Secondo Circolo Didattico "Giovanni XXIII" Paternò (CT)
Via Vulcano, 12 - 95047 Paternò (CT)
Tel. 095855485 fax 095841054
Cod. Mec. CTEE06800N; C.F. 80013160876
e-mail: ctee06800n@istruzione.it; ctee06800n@pec.istruzione.it

Manuale di gestione del protocollo informatico, dei flussi documentali e dell'archivio

a norma del d.lgs. 7 marzo 2005, n. 82, del DPCM 3 dicembre 2013 e del DPR 20 dicembre 2000, n.445.

Manuale di gestione del protocollo informatico, dei flussi documentali e dell'archivio

PREMESSA

Il presente manuale disciplina le attività di formazione, registrazione, classificazione, fascicolazione e conservazione sostitutiva relativi alla gestione del protocollo informatico e dei flussi documentali dell'Istituto "II Circolo Didattico Giovanni XXIII" di Paternò (CT).

SEZIONE I – AMBITO DI APPLICAZIONE

1.1 Ambito di applicazione

Il presente manuale è adottato ai sensi degli articoli 3, 4 e 5 del DPCM 03.12.2013 per la gestione delle attività di formazione, registrazione, classificazione, fascicolazione e conservazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti dell'Amministrazione.

1.2 Definizioni e norme di riferimento principali

Ai fini del presente Manuale si intende per:

- CAD; il decreto legislativo 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale e successive modificazioni.
- Regole tecniche per la conservazione: il decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, recante *"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".*
- Regole tecniche per il protocollo: il il decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, recante *"Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005".*
- Testo Unico: il decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Si riportano, di seguito, gli acronimi e i termini utilizzati più frequentemente:

- AOO: Area Organizzativa Omogenea, quale insieme di funzioni e di strutture 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 Testo Unico.
- Delegati: personale dell'Istituto "II Circolo Didattico Giovanni XXIII" di Paternò (CT) incaricato formalmente dal RSP per l'espletamento di funzioni previste dalla normativa vigente in materia di amministrazione digitale.
- MdG: Manuale di Gestione del protocollo informatico, dei documenti e degli archivi.
- OdS: Ordine di Servizio.
- PA: Pubblica Amministrazione.
- PEC: Posta Elettronica Certificata.

- RdP: Responsabile del Procedimento – il dipendente che assume su di sé la responsabilità dell'esecuzione degli adempimenti amministrativi relativi a un procedimento.
- RSP: Responsabile della gestione documentale, ovvero della tenuta del Protocollo informatico, della gestione dei flussi documentali, nonché degli archivi e della conservazione.
- RdU: Responsabile di Ufficio, da intendersi quest'ultimo quale UO.
- Scheda documentale: insieme di dati e metadati associati ad uno specifico documento, con eventuali relativi allegati, che ne tipizzano gli elementi informativi, utili in fase di protocollazione, fascicolazione, conservazione, gestione e ricerca.
- Tab (o pagina): sezione della scheda documentale con un insieme di informazioni e metadati relativi al documento informatico.
- UOP: Unita Organizzativa di registrazione di Protocollo – identifica l'ufficio che svolge attività di registrazione di protocollo.
- UO: ai sensi della normativa di riferimento, corrisponde alla Unità Organizzativa Responsabile e di Riferimento – vale a dire un insieme di uffici o un ufficio che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione unitarie e coordinate.

Si rimanda al glossario per la definizione dei termini e la corretta interpretazione del dettato del presente manuale.

1.3 Area organizzativa omogenea

Sotto il profilo normativo e archivistico, una AOO può essere definita come un insieme di risorse umane e strumentali dotati di propri organi di governo e di gestione per adempiere a determinate funzioni primarie. Di conseguenza una AOO usufruisce, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. Una UO rappresenta, invece, un sottoinsieme di una AOO, vale a dire un complesso di risorse umane e strumentali cui sono affidate una o più competenze omogenee, nel cui ambito i dipendenti assumono la responsabilità della gestione di procedimenti amministrativi e attività. Ai fini del presente Manuale, nell'ambito dell'Area organizzativa omogenea dell'Istituto "II Circolo Didattico Giovanni XXIII" di Paternò (CT) è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Il servizio stesso è funzionalmente assegnato all'Ufficio Protocollo. In assenza del responsabile del protocollo e del suo collaboratore, è, comunque garantita la continuità operativa del protocollo da parte di qualsiasi assistente amministrativo presente.
Per qualsiasi informazione statistica relativa all'Amministrazione si rimanda alle pagine del sito.

1.4 Servizio archivistico per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi

Al fine della gestione unica e coordinata dei documenti, l'Amministrazione ai sensi dell'art. 50 c. 3 del DPR 445 del 28 dicembre 2000, individua una sola Area Organizzativa Omogenea (AOO) e una sola struttura di protocollo ed archivio. Nell'ambito dell'area organizzativa omogenea, ai sensi

dell'art. 61, comma 1, del DPR 445/2000 ha competenza sulla gestione dell'intera documentazione archivistica, ovunque trattata, distribuita o conservata dell'Amministrazione, ai fini della sua corretta registrazione, classificazione, conservazione, selezione e ordinamento. Il responsabile del servizio, ai sensi dell'art. 4 del DPCM 03.12.2013 svolge le funzioni attribuitegli dai citati DPCM 03.12.2013 e DPR 445/2000. Ai sensi del DPCM 03.12.2013 – Regole tecniche in materia di sistema di conservazione, con decreto n. 71 del 12/11/2014, è stato individuato il Responsabile del procedimento di conservazione della documentazione generata in formato digitale che è specificatamente considerato pubblico ufficiale. Si precisa che la nomina del suddetto responsabile diventerà esecutiva a far data dal giorno in cui diventerà operativo il sistema informatico di conservazione sostitutiva.
L'AOO denominata II C.D. "Giovanni XXIII" è composta dai seguenti uffici:

CODICE	DESCRIZIONE
U1	UFFICIO DIREZIONE
U2	UFFICIO DIDATTICA
U3	UFFICIO PERSONALE A TEMPO DETERMINATO
U4	UFFICIO DSGA
U5	UFFICIO PROTOCOLLO
U6	UFFICIO PERSONALE A TEMPO INDETERMINATO

L'AOO si è dotata di una casella di Posta Elettronica Certificata Istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA). Tale casella costituisce l'indirizzo telematico della AOO e di tutti gli Uffici che ad essa fanno riferimento.

1.5 Le figure di sistema

Il Codice dell'Amministrazione Digitale e le nuove Regole tecniche, per la corretta gestione e la tutela di un archivio elettronico prevedono obbligatoriamente la presenza di varie figure che devono interagire tra loro, dal responsabile della conservazione, dal responsabile della sicurezza, dal responsabile del trattamento dei dati e dal responsabile del protocollo con compiti ben delineati:

- il Dirigente Scolastico è il responsabile della conservazione, col compito di coordinare e presidiare i sistemi informatici informativi e documentali garantendone una durata nel tempo; inoltre risulta anche responsabile per il trattamento dei dati personali, per cui deve occuparsi della protezione dei dati nei database e negli archivi digitali;
- la funzione di responsabile del protocollo dei flussi documentali e degli archivi è assunta dal DSGA Sig.ra Paratore Carmela Marcella che presidia la componente archivistica di qualsiasi sistema di conservazione dei documenti informatici;
- la funzione di responsabile del procedimento è affidata agli assistenti amministrativi dell'Ufficio Protocollo.

1.6 Individuazione del Responsabile del Servizio di tenuta del protocollo informatico e compiti

Il responsabile del protocollo è stato nominato con provvedimento prot. n. 3161/2016 del 09/09/2016 nella persona del Direttore dei Servizi Generali ed Amministrativi pro tempore Sig.ra Paratore Carmela Marcella e nominato coordinatore l'assistente amm.vo Sig.ra Castro Rosaria.
Il responsabile del servizio di Protocollo Informatico svolge le funzioni attribuitegli dal DPCM 31/10/2000 e dal DPR 445/2000 e Decreto del Presidente del Consiglio dei Ministri 03/12/2013, e cioè:

1. Predispone lo schema del manuale di gestione;
2. Partecipa ad attività di formazione, dà consulenza e cura la formazione degli assistenti sulla nuova procedura di gestione del protocollo;
3. Garantisce che le operazioni di assegnazione, registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
4. Garantisce la corretta produzione del registro giornaliero di protocollo;
5. Garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali e gestione archivio, escluse le funzionalità di accesso a nuovi utenti;
6. Vigila sull'osservanza delle disposizioni del presente regolamento;
7. Cura che le funzionalità del sistema in caso di guasti o anomalie collegate al software siano ripristinate nel più breve tempo possibile tramite apposita assistenza offerta dalla ditta che ha fornito il servizio; guasti ed anomalie dell'hardware sono gestiti dall'assistente amministrativo che segue gli acquisti;
8. Partecipa alla redazione del piano della sicurezza informatica d'intesa con il responsabile della conservazione, il responsabile dei sistemi informatici e dei dati personali;
9. Definisce ed assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna tra i vari uffici;
10. Si occupa dell'aggiornamento del titolario di classificazione integrato con le informazioni relative ai tempi, ai criteri ed alle regole di selezione e conservazione;
11. Indica le modalità di produzione e di conservazione delle registrazioni di protocollo informatico; in particolare, dà l'indicazione delle soluzioni tecnologiche ed organizzative che garantiscono di registrare in modo immodificabile e contemporaneo alla segnatura; definisce le modalità di registrazione delle informazioni annullate o modificate in ogni sezione di registrazione.

Ai sensi del DPCM 03.12.2013 (Regole tecniche in materia di sistema di conservazione) con atto prot. n. 3160/2016 del 09/09/2016 è stato individuato il Dirigente Scolastico Prof. Roberto Maniscalco in qualità di responsabile del procedimento di conservazione della documentazione generata in formato digitale che è specificatamente considerato pubblico ufficiale i cui compiti sono indicati nell'apposita sezione al punto 7.1. Tale nomina diverrà esecutiva all'attivazione del sistema di conservazione sostitutiva.

1.7 Unicità del Protocollo informatico

Nell'ambito dell'area organizzativa omogenea, la numerazione delle registrazioni di protocollo è unica e rigidamente progressiva. Essa inizia da uno all'inizio di ogni anno solare e si chiude al 31 dicembre. Tuttavia, a norma dell'art. 53, comma 5 del DPR 445/2000 sono possibili registrazioni particolari.

1.8 Modello organizzativo e modalità di gestione del protocollo informatico

Nell'Istituto "II Circolo Didattico Giovanni XXIII" di Paternò (CT) la gestione dei flussi documentali e del protocollo informatico avviene a partire dalla data 29/07/2016 tramite il seguente software: ARGO GECODOC PRO 3.0 ovvero, l'automazione di un processo che coinvolge tutti gli assistenti amministrativi, il Direttore SGA e il Dirigente Scolastico secondo uno schema di regole procedurali definite.
L'Istituto "II Circolo Didattico Giovanni XXIII" di Paternò (CT) è dotato di un archivio digitale dove ogni utente, dopo essersi autenticato, entra nella sua work list e trova varie azioni da compiere a seconda del ruolo di appartenenza. La firma digitale è competenza esclusiva del Dirigente Scolastico sia in arrivo che in partenza.
Il modello organizzativo è centralizzato per la registrazione di atti in arrivo; la registrazione degli atti in partenza è demandata ad ogni singolo ufficio.
Le operazioni di consultazione dell'archivio protocollo possono essere effettuate da parte di tutti gli utenti abilitati, non solo per gli atti di propria competenza ma per tutti gli atti secondo i sistemi di ricerca generale o specifica.
Per ciò che concerne la modalità di gestione del protocollo informatico la società fornitrice del software gestisce per conto dell'Istituto "II Circolo Didattico Giovanni XXIII" di Paternò (CT) la conservazione dei dati e documenti di protocollo secondo quanto specificato nel relativo contratto e nell'attestazione di conformità agli standard previsti dalla normativa del protocollo informatico.

