Emergenza; nel suo interno la parte più corposa è quella correlata con l'infrastruttura tecnologica messa in essere.

Nell'ambito del Contingency Plan hanno particolare rilevanza i seguenti documenti:

- **Schema grafico procedurale**: uno schema di progetto non troppo dettagliato che evidenzia le fasi, le macro attività e le loro correlazioni temporali significative;

- **Lista Attività**: è il vero e proprio piano di attivazione, suddiviso in fasi, che riporta:
  - Codice – è il codice dell'attività;
  - Descrizione – è una breve descrizione dell'attività;
  - Durata – è il tempo stimato di durata dell'attività;
  - Responsabile – riporta il ruolo del responsabile del gruppo che deve svolgere l'attività;
  - Note/Riferimenti – riporta alcune brevi note relative all'attività ed eventualmente il riferimento alla procedura di dettaglio contenuta negli allegati.

- **Milestone e sincronismi**: in tale documento sono indicati i momenti principali di controllo e verifica ed i sincronismi fra le attività

- **Diario Operativo**: viene compilato nel caso di attivazione del Contingency Plan; possono essere generati più diari ognuno dei quali deve contenere:
  - Check List – è sostanzialmente una copia della lista attività che riporta oltre al codice ed alla descrizione i seguenti campi:
    - Esecutore – il nome del o delle persone che hanno svolto l'attività;
    - Inizio e Fine – gli orari di inizio e fine dell'attività;
    - Note/Problemi – dove vengono riportati eventuali problemi riscontrati o note operative mancanti nel Contingency Plan.
  - Problemi riscontrati – una lista dei problemi incontrati sul processo in generale, cioè relativi a più attività più o meno interdipendenti.
  - Relazione Finale – una relazione che riassume il processo di attivazione del Recovery Site e riporta eventuali differenze nel risultato rispetto a quanto presente nel piano.

- **Procedure di Dettaglio**: sono le procedure dettagliate, richiamate nella Lista Attività, sviluppate qualora le persone tecniche lo ritengano necessario a completamento della descrizione di ogni attività; una procedura di dettaglio deve essere redatta con un adeguato livello di dettaglio, pensando che a seguirla vi siano delle figure con le necessarie competenze tecniche ma assolutamente prive di conoscenza dell'ambiente in cui stanno operando.

6.9 References

Questo documento fornisce i riferimenti a tutti gli attori che possono essere coinvolti nella gestione dell'emergenza. In particolare vi sono i riferimenti a:

- elenchi del personale interno coinvolto;
- contratti di manutenzione ed assicurativi;
- elenchi di società o consulenti esterni in grado di intervenire su specifiche tematiche;
- ogni riferimento o contatto possa esse considerato utile alla gestione di un'eventuale situazione disastrosa.

6.10 Test Specification & Procedures

Riporta la definizione dei test e delle relative procedure da seguire per verificare il corretto funzionamento della soluzione di Disaster Recovery. L'insieme di tutti i test definiti deve coprire tutti i requisiti definiti; per compilare il documento è quindi opportuno partire dai requisiti funzionali e non dalle procedure tecniche di test.

6.11 Comunicazione verso il Cliente

Per incidente, InfoCert, intende una qualunque segnalazione di malfunzione, violazione della sicurezza delle informazioni (in termini di riservatezza, integrità, disponibilità) o altri danni o rischi alle strutture\beni aziendali. Il processo di Incident Management prevede la gestione della procedura della gestione della comunicazione verso il cliente che governa anche la comunicazione su fermi programmati (rilascio aggiornamenti software, aggiornamenti documenti\ manualistica\ modulistica.., rilascio nuovi servizi, aggiornamenti siti web) e comunicazione su fermi non

programmativi, relativi ad incidenti\ malfunzioni gravi\ bloccanti verticali su un servizio o su più sevizi.

Il processo di comunicazione esterna aziendale, di competenza della funzione marketing, ha la responsabilità di raccogliere tutte le informazioni necessarie relative all'incidente in corso e di impostare la modalità più opportuna di composizione della comunicazione e della relativa distribuzione ai destinatari \ clienti.