SEZIONE II – FORMAZIONE DEI DOCUMENTI

2.1 Modalità di formazione dei documenti e contenuti minimi

Le modalità di formazione dei documenti, del loro contenuto e della loro struttura sono determinate dalla Dirigenza e da quanto previsto dal presente manuale; per quanto riguarda i documenti informatici la loro produzione è regolata sulla base di modelli standard presenti nel sistema informatico di gestione documentale. I documenti dell'Amministrazione sono prodotti con sistemi informatici, come previsto dalla normativa vigente.
Ogni documento creato per essere formalmente inoltrato all'esterno o all'interno ha le seguenti caratteristiche:

- Si riferisce ad un solo protocollo;
- Può fare riferimento anche a più pratiche e fascicoli;
- L'oggetto del documento tratta in modo omogeneo ed attinente un argomento.

Le firme necessarie alla sua redazione e perfezione giuridica devono essere apposte prima della sua protocollazione.

Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- La denominazione dell'amministrazione;
- Codice Area Organizzativa Omogenea (AOO);
- Codice Registro di protocollo;
- Numero registrazione di protocollo;
- Data di registrazione protocollo;
- Oggetto del documento;
- Eventuali allegati;
- Estremi identificativi del responsabile del procedimento (L. 241/90);
- Sottoscrizione elettronica con firma digitale o elettronica del responsabile di gestione.

2.2 Formato dei documenti informatici

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma digitale o avanzata, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione, come riportato sul sito dell'Agenzia per l'Italia Digitale (www.agid.gov.it), al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura. A titolo d'esempio si utilizzano preferibilmente: PDF e PDF/A. per quanto riguarda la gestione e la conservazione dei documenti dell'Ente, si rimanda al Manuale della Conservazione appositamente redatto (ovvero che verrà redatto secondo la normativa vigente). La rappresentazione dei documenti informatici, che ne consente la consultazione da parte dei soggetti interessati, è resa possibile tramite l'utilizzo di appositi formati per la fruizione dei quali è necessario ed indispensabile l'utilizzo delle relative applicazioni.

L'Organizzazione garantisce che, per la rappresentazione dei documenti informatici, il presente sistema utilizza esclusivamente formati statici, ossia non contenenti codici eseguibili o macro-istruzioni che possano alterarne il contenuto tra un accesso e il successivo, indipendentemente dalla volontà dell'utente che li consulta.

I documenti informatici sono generati, memorizzati ed organizzati tramite l'utilizzo coordinato di appositi software.

2.3 Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma digitale o avanzata conforme alle disposizioni di legge. I titolari di firma digitale sono abilitati all'utilizzo del dispositivo di firma solo ed esclusivamente nell'esercizio delle proprie funzioni in qualità di dipendenti di questa istituzione scolastica. L'assegnazione dei dispositivi di firma compete al Responsabile della gestione documentale, il quale provvede ad autorizzare l'utilizzo della firma digitale o avanzata a seguito di segnalazione del Dirigente Scolastico dell'Istituto.

Il servizio archivistico è responsabile del controllo della scadenza dei certificati di firma e del loro eventuale rinnovo.

2.4 Verifica delle firme digitali

La sequenza delle operazioni previste per la verifica di integrità del documento firmato digitalmente è la seguente:

- Apertura del file firmato;
- Verifica della validità del certificato e della corrispondenza delle impronte del documento.

Queste attività sono realizzate mediante un'applicazione appositamente messa a disposizione da parte dell'ente fornitore dei certificati di firma digitale in dotazione all'Ente (si rinvia alla seguente pagina http://www.agid.gov.it/identita-digitali/firme-elettroniche/software-verifica , dove si può trovare una lista di software che possono essere usati per la verifica della firma).

2.5 Tipologie particolari di documenti per i quali si stabiliscono modalità di trattamento specifiche

Le eventuali modifiche alle tipologie di documentazione sottoposta a trattamento specifico e a registrazione particolare sono evidenziate in un elenco a parte.

SEZIONE III – RICEZIONE DEI DOCUMENTI

3.1 Ricezione dei documenti cartacei

I documenti su supporto cartaceo possono arrivare all'Ente attraverso:

a. Il servizio postale;
b. La consegna diretta agli uffici, ai funzionari o agli uffici utente;
c. Fax.

L'istituzione scolastica si riserva il diritto a non accettare documenti pervenuti via fax se presentano caratteristiche di unicità (firma autografa, timbri, punzoni) e non accompagnati dalla trasmissione di una copia del documento di identità, ovvero provenienti da altre Pubbliche Amministrazioni a norma di quanto previsto dall'articolo 14 *"Misure per favorire la diffusione del domicilio digitale"*, del c.d. Decreto del Fare (Decreto legge n. 69/2013, pubblicato in G.U. il 21/06/2013 in seguito alle modificazioni apportate dalla legge di conversione n. 98 del 9 agosto 2013) che ha stabilito, infatti, che ai fini della verifica della provenienza delle comunicazioni è in ogni caso esclusa la trasmissione di documenti a mezzo fax.

Lo stesso art. 47 del CAD, rubricato appunto *"Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni"*, stabilisce che le comunicazioni di documenti tra PPAA avvengano mediante l'utilizzo della posta elettronica o in cooperazione applicativa e che esse siano valide ai fini del procedimento amministrativo solo una volta che se ne sia verificata la provenienza.

Il comma 2 dello stesso articolo prevede, poi, che ai fini della verifica della provenienza, le comunicazioni sono valide se:

a. Sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
b. Ovvero, sono dotate di segnatura di protocollo di cui all'articolo 55 del DPR 28 dicembre 2000, n. 445;
c. Ovvero, e comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71. È in ogni caso esclusa la trasmissione di documenti a mezzo fax;

d. Ovvero, trasmesse attraverso sistemi di posta elettronica certificata di cui al DPR 11 febbraio 2005, n. 68;

I documenti, esclusi quelli non soggetti a registrazione di protocollo, devono pervenire al protocollo per la loro registrazione.
Quelli arrivati via fax sono soggetti alle stesse regole di registrazione degli altri documenti cartacei se rispondono a parametri di autenticità, leggibilità e integrità previsti dalla normativa vigente.
Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema ha già attribuito ad altri documenti, anche se questi sono strettamente correlati tra loro.
Non è pertanto consentito, in nessun caso, l'utilizzo di un unico numero di protocollo per il documento in arrivo e il documento in partenza. La documentazione che non è stata registrata in arrivo o in partenza viene considerata giuridicamente inesistente per l'Amministrazione.
I documenti che transitano attraverso il servizio postale tradizionale sono ritirati, ogni giorno lavorativo a cura del personale collaboratore scolastico addetto al centralino e consegnati al Direttore SGA (o al suo sostituto) che a sua volta li consegna, dopo aver preso visione del contenuto, all'Ufficio Protocollo che ha cura di mostrarne la visione al dirigente scolastico. I documenti pervenuti ad altri uffici, mediante uno qualunque dei mezzi citati, sono fatti pervenire, a cura del personale che li riceve, all'Ufficio Protocollo.
La corrispondenza indirizzata alla cortese attenzione del personale è regolarmente aperta e registrata al protocollo.
Non è ammessa la ricezione di corrispondenza di carattere personale; il servizio archivistico è in ogni caso tenuto a verificare il contenuto della corrispondenza pervenuta.
A chi richieda ricevuta di un documento consegnato, compatibilmente con le possibilità del servizio, verrà consegnata l'apposita stampa ottenibile dal sistema informatico o redatto apposito documento analogico.
La corrispondenza in arrivo viene aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata. Laddove, per esigenze interne all'ufficio, non sia possibile registrare la totalità dei documenti pervenuti, si procederà selezionando quelli con scadenza imminente; i restanti documenti verranno registrati il giorno lavorativo successivo, riportando la data di ricezione e quella di registrazione.

3.2 Rilascio di ricevute attestanti la ricezione dei documenti

Qualora venga richiesto il rilascio immediato di una ricevuta attestante l'avvenuta consegna di un documento, l'ufficio abilitato alla registrazione di protocollo dei documenti in arrivo, non potendo rilasciare subito la ricevuta di protocollo, si riserva di inviare successivamente, via posta elettronica, la segnatura digitale con il relativo file .xml dove è indicata anche il numero di protocollo assegnato all'atto.

3.3 Ricezione dei documenti informatici

Un documento informatico, sottoscritto con firma elettronica qualificata o firma digitale, può essere recapitato a mezza posta elettronica certificata (PEC) o equivalente.

La ricezione dei documenti informatici è assicurata tramite una casella di posta elettronica certificata (casella istituzionale) riservata a questa funzione, integrata con il sistema informatico ed accessibile solo all'ufficio/postazione preposto/ e alla registrazione di protocollo. Gli indirizzi della casella di posta elettronica istituzionale e della casella di posta elettronica certificata sono reperibili sul sito web di questa istituzione scolastica (www.2circolopatern.gov.it).
Il responsabile del servizio provvede a renderlo pubblico e a trasmetterlo all'Agenzia per l'Italia Digitale ai sensi dell'art. 12 del DPCM 03,12,2013 i documenti informatici eventualmente pervenuti ad altri indirizzi mail, devono essere re-inoltrati dal mittente all'indirizzo di posta certificata dell'Ente per la registrazione. Per quanto riguarda la gestione della posta elettronica si veda quanto previsto successivamente.
L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti.
Il personale addetto alla protocollazione controlla quotidianamente i messaggi pervenuti nelle caselle di posta istituzionale certificata (PEC) e posta istituzionale ordinaria non certificata (PEO) e verifica se il documento ricevuto sia da protocollare.
La posta elettronica individuale non può essere utilizzata per la ricezione o la spedizione di documenti a firma digitale per i quali è prevista l'apposita casella di pec o peo. Le caselle di posta personale, di cui ogni assistente amministrativo è dotato, vanno utilizzate per comunicazioni a carattere informale e per le comunicazioni di natura non ufficiale o per scambi di documenti non definitivi, per i quali non è necessario acquisire certezza di invio o ricezione.
Non si possono inviare messaggi dalla casella di posta personale quando il contenuto di questi impegni l'Amministrazione verso terzi.

3.4 Errata ricezione di documenti

Nel caso in cui pervengano messaggi/documenti dal cui contenuto si rileva che sono stati erroneamente ricevuti, si provvederà a rispedire il messaggio al mittente utilizzando lo stesso canale tramite il quale il messaggio/documentazione è giunto (mail/mail; Posta Ordinaria/Posta Ordinaria; Fax/Fax; ecc…).

SEZIONE IV – SCANSIONE DEI DOCUMENTI SU SUPPORTO CARTACEO

4.1 Acquisizione di documenti cartacei tramite scanner

Tutti i documenti analogici pervenuti al protocollo generale sono acquisiti mediante scanner, compatibilmente con il relativo formato e gli strumenti tecnologici disponibili. L'immagine digitale così ottenuta è archiviata nel sistema informatico in modo da poter essere sempre consultata ed eventualmente riprodotta in copia. L'addetto al protocollo deve verificare la leggibilità delle immagini acquisite e la loro esatta corrispondenza con il cartaceo e scandire in formato pdf non immagine, nel rispetto dei requisiti di accessibilità; occorre sempre rendere accessibili documenti provenienti da altri enti se devono essere pubblicati sul sito scolastico.

SEZIONE V – ASSEGNAZIONE, RECAPITO, PRESA IN CARICO DEI DOCUMENTI

5.1 Il processo di assegnazione dei documenti

Per assegnazione di un documento si intende l'operazione di individuazione dell'ufficio cui compete la trattazione del relativo affare o procedimento amministrativo. La lavorazione dei documenti ricevuti dall'Amministrazione e la designazione dei relativi responsabili di procedimento è effettuata direttamente dal Direttore SGA scegliendo il nominativo corrispondente all'interno del work flow.

5.2 Recapito e presa in carico dei documenti

I documenti dopo la fase di protocollo arrivano nella work list dei responsabili di procedimento che possono procedere con la lavorazione, creare una pratica o inserire file in una pratica già esistente o semplicemente prenderne visione.
Il sistema di gestione informatica dei documenti tiene traccia di tutti questi passaggi, memorizzando per ciascuno di essi, l'identificativo dell'utente, lo stato del documento nelle varie fasi: assegnazione, controllo dsga al protocollo, protocollato, la data e l'ora di esecuzione, lo stato del documento, il suo ID di processo e di attività.

SEZIONE VI – REGISTRAZIONE DEI DOCUMENTI

6.1 Documenti soggetti a registrazione di protocollo

Tutti i documenti prodotti e ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, ad eccezione di quelli indicati nel successivo articolo, sono registrati al protocollo.

6.2 Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo:

- bollettini ufficiali, notiziari della pubblica amministrazione;
- note di ricezione delle circolari ed altre disposizioni;
- materiale statistico e certificazioni anagrafiche;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti i documenti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa presente o futura;
- tutte le comunicazioni e tutti i documenti utilizzati nell'ambito dell'Ente aventi rilevanza esclusivamente interna, siano essi predisposti in forma cartacea che in formato elettronico.

6.3 Registrazione di protocollo dei documenti ricevuti e spediti

La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione. I requisti necessari di ciascuna registrazione di protocollo sono:

a. numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;

b. data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
c. mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
d. oggetto del documento, registrato in forma non modificabile;
e. data e numero di protocollo dei documenti ricevuti, se disponibili;
f. impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
g. classificazione: categoria, classe, fascicolo;
h. assegnazione.

Inoltre possono essere aggiunti:

i. data di arrivo;
j. allegati (numero e descrizione);
k. estremi provvedimento differimento termini di registrazione;
l. mezzo di ricezione/spedizione (lettera ordinaria, prioritaria, raccomandata, corriere, fax, PEC, PEO,…);
m. ufficio di competenza;
n. tipo documento;
o. livello di riservatezza;
p. elementi identificativi del procedimento amministrativo, se necessario.

6.4 Registrazione dei documenti interni informali

Nei documenti interni informali includiamo tutti quei documenti di lavoro di natura non ufficiale, temporanea ed interlocutoria, a carattere informativo, operativo, preparatorio (ad es.: sono documenti che non possiedono carattere di particolare ufficialità, bozze, appunti, etc…).
Per questa tipologia di documenti che ha rilevanza solo interna, ci si avvale dei sistemi di comunicazione interna con possibilità di sottoscrizione e protocollazione, laddove il Responsabile di Gestione lo ritenga necessario.

6.5 Segnatura di protocollo

La segnatura di protocollo apposta o associata al documento è effettuata contemporaneamente alla registrazione di protocollo per mezzo di timbri.
I requisiti necessari di ciascuna segnatura di protocollo sono:

a. codice identificativo dell'amministrazione, per i protocolli informatici;
b. codice identificativo dell'area organizzativa omogenea, per i protocolli informatici;
c. data di protocollo;
d. numero di protocollo;
e. indice di classificazione.

Per i documenti informatici trasmessi ad altre Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file

conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD) e comprendono anche:

f. oggetto del documento;
g. mittente/destinatario.

6.6 Annullamento delle registrazioni di protocollo

Le registrazioni di protocollo, tutte o in parte, possono essere annullate con una specifica funzione del sistema di gestione informatica dei documenti e con autorizzazione del Responsabile della gestione documentale a seguito di motivata richiesta scritta o per iniziativa dello stesso responsabile. Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema. Non è possibile annullare il solo numero di protocollo e mantenere valide le altre informazioni della registrazione.

6.7 Differimento dei termini di protocollazione

La registrazione della documentazione pervenuta avviene nell'arco della giornata. Il responsabile del servizio, con apposito provvedimento motivato, può autorizzare la registrazione in tempi successivi, fissando un limite di tempo entro il quale i documenti devono essere protocollati. Ai fini giuridici i termini decorrono dalla data di ricezione riportata sul documento analogico tramite un apposito timbro; il sistema informatico mantiene traccia del ricevimento dei documenti.

6.8 Registro giornaliero e annuale di protocollo

Il contenuto del registro e del sistema di protocollo informatico, unitamente alla memoria informatica dell'Ente, alla fine di ogni giorno è salvato su supporti di memorizzazione.
Delle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.
Per quanto riguarda le procedure di conservazione della memoria informatica vedi anche la sezione XII.

6.9 Requisiti minimi di sicurezza dei sistemi di protocollo informatico

Il sistema di protocollo informatico assicura:

a. l'univoca identificazione ed autenticazione degli utenti;
b. la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
c. la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
d. la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Il sistema di protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti ed il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Le registrazioni devono essere protette da modifiche non autorizzate.
Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.
Il sistema di protocollo rispetta le misure di sicurezza previste dalla normativa in vigore.

6.10 Registro di emergenza

Il responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su registri di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema. Tale autorizzazione consta in proprio provvedimento, riportante la causa, la data e l'ora di inizio dell'interruzione del funzionamento del sistema informatico di protocollo. In questi casi, dovranno essere compilati in ogni loro parte e firmati, i Moduli di Registrazione di Emergenza.
Si applicano le modalità di registrazione dei documenti sul registro di emergenza e di recupero delle stesse nel sistema di protocollo informatico, in ottemperanza all'articolo 63 del DPR 445/2000.
Il Registro di emergenza si rinnova ogni anno solare, e pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno. Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza. I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale. La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo. In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

6.11 Registro di fascicoli riservati

Considerato che l'Agenzia per l'Italia Digitale con un suo comunicato del 30/10/2013 attesta il nulla osta all'istituzione e all'impiego di un *"registro di protocollo riservato"*, coerentemente alla normativa vigente in materia di protocollo informatico e gestione documentale, indicando che tale registro e quello generale di protocollo devono essere esclusivamente di tipo informatico, si procede all'inserimento di dati riservati all'interno del raccoglitore denominato *"registro di fascicoli riservati"* da implementare. I documenti cartacei vengono conservati dal Dirigente Scolastico.

SEZIONE VII – DOCUMENTAZIONE PARTICOLARE

7.1 Determinazioni Dirigenziali, decreti e contratti

Determinazioni dirigenziali e decreti, documenti già soggetti per normativa specifica a registrazione particolare da parte dell'Istituto possono essere gestiti da software di produzione e conservazione di questa tipologia particolare di documentazione, a condizione che detti software consentano di eseguire su di essi tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico. Ogni registrazione deve riportare necessariamente:

a. dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile);
b. dati di classificazione;

c. numero di repertorio progressivo e annuale (generato in modo non modificabile).

Per quanto riguarda le notifiche e le pubblicazioni all'albo on line e su Amministrazione Trasparente si rimanda alle apposite linee guida.
I contratti del personale vengono gestiti attraverso la piattaforma SIDI.

7.2 Documentazione di gare di appalto

Qualora non effettuata con le procedure MePA, le offerte di gare di appalto o altra documentazione da consegnarsi all'Ente in busta chiusa sono registrate al protocollo. Dopo l'apertura della busta a cura dell'ufficio che gestisce la gara verrà riportato su ciascun documento contenuto il medesimo numero di protocollo assegnato alla busta.
A tale scopo sono annotate le seguenti informazioni:

1. denominazione dell'Ente;
2. data apertura busta;
3. data e numero di protocollo della busta.

7.3 Gestione delle fatture

L'ufficio contabile è responsabile della gestione delle fatture attraverso la piattaforma SDI (Sistema di Interscambio).

7.4 Documenti su supporto cartaceo indirizzati nominalmente a personale dell'Ente, lettere anonime e documenti non firmati

La corrispondenza indirizzata nominativamente è regolarmente aperta e registrata al protocollo. Le lettere anonime vengono protocollate, se intestate genericamente all'istituto; se specificatamente indirizzate, sono consegnate al destinatario, il quale ne potrà disporre la protocollazione.
Le lettere con firma illeggibile, delle quali non è identificabile in altro modo il mittente, non si registrano a protocollo, ma si inviano al destinatario, il quale ne potrà disporre la protocollazione solo a seguito di eventuali accertamenti, indicando l'identità del mittente.

7.5 Corrispondenza con più destinatari e copie per conoscenza

Tutte le comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo.
Se in uscita, i destinatari possono essere descritti in elenchi associati al documento.
Dei documenti analogici prodotti/pervenuti di cui si necessita la distribuzione interna all'ente, si faranno copie informatiche degli stessi.

7.6 Allegati

Gli allegati che pervengono via mail vengono automaticamente archiviati all'interno del software di archiviazione utilizzato: ARGO GECODOC PRO 3.0.
È inoltre possibile l'archiviazione mediante drag and drop degli allegati negli appositi raccoglitori virtuali concordati con la Dirigenza del II Circolo Didattico "Giovanni XIII" di Paternò (CT) e l'attribuzione agli stessi dei dati minimi obbligatori.

7.7 Documenti di competenza di altre amministrazioni
Qualora pervengano all'Ente documenti di pertinenza di altre amministrazioni, queste verranno restituite al destinatario. Se il documento viene erroneamente protocollato, il numero di protocollo deve essere annullato ed il documento inviato al destinatario. Nel caso in cui il destinatario non sia individuabile, il documento deve essere rimandato al mittente.

7.8 Oggetti plurimi
Qualora un documento in entrata presenti più oggetti relativi a procedimenti diversi e, pertanto, da assegnare a più fascicoli, si dovranno produrre copie autentiche dello stesso documento e successivamente registrarle, classificarle e fascicolarle indipendentemente l'una dall'altra. L'originale verrà inviato al destinatario indicato nel documento, oppure, nel caso di destinatari plurimi, al primo in indirizzo. Nel caso in cui l'individuazione di più oggetti venga effettuata successivamente da parte del destinatario, questi deve inviare all'ufficio protocollo apposita comunicazione affinché si provveda nel medesimo modo.
Lo stesso principio deve essere utilizzato per la protocollazione di documentazione in partenza: si restituiranno al responsabile di procedimento documenti in uscita con più oggetti.