La gravità dell'incidente è definita dal processo di Incident Management in relazione al suo impatto sul business aziendale.

A fronte di un incidente classificato grave, il gruppo coordinamento d'emergenza[GCE], presieduto dal Direttore Generale, definisce la strategia comunicativa non standard impostando la metodologia comunicativa più adatta al governo della situazione in termini di contenuto di comunicazione, mezzo e tempistica di comunicazione, eventuale escalation informativa e target di riferimento.

Il processo è formalmente descritto dalla procedura aziendale "MG500-Gestire la comunicazione verso l'esterno" come riportato nel documento "MG115/TB02_Processi e Responsabilità_Integrated Management System".

7 Riferimenti contrattuali

Il sistema di conservazione erogato da InfoCert S.p.A. è regolato dai seguenti documenti contrattuali:

1. ***Condizioni Generali di Contratto***: con le sue disposizioni, regola la vendita del sistema di conservazione nelle diverse modalità di erogazione;
2. ***Richiesta di attivazione***: comporta l'adesione al servizio;
3. ***Dati tecnici per l'attivazione***; mediante la quale il Soggetto Produttore fornisce tutte le informazioni necessarie all'integrazione dei sistemi di conservazione nel proprio sistema di gestione;
4. ***Atto di affidamento*****:** rappresenta una formalizzazione dell'affidamento ad InfoCert del processo di conservazione e stabilisce espressamente quali attività di fatto vengano assunte da InfoCert e quali, al contrario, rimangano a carico dell'affidatario;
5. ***Specifiche Tecniche di integrazione*****:** fornisce tutte le informazioni tecniche necessarie ad operare l'integrazione con il sistema di conservazione;
6. ***Impegno alla riservatezza*****:** il documento, consegnato come allegato alle Specifiche Tecniche e firmato dal soggetto Produttore, va riconsegnato ad InfoCert.
7. ***Allegato Tecnico alla conservazione*****:** l'allegato descrive le modalità di fornitura del servizio e l'infrastruttura utilizzata per la sua erogazione.
8. ***Manuale Utente Conservazione*****:** il documento fornisce delle indicazioni sulle procedure utilizzate da InfoCert per la conservazione a norma AgID dei documenti inviati, e risponde alla necessità di documentare il processo dal lato Produttore.
9. ***Descrizione dei codici di errore*****:** fornisce una casistica esaustiva dei messaggi di errore previsti dal servizio di conservazione e delle azioni che è necessario intraprendere per porvi rimedio.

8 Allegati al Manuale della Conservazione

1) SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc
2) AL/NDOC – Allegato Tecnico al Contratto LegalDoc
3) Manuale Utente della Conservazione – Manuale dei processi di conservazione LegalDoc
4) SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc
5) MG115– Manuale della Qualità InfoCert
6) Processo MG/165 – Gestire SGSI - **documento riservato ad uso interno**
7) Procedura PR455 – Incident Management InfoCert
8) **ICERT-INDI-MO -** Manuale Operativo CA
9) MG/CONF – Gestione della configurazione di LegalDoc
10) MG445/DOC-Template Verbale Incidente
11) MU/ESIB Manuale Utente Esibitore LegalDocD.
12) Struttura organizzativa conservazione
13) MG115/TB02_Processi e Responsabilità_Integrated Management System
14) Procedura PR456 – Problem Management InfoCert
15) Procedura MG500 – Gestire Comunicazione verso l'esterno
16) LDOC-Architettura logica e fisica del sistema di conservazione
17) MG-CONF - Gestione della configurazione NDOC

La documentazione relativa alle procedure e/o ai processi interni di InfoCert è resa disponibile solo su esplicita richiesta del Cliente.

La documentazione contrattuale e tecnica è resa disponibile all'atto del perfezionamento dell'accordo di servizio.

La documentazione riservata è resa disponibile solo all'atto del perfezionamento di una specifica non-disclosure agreement.