7.9 Produzione seriale di documenti sulla base di un modello generale
Nel caso di produzione in serie di documenti base che abbiano destinatari multipli e parti minime variabili di contenuti (quali la diversità di importi, date, ecc…), dovranno essere compilati gli elenchi dei destinatari e delle parti variabili dei documenti base ad essi riferiti. Gli elenchi devono essere conservati insieme al documento base nel fascicolo. Il documento base, ossia Minuta/Copia per atti, deve essere dotato di firma digitale o avanzata.
Sui documenti inviati ai destinatari, ai quali non si vuole apporre singolarmente la sottoscrizione, dovrà essere obbligatoriamente riportata l'indicazione del Responsabile del procedimento o del sottoscrittore, preceduto dall'acronimo F.to, e dalla seguente dicitura: *"L'originale del documento è conservato presso l'istituzione Scolastica. La firma è sostituita dall'indicazione del nome a norma del d.lgs. n. 39/1993".*

7.10 Trasmissioni telematiche
I dati con immissione diretta sul server dell'Ente destinatario sono trasmessi/ricevuti senza la produzione e conservazione dell'originale cartaceo. I documenti sono trasmessi senza firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate ad identificazione univoca attivati con i singoli Enti destinatari.
Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione.
Gli atti ed i provvedimenti amministrativi vengono pubblicati sul sito dell'istituto www.2circolopater.gov.it nella sezione *"Albo on line"* ed *"Amministrazione Trasparente"* secondo quanto previsto dalla normativa vigente.
La pubblicazione di atti all'Albo on-line e su Amministrazione Trasparente ha lo scopo di fornire presunzione di conoscenza legale degli stessi, a qualunque effetto giuridico specifico essa assolva (pubblicità, notizia, dichiarativa, costitutiva, integrativa dell'efficacia, ecc …). Sono soggetti alla

pubblicazione all'Albo Pretorio e su Amministrazione Trasparente tutti gli atti per i quali la legge ne preveda l'adempimento.
I documenti restano pubblicati per il tempo stabilito dalle singole disposizioni di legge o di regolamento. In Albo Pretorio, salvo casi specifici, la durata è di quindici giorni. Per quanto non esplicitato si rinvia alle linee guida delle pubblicazioni albo pretorio on-line ed amministrazione trasparente.
Con decreto 3 aprile 2013, n. 55, del Ministro dell'Economia e delle Finanze, entrato in vigore il 6 giugno 2013, è stato approvato il regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica, ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.
Dal 6 giugno 2014 i fornitori devono produrre, nei confronti dell'Istituto esclusivamente fatture elettroniche, nel rispetto delle specifiche tecniche reperibili sul sito www.fatturapa.gov.it .
Le fatture elettroniche così ricevute vengono gestite per il tramite di apposite funzioni del sistema SIDI che provvede automaticamente a ricevere le fatture indirizzate dai fornitori all'Istituto "Secondo Circolo Didattico Giovanni XXIII" di Paternò (CT).
Dalla data di ricezione decorrono i termini per il pagamento della fattura, pari a 30 giorni salvo patti contrari tra le parti. Le fatture, in prima fase, vengono protocollate con le ordinarie modalità.
Il DSGA ovvero un suo delegato provvede a:

- riconoscere/rifiutare la fattura mediante il sistema SIDI entro 15 giorni dalla ricezione della medesima;
- adottare gli atti di spesa, avvalendosi delle usuali funzioni al SIDI, ad estinzione totale/parziale del debito corrispondente alla fattura;
- effettuare la conservazione sostitutiva dei fascicoli informatici così aperti.

In base alla legge 190/2012 l'istituto è tenuto a rendere noti all'ANAC, tutti i dati relativi all'espletamento di gare e bandi. Annualmente (entro il 31 gennaio dell'anno successivo a quello di riferimento) i dati devono essere trasferiti direttamente in formato aperto utilizzando lo standard XML.
L'istituto ha predisposto sul proprio sito web la già citata sezione apposita denominata "Amministrazione Trasparente" all'interno della quale collocare i file XML che descrivono le gare espletate.
L'indirizzo viene comunicato all'Autorità in modo che possa provvedere al recupero automatico delle informazioni contenute.

SEZIONE VIII – ASSEGNAZIONE DEI DOCUMENTI

8.1 Assegnazione

L'assegnazione dei documenti agli uffici utenti o ai responsabili di procedimento è effettuata dal responsabile della gestione documentale sulla base dell'elenco degli uffici e dei responsabili di procedimento.

Le abilitazioni all'assegnazione dei documenti, effettuate da altri uffici utente, sono rilasciate dal Responsabile della gestione documentale.
I documenti ricevuti dall'Ente, al termine delle operazioni di registrazione, classificazione, segnatura ed assegnazione, sono fatti pervenire in originale agli uffici che, per quanto a conoscenza dell'ufficio protocollo, hanno competenza sull'oggetto specificato nel documento.
La registrazione a protocollo sulla procedura informatica risulta in "carico" all'area amministrativa: è compito dell'ufficio procedere ad eventuale modifica di assegnazione.
Spettano al Responsabile del Procedimento amministrativo le incombenze relative alla gestione del documento: l'inserimento nel fascicolo di competenza preesistente o eventualmente in un nuovo fascicolo e l'invio delle copie per conoscenza.

8.2 Modifica delle assegnazioni

Nel caso di un'assegnazione errata, l'Ufficio che riceve il documento, lo rinvia al servizio archivistico che provvederà alla riassegnazione per poi trasmetterlo al nuovo assegnatario. La responsabilità del mancato rispetto di quanto sopra descritto è da attribuirsi all'Ufficio che non ha rimandato al servizio archivistico il documento erroneamente trasmesso.
Delle operazioni di riassegnazione e degli estremi del provvedimento di autorizzazione è lasciata traccia nel sistema informatico di gestione dei documenti.
In caso di documentazione informatica, il software di gestione documentale provvederà automaticamente a rendere visibile il documento riassegnato al destinatario di competenza.

8.3 Consegna dei documenti analogici

I documenti analogici/cartacei protocollati ed assegnati sono resi disponibili ai destinatari mediante l'uso di apposite cartelle.

8.4 Consegna dei documenti informatici

I documenti informatici e/o le immagini digitali dei documenti cartacei acquisite con lo scanner sono resi disponibili agli uffici, o ai responsabili di procedimento, tramite il sistema informatico di gestione documentale.

SEZIONE IX – CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

9.1 Classificazione dei documenti

Gli addetti al servizio di ricezione eseguono la prima classificazione del documento e provvedono ad inserirlo nell'archivio digitale dove verranno attribuiti al documento i campi di ricerca e metadati necessari per la corretta gestione (l'inserimento è automatico per i documenti informatici ricevuti via mail, manuale con parametri preimpostati per tutti gli altri casi). I campi di ricerca e metadati

sono consultabili nella sezione *"Proprietà"* del raccoglitore cliccando al di sopra di esso con il tasto destro del mouse.
Gli addetti al servizio di ricezione, inoltre, provvedono ad inviare il documento tramite workflow al Responsabile della gestione che:

- esegue una verifica di congruità;
- in caso di errore ne dà immediata comunicazione all'addetto che ha ricevuto il documento;
- in caso di verifica positiva, assegna all'Area utente responsabile l'operazione di presa in carico del documento e provvede ad affidare la gestione della pratica e fascicolazione.

Alla fine della corretta presa in carico dei documenti, tutto il personale addetto ad ogni singola Area Utenti deve consultare giornalmente l'applicativo in dotazione ed avviare i processi di gestione documentale.

9.2 Formazione ed identificazione dei fascicoli

Tutti i documenti registrati al protocollo informatico e classificati, indipendentemente dal supporto sul quale sono forniti, sono riuniti in fascicoli attraverso le opportune funzioni del sistema di protocollo informatico.
La formazione di un nuovo fascicolo o di una nuova pratica è effettuata dal Responsabile del procedimento ed avviene attraverso l'operazione di apertura che prevede la registrazione nel sistema informatico delle seguenti informazioni:

a. categoria e classe del titolario di classificazione;
b. oggetto del fascicolo;
c. data di apertura;
d. ufficio a cui è assegnato;
e. responsabile del procedimento.

9.3 Processo di formazione dei fascicoli

In presenza di un documento da inserire in un fascicolo i Responsabili di Servizio/Procedimento stabilisce/ono, consultando le funzioni del protocollo informatico o il repertorio dei fascicoli, se esso si collochi nell'ambito di un affare o procedimento in corso (pratica), oppure se dà avvio ad un nuovo procedimento.
I documenti in arrivo sono fascicolati dai Responsabili di Procedimento, il Servizio archivistico mantiene comunque un'attività di controllo a cadenza almeno bimestrale sulla documentazione fascicolata. Il software di protocollo informatico non permette la conservazione sostitutiva della documentazione senza che prima la stessa venga fascicolata.
I documenti in partenza sono fascicolati dai Responsabili di Procedimento che hanno cura di inserirli fisicamente nel fascicolo in caso di documenti cartacei; nel caso di documenti informatici, il sistema provvede automaticamente, dopo l'assegnazione al fascicolo, ad inserire il documento nel fascicolo informatico stesso. I documenti pertanto verranno protocollati già con l'indicazione dell'identificazione del fascicolo.
Se il documento dà avvio ad un nuovo affare, i Responsabili di Procedimento aprono un nuovo fascicolo (con le procedure sopra descritte).

9.4 Modifica delle assegnazioni dei fascicoli

La riassegnazione di un fascicolo è effettuata dal servizio archivistico che provvede a correggere le informazioni del sistema informatico e del repertorio dei fascicoli e inoltra successivamente il fascicolo al responsabile del procedimento di nuovo carico. Delle operazioni di riassegnazione è lasciata traccia nel sistema informatico di gestione dei documenti.

9.5 Fascicolo ibrido

Il fascicolo è composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un affare o procedimento amministrativo che dà origine a due unità archivistiche di conservazione differenti; l'unitarietà del fascicolo è garantita dal sistema mediante l'indice di classificazione ed il numero di repertorio.

Alla chiusura del fascicolo, ai sensi del Codice dell'Amministrazione Digitale (d.lgs. 82/2005) sono previste due possibilità:

1. stampa e copia conforme cartacea dell'originale informatico;
2. scansione e copia conforme informatica dell'originale cartaceo.

È compito dei Responsabili di procedimento scegliere la soluzione ritenuta più idonea. Il Responsabile della gestione documentale mantiene, comunque, un'attività di controllo sulle procedure suddette.

Saranno, quindi, i responsabili di procedimento ad apporre la propria firma autografa in caso di produzioni di copia conformi cartacee oppure la propria il DSGA, Responsabile della Gestione, la propria firma digitale in caso di copie conformi informatiche.

Il documento originale sarà conservato secondo quanto previsto dal massimario di scarto.

I documenti originali informatici saranno sottoposti al procedimento di conservazione sostitutiva.

I documenti cartacei saranno inviati in archivio di deposito in apposite scatole contenenti l'indicazione della classificazione e dell'anno di produzione/ricevimento.

9.6 Tenuta dei fascicoli dell'archivio corrente

I fascicoli dell'archivio corrente sono formati a cura dei responsabili di procedimento e conservati, fino al trasferimento nell'archivio di deposito, presso gli uffici di competenza. Per quanto riguarda i fascicoli informatici, vedi Sezione 12.

9.7 Movimentazione dei fascicoli dell'archivio

Annualmente, gli uffici devono redigere un apposito piano di versamento costituito dall'elenco dei fascicoli relativi ad affari e a procedimenti conclusi, a seguito del quale consegneranno al Responsabile della gestione documentale i fascicoli da depositare nell'archivio di deposito.

Periodicamente e secondo un apposito piano di versamento (di norma una volta all'anno), il responsabile del procedimento deve consegnare all'archivio i fascicoli relativi ad affari e a procedimenti amministrativi non più necessari ad una trattazione corrente corredati dal relativo elenco di versamento.

Le serie Archivistiche e i relativi registri o repertori sono conservati per cinque anni presso la struttura che cura i rispettivi procedimenti; trascorso tale termine vengono versati all'Archivio di deposito.
È fatto divieto di prelevare anche temporaneamente gli atti dall'archivio di deposito senza l'autorizzazione del Responsabile della gestione documentale e la collocazione di apposita scheda di prelevamento.
Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli avevano nell'archivio corrente.
Prima di effettuare il conferimento di cui sopra, il Responsabile del procedimento verifica:

a. l'effettiva conclusione ordinaria della pratica;
b. l'effettiva trascrizione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;
c. il corretto aggiornamento della data di chiusura sulla camicia del fascicolo (in caso di documentazione cartacea). In caso di documentazione informatica, la data di chiusura del fascicolo elettronico viene assegnata automaticamente dal software di gestione documentale in uso;
d. lo scarto di eventuali copie e fotocopie di documentazione, al fine di garantire la presenza di tutti e soli documenti pertinenti alla pratica.
   Dell'avvenuto conferimento dei documenti viene predisposto un elenco di versamento con le modalità previste dal testo unico, copia del quale viene conservata dall'utente che ha versato la documentazione.
   Il materiale viene archiviato per materia con lo stesso ordine di classificazione dell'archivio corrente e per ordine cronologico.
   I fascicoli del personale sono conservati presso la competente U.O. e devono essere versati all'archivio di deposito dopo un anno dalla cessazione (e conclusione dei relativi adempimenti) dal servizio del dipendente.

SEZIONE X – SPEDIZIONE DEI DOCUMENTI DESTINATI ALL'ESTERNO

10.1 Spedizione dei documenti analogici

I documenti da spedire sono trasmessi all'ufficio spedizione in busta chiusa, completi della firma autografa del Responsabile della gestione documentale, della classificazione e del numero di fascicolo nonché delle eventuali indicazioni necessarie ad individuare il procedimento amministrativo di cui fanno parte. Nel caso di spedizione che utilizzi pezze di accompagnamento (raccomandate o altro mezzo di spedizione), queste devono essere compilate a cura dell'ufficio produttore.
Eventuali situazioni di urgenza che modifichino la procedura descritta devono essere valutate ed autorizzate dal Responsabile della gestione documentale.

10.2 Spedizione dei documenti informatici

La spedizione dei documenti informatici avviene all'interno del sistema informatico di gestione dei documenti con le procedure adottate dal manuale operativo dello stesso, dopo essere stati classificati, fascicolati e protocollati e comunque secondo i seguenti criteri generali:

1. i documenti informatici sono trasmessi all'indirizzo elettronico dei destinatari abilitato alla ricezione della posta per via elettronica, tramite casella di posta elettronica certificata;
2. per la spedizione l'amministrazione si avvale di una casella di posta elettronica certificata e dei servizi di autenticazione e marcatura temporale offerti da un certificatore abilitato (art. 27, comma 3, DPR 445/2000);
3. l'Ufficio protocollo/le postazioni decentrate di protocollo provvede/ono:
    - a verificare l'invio elettronico utilizzando i servizi di autenticazione e marcatura temporale;
    - a verificare l'avvenuto recapito dei documenti spediti per via elettronica;
    - ad archiviare le ricevute elettroniche collegandole alle registrazioni di protocollo.

Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dall'art. 49 del CAD d.lgs. 82/2005, come modificato dal d.lgs. 235/2010.
La spedizione di documenti informatici al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni senza che a queste l'amministrazione riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

SEZIONE XI – SCANSIONE DEI DOCUMENTI SU SUPPORTO CARTACEO

11.1 Documenti soggetti a scansione

I documenti cartacei che pervengono all'Organizzazione per mezzo di posta ordinaria, fax o telegramma vengono sottomessi ad un processo di dematerializzazione tramite scansione ed acquisizione di immagine e, successivamente, inseriti manualmente in archivio, nell'apposito raccoglitore *"Documenti in entrata"*.

11.2 Processo di scansione

Il processo di scansione si articolerà, di massima, nelle seguenti fasi:

1. acquisizione delle immagini in modo che ad ogni documento, anche composto da più fogli, corrisponda un unico file in un formato abilitato alla conservazione (PDF/PDF-A);
2. verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
3. collegamento delle rispettive immagini alla registrazione di protocollo, in modo non modificabile;
4. memorizzazione delle immagini, in modo non modificabile.

SEZIONE XII – CONSERVAZIONE E TENUTA DOCUMENTI

12.1 Conservazione dei documenti informatici

La documentazione in archivio di deposito è conservata a cura del Servizio archivistico.
A far data dal 29/07/2016, i documenti informatici del II Circolo Didattico "Giovanni XXIII" di Paternò (CT) sono conservati a cura del Responsabile della Conservazione in modo conforme a quanto previsto dal DPCM 03.12.2013 – Regole tecniche in materia di sistema di conservazione, dal DMEF del 17 giugno 2014, dal DPR 633/72, dalla Circolare dell'Agenzia delle Entrate n. 45/E del 19 ottobre 2005, dalla Circolare dell'Agenzia delle Entrate n. 36/E del 6 dicembre 2006 e loro successive modificazioni o integrazioni.
Al termine delle operazioni di registrazione e segnatura di protocollo, il Responsabile della Conservazione provvede, quindi, in collaborazione con i sistemi informativi e con il supporto della tecnologia disponibile, a conservare i documenti informatici in modo non modificabile e garantendone la leggibilità nel tempo, in appositi archivi informatici e a controllare periodicamente a campione la leggibilità dei documenti stessi. L'intervento del Responsabile della conservazione provvede alla conservazione integrata dei documenti e delle informazioni (metadati), prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi.

12.2 Censimento depositi documentari delle banche dati e dei software

Ogni anno il responsabile della gestione documentale provvede ad effettuare il censimento dei depositi documentari, dei registri particolari, delle banche dati e dei software di gestione documentale in uso all'ente, per programmare i versamenti dei documenti cartacei all'archivio di deposito, dei documenti informatici sui supporti di memorizzazione.

12.3 Selezione e conservazione dei documenti

Ogni anno, in base al massimario di scarto, viene effettuata la procedura di selezione della documentazione da proporre allo scarto e attivato il procedimento amministrativo di scarto documentale con l'invio della proposta alla competente Soprintendenza archivistica. I fascicoli non soggetti ad operazioni di scarto sono trasferiti nell'archivio storico per la conservazione permanente, sia essa analogica o digitale. Il manuale di gestione e i relativi aggiornamenti devono essere conservati integralmente e perennemente nell'archivio dell'Ente.

SEZIONE XIII – PIANO DI SICUREZZA

13.1 Obiettivi del Piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dal C.D. siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

13.2 Generalità

Il piano di sicurezza, **che si basa sui risultati** dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche adottate dall'Istituto, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della scuola;
- le modalità di accesso al Protocollo Informatico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato b) del d.lgs. 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, come aggiornato dal d.lgs. n. 62/2012, in caso di trattamento di dati personali;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

13.3 Formazione dei documenti informatici – aspetti di sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificazione del soggetto che ha formato il documento e l'amministrazione di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti a essere gestiti mediante strumenti informatici e a essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti.

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma digitale o avanzata, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione, come riportato sul sito dell'Agenzia per l'Italia Digitale *(www.agid.gov.it)*, al fine di garantire la loro inalterabilità nel tempo del contenuto e della struttura. A titolo d'esempio si utilizzano preferibilmente PDF e PDF/A.

13.4 Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) presenti o transitate nel sistema di Protocollo Informatico che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;

- dai log dei dispositivi di protezione periferica del sistema informatico (Intrusion Detection System (IDS), sensori di rete e firewall);
- dalle registrazioni del software di Protocollo Informatico.

13.5 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando un sistema di autorizzazione basato sulle credenziali di accesso al proprio computer tramite Active Directory. La profilazione degli utenti avviene in via preventiva e consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad ogni singolo utente.

Il sistema di protocollo informatico adottato dall'istituto:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente del protocollo informatico può accedere solamente ai documenti che sono stati direttamente assegnati. Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

13.6 Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti con il permesso del Responsabile della gestione documentale. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

13.7 Profili utente e responsabilità

Il sistema garantisce la tutela dei dati personali e dei dati sensibili tramite l'assegnazione differenziata dei diritti di modifica e di visualizzazione dei documenti di protocollo in rapporto alle funzioni ed al ruolo svolto dagli utenti.

Il sistema prevede diverse possibilità di combinazione dei profili di accesso al protocollo informatico:

- visibilità: possibilità per un utente abilitato di visualizzare una registrazione di protocollo, con l'esclusione dei documenti riservati;
- inserimento: possibilità per un utente abilitato di inserire i dati e provvedere ad una registrazione di protocollo;
- modifica: possibilità per un utente abilitato di modificare i dati gestionali di una registrazione di protocollo, con l'esclusione dei dati obbligatori;
- annullamento: possibilità di un utente abilitato di annullare una registrazione di protocollo.

13.8 Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene a cura del Responsabile della Conservazione in modo conforme a quanto previsto dal DPCM 03.12.2013 – Regole tecniche in materia di sistema di conservazione, dal DMEF del 17 giugno 2014, dal DPR 633/72, dalla circolare dell'Agenzia delle Entrate n.45/E del 19 ottobre 2005, dalla circolare dell'Agenzia delle Entrate n. 36/E del 6 dicembre 2006 e loro successive modificazioni o integrazioni, come specificato nel Manuale della Conservazione e nella sezione XII.

SEZIONE XIV – ACCESSO

14.1 Accessibilità da parte degli utenti appartenenti all'Amministrazione

La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili e password, o altre tecniche e dispositivi di autenticazione sicura.
L'Amministrazione, in conformità alla normativa vigente, assicura il diritto di accesso ai documenti riguardanti il procedimento amministrativo da parte degli utenti esterni, garantendo la tutela alla riservatezza.
I documenti conservati nell'Archivio sono liberamente consultabili ai sensi del combinato disposto degli artt. 58, 59 e 60 del Testo Unico, fatte salve le norme vigenti sul segreto e sulla tutela della riservatezza.

14.2 Accesso esterno

L'accesso al sistema informatico da parte di utenti esterni può avvenire solo con l'impiego di sistemi di riconoscimento e autenticazione sicuri, basati su certificato digitale secondo quanto previsto dall'art. 65 del d.lgs. 7 marzo 2005, n. 82 e, nei casi di particolari procedimenti amministrativi, con credenziali di accesso rilasciate dall'Ente.

SEZIONE XV – APPROVAZIONE, REVISIONE E PUBBLICAZIONE

15.1 Approvazione

Il presente manuale è adottato dall'Amministrazione con suo provvedimento proprio, su proposta del Responsabile della gestione documentale, dopo aver ricevuto il nulla osta della competente Soprintendenza archivistica

15.2 Revisione

Il presente manuale è rivisto, ordinariamente, ogni due anni su iniziativa del Responsabile della gestione documentale. Qualora se ne presenti la necessità, si potrà procedere a revisione o integrazione del manuale anche prima della scadenza prevista. Le modifiche al manuale sono comunicate alla Soprintendenza archivistica.

15.3 Pubblicazione

Il Manuale di gestione è reso pubblico tramite la sua diffusione sul sito web dell'Amministrazione.

Approvato dal Consiglio di Circolo in data 05/10/2016 con delibera n. 3.

Paternò, lì 19/09/2016

Il Coordinatore del protocollo
(Sig.ra Rosaria Castro)

Il Dirigente Scolastico
(Prof. Roberto Maniscalco)

Manuale della Conservazione

di InfoCert S.p.A.

Società soggetta a direzione e controllo di TecnoInvestimenti S.p.A.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	Luglio 2014	Biagi, Esposito, Maccà, Loffi	*Responsabili*
Verifica		Dal Borgo	Responsabile del servizio della Conservazione
Approvazione		Dal Borgo	Responsabile del servizio della Conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
01	Luglio 2014	Prima versione	
02	Novembre 2015	Utilizzo dello schema proposto da AgID	
03	Febbraio 2016	Correzioni formali e di layout	
04	Marzo 2016	Correzioni formali e di layout	

INDICE DEL DOCUMENTO

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale della Conservazione di InfoCert S.p.A. (Società soggetta a direzione e controllo di TecnoInvestimenti S.p.A.), ai sensi del Decreto del Presidente del Consiglio dei Ministri del 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.
Il 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.
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.

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

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	Processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari

	obblighi di legge.
AGID	Agenzia per l'Italia Digitale.
ARCHIVIO	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un Soggetto Produttore durante lo svolgimento dell'attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
AREA ORGANIZZATIVA OMOGENEA	Insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.
ASP	Application Service Provider.
ATTESTAZIONE DI CONFORMITA' DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITA'	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
BASE DATI	Collezione di dati registrati e correlati tra loro.
CA	Certification Authority.
CAD	Codice Amministrazione Digitale D.lgs. 82 del 7 marzo 2005 e successive modifiche.
CAS	Content Addressed Storage.
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.
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 titoli e classi.
CODICE (DELL'AMMINISTRAZIONE DIGITALE)	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
CODICE ESEGUIBILE	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
CONSERVATORE ACCREDITATO	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia Digitale.
CONSERVAZIONE	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, descritto nel presente manuale di conservazione e che risponde a quanto stabilito nel DPCM del 03 dicembre 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.
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.
D. LGS	Decreto Legislativo.
DPCM	Decreto della Presidenza del Consiglio dei Ministri.
DPR	Decreto del Presidente della Repubblica.
DOCUMENTO ANALOGICO	Rappresentazione analogica di atti, fatti o dati

	giuridicamente rilevanti.
DOCUMENTO INFORMATICO	Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
ESIBIZIONE	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
EVIDENZA INFORMATICA	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
EXTENSIBLE MARKUP LANGUAGE	Linguaggio derivato dall'SGML (Standard Generalized Markup Language), metalinguaggio che permette di creare altri linguaggi. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags).
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	Insieme di dati in forma elettronica allegati oppure connessi

AVANZATA	a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1 comma 1 lettera q-bis) Decreto Legislativo del 7 marzo 2005 n. 82). Si vedano anche le regole tecniche, pubblicate nella G.U. il 21 maggio 2013.
FORMATO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
GU	Gazzetta Ufficiale della Repubblica Italiana.
HSM	Hardware Security Module.
IDENTIFICATIVO UNIVOCO (di seguito detto Token)	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione. Detto anche token LegalDoc.
IMMODIFICABILITA'	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
I.N.RI.M	Istituto Nazionale di Ricerca Metrologica.
INSIEME MINIMO DI METADATI DEL DOCUMENTO INFORMATICO	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM del 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
INTEGRITA'	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
INTEROPERABILITA'	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.

LEGALDOC	Servizio di conservazione digitale a norma di InfoCert.
LEGGIBILITA'	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
MARCA TEMPORALE	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (art. 1, lettera m del DPCM 22 febbraio 2013). La marca temporale emessa in conformità con quanto previsto dal DPCM 22 febbraio 2013, titolo IV è opponibile ai terzi ai sensi dell'art. 41 dello stesso decreto.
MEF	Ministero dell'Economia e delle Finanze.
METADATI	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM del 3 dicembre 2013.
NTP	Network Time Protocol.
OAIS	Open Archival Information System: è lo standard ISO 14721:2003 e definisce concetti, modelli e funzionalità inerenti agli archivi digitali e gli aspetti di digital preservation.
PACCHETTO INFORMATIVO	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
PORTABLE DOCUMENT FORMAT	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	Sistema di posta elettronica nel quale è fornita al mittente

CERTIFICATA	documentazione elettronica attestante l'invio e la consegna di documenti informatici.
PRESA IN CARICO	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
PRODUTTORE	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
PA	Pubblica Amministrazione.
PEC	Posta Elettronica Certificata.
PU	Pubblico Ufficiale.
RAPPORTO DI VERSAMENTO	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore; in LegalDoc è l'insieme degli Indici del Pacchetto di Archiviazione associati ad ogni documento inviato in conservazione in un'unica sessione, che fanno parte del pacchetto di versamento.
REST	Representational State Transfer.
RESPONSABILE DELLA CONSERVAZIONE	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 del DPCM del 3 dicembre 2013.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	Risorsa di InfoCert, che, su affido del Responsabile della Conservazione, gestisce le politiche generali del sistema di conservazione, nel rispetto del modello organizzativo esplicitato nel presente Manuale e di quanto previsto nelle Specificità del Contratto (Atto di affidamento).
RESPONSABILE DELLA GESTIONE DOCUMENTALE O RESPONSABILE DEL SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

ARCHIVI	
RESPONSABILE DELLA SICUREZZA INFORMATICA	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
RESPONSABILE DEL TRATTAMENTO DEI DATI	Persona fisica o giuridica o pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
RIFERIMENTO TEMPORALE	Evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art. 1, lettera m del DPCM 22 febbraio 2013).
SaaS	Software as a Service.
SCARTO	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e/o di interesse storico culturale.
SISTEMA DI CLASSIFICAZIONE	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Nell'ambito della Pubblica Amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico.
STATICITA'	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.
TSA	Time Stamping Authority.
TSS	Time Stamping Service.
TU	Testo Unico.
URL	Universal Resource Locator.
UTC	Universal Coordinated Time – Tempo Universale Coordinato.
UTENTE	Persona fisica, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO AGLI ARCHIVI DI STATO	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello

	Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.
WORM	Write Once Read Many.

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

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

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

comma3, lettera b), 35, comma 2, 36, comma 2, e 71;

- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Torna al sommario

3.2 Standard di riferimento

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

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information

security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

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

Torna al sommario

4. RUOLI E RESPONSABILITÀ

Si riportano di seguito le figure di Responsabilità legate al servizio di conservazione e le rispettive attività di competenza che si sono susseguiti nel tempo in InfoCert:

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
Responsabile del servizio di Conservazione	Pio Barban	• 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.	Dal 1° luglio 2007 al 15 luglio 2008.	
Responsabile del servizio di Conservazione	Antonio Dal Borgo	• 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;	Dal 15 luglio 2008. Assunzione a tempo indeterminato	

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
		• 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.		
Responsabile Sicurezza dei sistemi per la conservazione	Alfredo Esposito	• 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.	Dal 1° gennaio 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;	Dal 2 dicembre 2014 al 31 agosto 2015.	

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
		• 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.		
Responsabile funzione archivistica di conservazione	Marta Gaia Castellan	• 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.	Dal 1° settembre 2015. Assunzione a tempo indeterminato.	
Responsabile trattamento dati personali	Alfredo Esposito	• Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; • Garanzia che il trattamento dei	Dal 1° gennaio 2011. Assunzione a tempo	

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
		dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	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	Dal 1° marzo 2014. Assunzione a tempo indeterminato.	

RUOLI	NOMINATIVI	ATTIVITA'	PERIODO NEL RUOLO	EVENTUALE DELEGA
		hardware e software di base del sistema di conservazione.		
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.	Dal 1° gennaio 2013. Assunzione a tempo indeterminato.	

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Profilo di InfoCert

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

InfoCert S.p.A. 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)

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 "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.Lgs 231)
- Controllo di gestione
- Sistema gestione sicurezza sul lavoro.

Torna al sommario

5.2 Organigramma

L'organigramma di InfoCert è stato depositato presso AgID durante le procedure di accreditamento. Di seguito sono riportate le figure di responsabilità che intervengono nei processi e nelle attività di Conservazione.

Torna al sommario

5.3 Strutture organizzative

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	Soggetto Produttore
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							R
10. Invio al sistema di conservazione del pacchetto di versamento							R

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	Soggetto Produttore
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					E	
15. Scarto dei pacchetti di archiviazione	R	V			A	E	
16. Chiusura del servizio di conservazione al termine di un contratto	R	V			A	E	
17. Conduzione e manutenzione del sistema di conservazione	A				R	E	
18. Monitoraggio del sistema di conservazione	A	V			R	E	
19. Change management		V		V	A	R	
20. Verifica periodica di conformità a normativa e	A	R	V	V	A		

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	Soggetto Produttore
standard di riferimento							

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

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 dai documenti contrattuali descritti al capitolo 10 ‘Specificità del Contratto’ e dagli articoli 5 e 6 del DPCM del 3 dicembre 2013.

Tutte le verifiche in carico al Responsabile del servizio della Conservazione sono garantite anche dal servizio di auditing interno.Il processo di conservazione è normalmente effettuato da procedure totalmente automatizzate, che non necessitano dell'intervento di altri soggetti o delegati.

InfoCert si riserva, come specificato nelle Condizioni generali del Contratto, la possibilità di avvalersi di partner tecnologici per l'esecuzione di operazioni, singole attività, servizi relativi a funzioni o fasi del processo di conservazione, a terzi soggetti, fornitori esterni, che per conoscenza, esperienza, capacità e affidabilità forniscano idonee garanzie.

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

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

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

Per “pacchetto di versamento” si intende l’insieme di documenti che il Soggetto Produttore invia al sistema di conservazione in 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 nelle ‘Specificità del Contratto’ 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, ad oggi, il “pacchetto di distribuzione” coincide con il “pacchetto di archiviazione”.

Eventuali specificità sono concordate con il Soggetto Produttore e descritte nelle ‘Specificità del Contratto’ SPT/NDOC- Specifiche tecniche per l’integrazione e AL/NDOC – Allegato Tecnico al Contratto LegalDoc.

Torna al sommario

6.1 Oggetti conservati

Tipologie documentali, metadati e formati sono sempre concordati con il Soggetto Produttore, e vengono elencati nelle ‘Specificità del Contratto’ - ‘Dati Tecnici di attivazione’.

I visualizzatori dei formati standard, previsti nell’allegato 2 del DPCM 3 dicembre 2013, sono automaticamente assegnati all'atto dell’attivazione del proprio ambiente di conservazione e sono forniti da InfoCert al Soggetto Produttore all'atto di attivazione del servizio. Tutti i documenti inviati in conservazione saranno associati al visualizzatore configurato per il particolare formato.

Qualora un Soggetto Produttore necessiti di formati aggiuntivi rispetto a quelli standard, dovrà segnalarlo nei ‘Dati Tecnici di attivazione’ (compresi nelle ‘Specificità del Contratto’) e conservare gli appositi visualizzatori in una sezione predefinita dell’ambiente assegnato. I formati aggiuntivi devono essere concordati, dunque, tra il Soggetto Produttore e InfoCert in fase contrattuale e non è possibile caricare visualizzatori per formati non preventivamente concordati e configurati nel sistema. 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.

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**	**Soggetto Produttore**
1. Creazione del file dei parametri di upload, del file della scheda tecnica e predisposizione dei file del visualizzatore.							**R**
2. Invio della richiesta al sistema di conservazione.							**R**
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 dello stesso ed invio al soggetto Produttore.	**R**				**E**	**V**	

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

Nel dettaglio:

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

INPUT		Predisposizione file
Sistema di conservazione		Predisposizione del file della scheda tecnica da associare al visualizzatore.
		Predisposizione del file del visualizzatore.
		Creazione del file dei parametri di upload.
OUTPUT		File predisposti

ATT.2 Invio della richiesta al sistema di conservazione

INPUT		*Richiesta di caricamento dei visualizzatori da preparare*
Sistema di Gestione		Invocazione del servizio di caricamento dei visualizzatori da parte del sistema di gestione del Soggetto Produttore.
		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 caricamento dei visualizzatori da validare*

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.
		Invio dell'esito e del file IPDA al Soggetto Produttore.
OUTPUT	*Visualizzatore caricato*	

Torna al sommario

6.2 Pacchetto di versamento

Di seguito è riporta la tabella di sintesi del processo di versamento del pacchetto, 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**	**Soggetto Produttore**

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**	**Soggetto Produttore**
1. Invio al sistema di conservazione del pacchetto di versamento.							**R**
2. Validazione del pacchetto di versamento.	**R**				**E**	**V**	**R**
3. Generazione del pacchetto di archiviazione.	**R**				**E**	**V**	
4. Memorizzazione e creazione “copia di sicurezza”.	**R**			V	**E**	**V**	
5. Invio dell'IPdA al Soggetto Produttore.	**R**						

L'art. 7 comma c) del DPCM del 3 dicembre 2013 introduce, inoltre, l’obbligo 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 (per i dettagli tecnici si rimanda a ‘Specificità del Contratto’ SPT/NDOC- Specifiche tecniche per l’integrazione).

Il rifiuto dei pacchetti di versamento avviene nella modalità descritta nelle 'Specificità del Contratto' SPT/NDOC- Specifiche tecniche per l'integrazione e con le casistiche definite SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc.

Le eventuali personalizzazioni specifiche di un contratto sono descritte nei documenti elencati e descritti nel capitolo 10 - 'Specificità del Contratto'

Torna al sommario

6.3 Pacchetto di archiviazione

Per "pacchetto di archiviazione" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert descritto nelle 'Specificità del Contratto' 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.

L'Indice del Pacchetto di Archiviazione è un file in formato XML, marcato temporalmente e firmato digitalmente dal Responsabile del servizio della Conservazione, generato dal sistema, che contiene i metadati e le informazioni di conservazione del documento e viene con esso conservato.

In particolare nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA
- il token del documento (ovvero il suo identificativo univoco)
- l'operazione eseguita (conservazione, rettifica, scarto e cancellazione)
- il bucket (ovvero l'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'impronta di Hash del documento.

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

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

Torna al sommario

6.4 Pacchetto di distribuzione

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.

Le procedure di esibizione permettono di estrarre dal sistema un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione utilizzando il relativo token (ovvero l'identificativo univoco del documento da esibire). Insieme ai file costituenti il pacchetto di distribuzione, sono rese disponibili anche le informazioni che qualificano il processo di conservazione, ossia il file IPdA e un'Attestazione di corretta conservazione e datacertazione firmata dal Responsabile del servizio di Conservazione.

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.

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.

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 del 03 dicembre 2013 e dell'articolo 5 del DMEF del 17 giugno 2014.

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 al 'MU/ESIB Manuale Utente Esibitore LegalDoc' – 'Specificità del Contratto' per il dettaglio delle funzionalità di verifica del sistema.

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

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

Il sistema consente le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati;
- **conservazione del pacchetto di archiviazione**: il 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 e la rettifica si applica al pacchetto di archiviazione;
- **scarto/cancellazione del pacchetto di archiviazione:** si applica al pacchetto di archiviazione e solo se ritenuto privo di valore amministrativo e di interesse storico culturale dal Produttore. Il sistema terrà comunque evidenza del documento all'interno dell'archivio a norma, nel rispetto del principio di tracciabilità.
- **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, utilizzando uno o più metadati popolati in fase di caricamento;

- **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, quindi, 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.

Torna al sommario

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Di seguito è riporta la tabella che descrive l'acquisizione dei pacchetti, seguendo lo schema: input\dettaglio delle attività\output.

ATT.1 Invio al sistema di conservazione del pacchetto di versamento

INPUT	*Documento da inviare al sistema di conservazione tramite il pacchetto di versamento*	
Sistema di gestione documentale del Soggetto Produttore		Invocazione del sistema di conservazione da parte del sistema di gestione, secondo lo standard descritto nelle SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc.
		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 nelle SPT/NDOC – Specifiche

		tecniche per l'integrazione di LegalDoc.
OUTPUT		*pacchetto di versamento inviato*

Per maggiori dettagli si rimanda al documento "SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc" – 'Specificità del Contratto'.

Torna al sommario

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

ATT.1 Validazione del pacchetto di versamento

INPUT		*Pacchetto di versamento*
Sistema di conservazione		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 al documento e ai file che lo compongono per il mantenimento della tracciabilità delle

		operazioni.
OUTPUT		*pacchetto di versamento verificato*

Torna al sommario

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

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

ATT.1 Generazione del pacchetto di archiviazione

INPUT		*Pacchetto di archiviazione*
Sistema di conservazione		Eventuale apposizione della firma digitale sul file di dati (se prevista da accordi contrattuali appositi esplicitati nei 'Dati Tecnici di attivazione', che fanno parte delle 'Specificità del contratto')
		Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) 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 da 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.2 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.3 Invio dell'IPdA al soggetto Produttore

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

Torna al sommario

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

All'interno delle 'Specificità del Contratto' SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc è presente la griglia riassuntiva dei codici errore che il servizio LegalDoc restituisce in seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto. La griglia riporta le seguenti informazioni:

- Codice di errore - codifica abbreviata dell'errore avvenuto
- Messaggio di errore - breve descrizione dell'errore avvenuto

I campi codice e descrizione vengono inseriti nel corpo della risposta HTTP.

L'assistenza LegalDoc è contattabile mediante l'invio di un messaggio di posta elettronica certificata alla casella: assistenza.legaldoc@legalmail.it dalla casella di posta certificata del Produttore.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Di seguito è riporta la tabella che descrive la gestione dei pacchetti di archiviazione, seguendo lo schema: input\dettaglio delle attività\output.

ATT.1 Verifica del pacchetto di versamento

INPUT	*Pacchetto di versamento*	
Sistema di conservazione	1	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.
	2	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.
	3	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.
	4	Aggiornamento dei database del sistema con i dati relativi al documento e ai file che lo compongono per il mantenimento della tracciabilità delle operazioni.

OUTPUT	*pacchetto di versamento verificato*

ATT.2 Formazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*	
Sistema di conservazione	1	Eventuale apposizione della firma digitale sul file di dati (se prevista da accordi contrattuali)
	2	Creazione del file XML IPdA (Indice del Pacchetto di Archiviazione) 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 assegnato al documento,
	2	Marcatura e firma da parte del Responsabile del servizio di Conservazione del file IPdA. Copia del file sul supporto primario.
	3	Indicizzazione del documento conservato al fine di poter reperire lo stesso in seguito.
	4	Aggiornamento del database del sistema interessato alle modifiche di cui sopra.
OUTPUT	*pacchetto di archiviazione*	

ATT.3 Memorizzazione del pacchetto di archiviazione

INPUT	*Pacchetto di archiviazione*	
Sistema di conservazione	1	Memorizzazione del pacchetto di archiviazione su supporto magnetico, mediante un sistema di archiviazione permanente dei contenuti digitali
	2	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.
	3	La procedura di creazione della copia di sicurezza avviene in maniera automatica e gestita dal sistema di Storage.
OUTPUT	*Documenti conservati*	

Torna al sommario

7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

ATT1. Ricerca del documento da esibire

INPUT	*Lista di token archiviati dal sistema*	
Sistema di Gestione documentale del Soggetto Produttore		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*	
Sistema di Gestione documentale del Soggetto Produttore		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 nelle 'Specificità del Contratto' SPT/NDOC – Specifiche tecniche per l'integrazione di LegalDoc. In questa chiamata viene utilizzato il

		token ricavato in precedenza.
OUTPUT		*Richiesta di esibizione eseguita*

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

INPUT		*Richiesta di esibizione*
Sistema di conservazione		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.4 Risposta 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 distribuzione.
		Invio della risposta al sistema del Soggetto Produttore.
OUTPUT		*Documento esibito*

Torna al sommario

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

Per duplicato si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Per copia si intende il documento informatico avente contenuto identico al documento da cui è tratto, ma con forma diversa.

La conservazione avviene su supporto primario e su supporto secondario, quindi con duplicazione automatica. Come descritto in seguito, tali supporti sono magnetici ad alte capacità e performance, che garantiscono la ridondanza interna del dato. È inoltre eseguito un backup periodico su tape magnetico.

La creazione di copie informatiche, invece, 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.

Possono essere generati anche duplicati o copie attraverso l'Esibitore o su supporto ottico, su specifica richiesta del Soggetto Produttore.

Nel primo caso il Produttore/Utente agisce autonomamente con apposite credenziali attraverso l'Esibitore di LegalDoc. Nel secondo caso il Soggetto Produttore inoltra la richiesta ai suoi riferimenti abituali (help desk o account) che poi provvedono alla veicolazione verso gli operatori interni.

L'intervento di un Pubblico Ufficiale per attestare la conformità di una copia all'originale avviene secondo quanto previsto dagli articoli 22 e 23 del Codice e dalle Regole Tecniche del DPCM del 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Lo scarto avviene mediante cancellazione dei documenti conservati ed è espressamente richiesto dal Soggetto Produttore, mediante apposita lista debitamente firmata. La lista sarà essa stessa oggetto di conservazione.

Per determinare i tempi si rimanda al Massimario di selezione e scarto, collegato con il Titolario o Piano di classificazione e alle informazioni contenute nel Manuale di gestione del protocollo e degli archivi adottato dell'Ente ai sensi del DPCM del 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

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, articolo 21.

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

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

Torna al sommario

7.9 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, il Responsabile del servizio della Conservazione provvede a comunicare al Soggetto Produttore la lista dei pacchetti di archiviazione conservati.

Nel caso di rescissione del contratto, il Responsabile del servizio della Conservazione provvede a consegnare al Soggetto Produttore, su adeguati supporti, i pacchetti di distribuzione, coincidenti con i pacchetti di archiviazione.

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.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

La descrizione dell'architettura generale del sistema di conservazione è stata depositata in AgID in fase di accreditamento.

Il sistema è organizzato su più siti. 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).

Il sistema è reso in modalità SaaS (Softwareas 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 nei documenti delle 'Specificità del Contratto'.

Il sistema è accessibile dalla apposita URL di rete e il Soggetto Produttore richiama il sistema di conservazione secondo le modalità concordate.

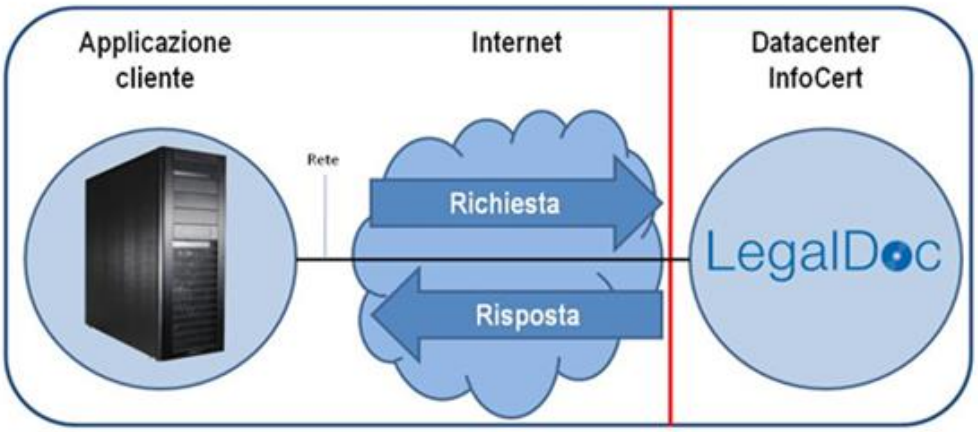

Figura1: Rappresentazione del servizio attraverso la rete

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 dei Soggetti Produttori.

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

Torna al sommario

8.1 Componenti Logiche

Il servizio LegalDoc è basato su tecnologia REST e svolge le operazioni di conservazione, esibizione, rettifica, cancellazione e ricerca.

Torna al sommario

8.2 Componenti Tecnologiche

8.2.1 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 e 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.

Torna al sommario

8.2.2 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.

Torna al sommario

8.2.3 Servizio di marcatura temporale

Per l'emissione delle marche temporali il sistema si avvale del servizio di marcatura di InfoCert, Certification Authority accreditata. 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.

Torna al sommario

8.2.4 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.

Torna al sommario

8.3 Componenti Fisiche

InfoCert, in accordo con i Soggetti Produttori e come previsto dalle Condizioni Generali del Contratto si avvale di partner tecnologici per le componenti fisiche del data center.

Torna al sommario

8.3.1 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.

Torna al sommario

8.3.2 Sistema Storage

Il sistema di conservazione di InfoCert e dei suoi partner tecnologici, 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.

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 e dai suoi partner tecnologici 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 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.

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.

Torna al sommario

8.3.3 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 Metrologica – 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.

Torna al sommario

8.4 Procedure di gestione e di evoluzione

Il sistema di conservazione di 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.

Torna al sommario

8.4.1 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.

Torna al sommario

8.4.2 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.

Torna al sommario

8.4.3 Archivio dei viewer consegnati dal Soggetto Produttore

InfoCert ha stabilito dei formati standard per i documenti da inviare in conservazione, dettagliati nei ‘Dati Tecnici di attivazione’ 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.

Se un 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 dell’interfaccia di LegalDoc, 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.

Torna al sommario

8.4.4 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.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

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 erogati, 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:

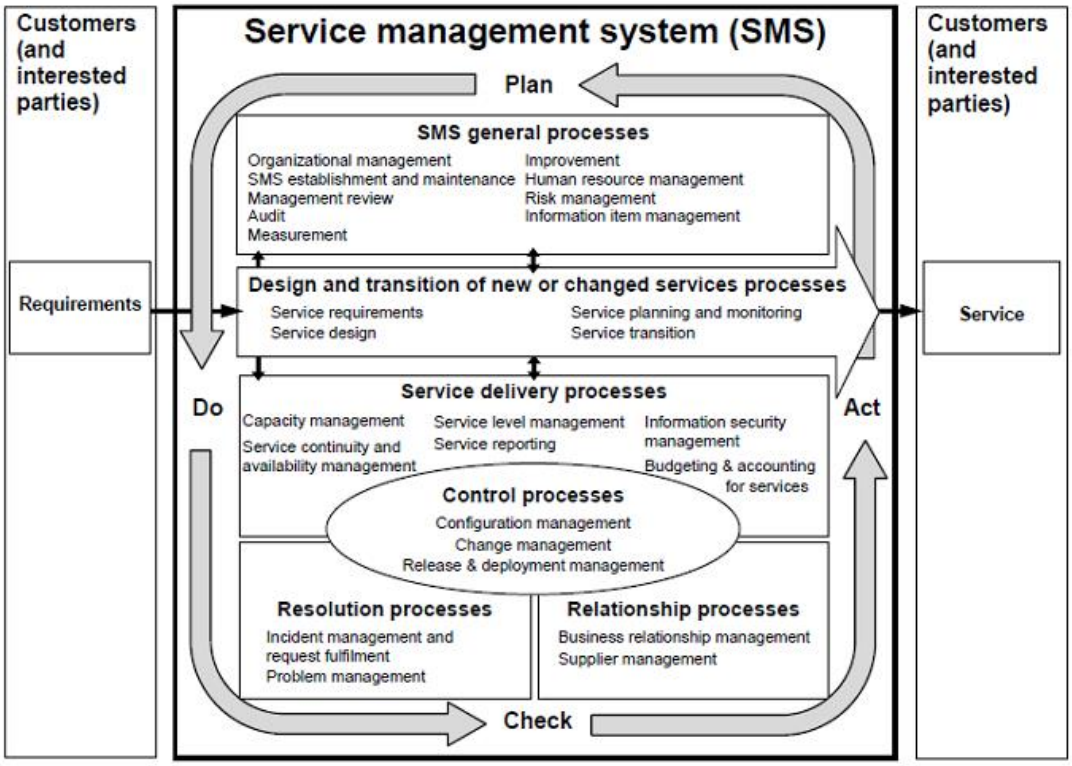

Figura2: Rappresentazione grafica processi della norma ISO/IEC 20000:11

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 dei 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 (Key Performance Indicator):

- Orario di servizio
- Disponibilità di servizio.

Nel documento "Processo MG115/TB02_Processi e Responsabilità_Integrated Management System", depositato in AgID, 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).

Torna al sommario

9.1 Procedure di monitoraggio

Il Data Center di 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.

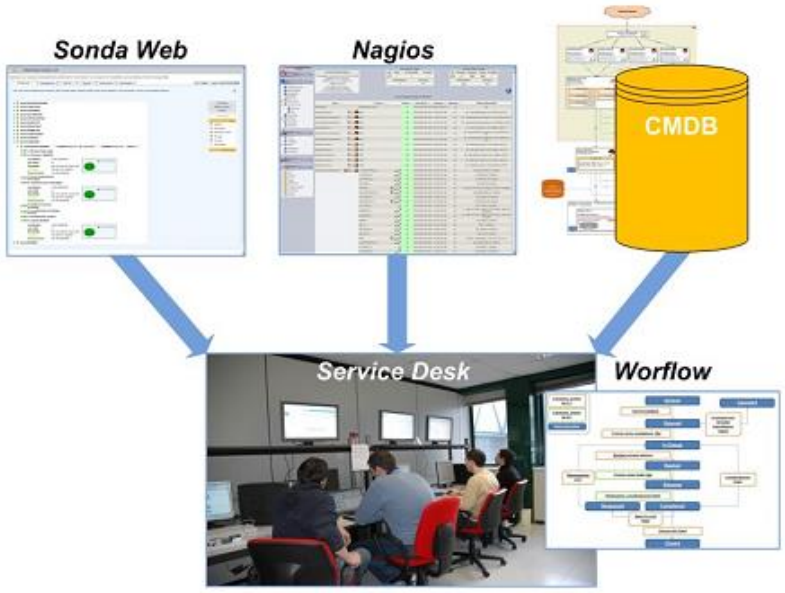

Figura3: Rappresentazione grafica del processo di Incident Management

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).

9.1.1 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.

Torna al sommario

9.1.2 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.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

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 un'ulteriore prova di leggibilità, effettuata direttamente dal Soggetto Produttore.

Inoltre, come descritto dall'art. 7 comma 1 lettera g) del DPCM del 3 dicembre 2013, “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 possano inficiarne 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.

Torna al sommario

9.3 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 e, se presenti, verifica della firma digitale e della marcatura temporale del documento;
- 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 (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 strumento progettato allo scopo. Questo strumento sceglie casualmente un campione di documenti (tipicamente 20) 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.

9.4 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.

Torna al sommario

9.4.1 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.

Torna al sommario

9.4.2 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 è 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.

Torna al sommario

9.4.3 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 Produttore, o di una accettazione globale fatta alla fine del processo produttivo secondo quanto previsto dalla procedura.

Torna al sommario

9.4.4 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.

Torna al sommario

9.5 Soluzioni adottate in caso di anomalie

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.

Torna al sommario

9.5.1 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.

Torna al sommario

9.5.2 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.

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 Management 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 e riguarda 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.

Torna al sommario

10. SPECIFICITÀ DEL CONTRATTO

Il sistema di conservazione di InfoCert è regolato dai seguenti documenti contrattuali, che contengono e descrivono tutte le esigenze richieste dai Soggetti Produttori. La documentazione contrattuale e tecnica elencata è resa disponibile all'atto del perfezionamento dell'accordo di servizio.

1. ***Condizioni Generali di Contratto*** che regola la vendita del servizio di conservazione nelle diverse modalità di erogazione;
2. ***Richiesta di attivazione*** che comporta l'adesione al servizio;
3. ***Dati tecnici per l'attivazione*** con cui il Soggetto Produttore fornisce tutte le informazioni necessarie su tipologie documentali, metadati e credenziali di accesso di cui necessita;
4. ***Atto di affidamento*** che 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, come stabilito dagli articoli 5 e 6 del DPCM del 3 dicembre 2013;
5. ***Specifiche Tecniche di integrazione*** che fornisce tutte le informazioni tecniche necessarie ad operare l'integrazione tra i Sistemi di Gestione documentali del Produttore e il sistema di conservazione di InfoCert;
6. ***Impegno alla riservatezza***;
7. ***Allegato Tecnico*** che descrive le modalità di fornitura del servizio e l'infrastruttura tecnico-tecnologica utilizzata per la sua erogazione;
8. ***Manuale Utente*** che risponde alla necessità di documentare operativamente il processo dal punto di vista del Produttore/Utente;
9. ***Descrizione dei codici di errore*** per fornire una casistica esaustiva dei possibili messaggi di errore del servizio di conservazione e delle azioni che è necessario intraprendere per porvi rimedio.

La documentazione relativa alle procedure e/o ai processi interni di InfoCert, invece, è resa disponibile solo su esplicita richiesta del Soggetto Produttore e all'atto del perfezionamento di una specifica NDA (non-disclosure agreement).

Torna al sommario

Allegato al Manuale del servizio di conservazione dei documenti informatici

DIREZIONE DIDATTICA STATALE II CIRCOLO - "GIOVANNI XXIII"

Indice generale

1. Scopo e campo di applicazione del documento

Il presente documento integra il contenuto del Manuale di conservazione di InfoCert S.p.A., redatto ai sensi del DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione, e reperibile sul sito dell'AgID.

La Scuola, infatti, avvalendosi della facoltà prevista dalle Regole tecniche in materia di sistema di conservazione, ha affidato la conservazione dei documenti informatici da essa prodotti ad InfoCert S.p.A., conservatore accreditato presso AgID, mediante utilizzo del sistema LegalDoc. L'atto di affidamento allo svolgimento delle attività del Responsabile della Conservazione viene conferito dalla Scuola ad InfoCert contestualmente alla sottoscrizione del contratto di adesione al servizio LegalDoc.

In particolare, il presente documento descrive: le classi documentali oggetto di conservazione, le relative policy di conservazione, i metadati utilizzabili per l'indicizzazione dei documenti, e le modalità di integrazione tra il sistema di gestione documentale in uso presso la scuola e il sistema di conservazione.

2. Ruoli e competenze

I ruoli coinvolti nell'iter procedurale vengono descritti nella seguente tabella

Ruolo	**Descrizione**
Produttore	E' il soggetto cui fa capo la responsabilità dello specifico atto oggetto di conservazione nella sua integrità e nel suo contenuto.
Responsabile della conservazione	E' il soggetto, interno al produttore, cui fa capo la responsabilità di verifica del corretto svolgimento del processo di conservazione: trasferimento del pacchetto di versamento al sistema di conservazione e verifica dell'esito della procedura (accettazione o rifiuto).
Conservatore	E' il soggetto cui è stato affidato il Servizio di Conservazione a norma dei documenti nformatici e a cui fa capo la responsabilità del corretto svolgimento del processo stesso.
Responsabile del servizio di conservazione	E' il soggetto, interno al conservatore, che svolge materialmente il processo di conservazione.

2.1 Soggetto Produttore

Ente	DIREZIONE DIDATTICA STATALE II CIRCOLO - "GIOVANNI XXIII"
Sede amministrativa	PATERNO'
Recapiti	Via Vulcano 12
e-mail	ctee06800n@istruzione.it
Codice Ministeriale	CTEE06800N
Bucket	B42038
Policy	P41881

2.2 Responsabili della conservazione

Il responsabile interno della conservazione è MANISCALCO ROBERTO.

3. Descrizione degli oggetti sottoposti a conservazione

3.1 Definizione di documento

L'unità minima oggetto di conservazione è il documento.
Un documento conservato presso il sistema di conservazione ha le seguenti caratteristiche:

- è costituito da un file;
- è memorizzato sui supporti previsti dalla procedura di conservazione;
- è identificato in maniera univoca attraverso una stringa denominata token;
- è conservato insieme al file dei parametri di conservazione, al file di indici del documento e al file di ricevuta (file IPdA).

Il documento viene memorizzato ed esibito come un tutt'uno: non è pertanto possibile estrarre dal sistema parti di un documento.

Ai sensi di legge, la Scuola assicura che i documenti inviati in conservazione sono statici, non modificabili, ovvero redatti in modo tale per cui il contenuto non possa essere alterabile durante le fasi di conservazione ed accesso ed è immutabile nel tempo.

3.2 Formato dei documenti elettronici

I formati gestiti nel processo di conservazione rientrano tra quelli previsti dall'Allegato 2 al DPCM del 3 dicembre 2013, e specificamente sono: xml, pdf, txt, jpeg, gif, tiff, eml. I file possono essere firmati digitalmente e/o marcati temporalmente.
Nessun controllo viene eseguito sulla presenza o meno della firma digitale sui documenti inviati in conservazione.

4. Descrizione del processo di conservazione e di esibizione

Sia il processo di conservazione che di esibizione avvengono mediante invocazione dei rispettivi servizi del sistema LegalDoc, da parte del sistema di gestione documentale Gecodoc, previa autenticazione delle credenziali di accesso.

4.1 Conservazione dei documenti

Il Soggetto Produttore, al momento dell'invio in conservazione, associa ad ogni documento informatico, 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 è firmato dal Responsabile del servizio della conservazione, che attesta la correttezza del processo, ed è marcato temporalmente (in modo da dare certezza del momento temporale in cui è stato formato). La struttura del file IPdA rispecchia quanto richiesto nell'Allegato 4 del DPCM del 2013.
In particolare nel file sono riportati:

- informazioni sull'applicazione che ha generato l'IPdA
- il token del documento;
- l'operazione eseguita;
- il bucket (area di conservazione) associato al Soggetto Produttore e la policy utilizzata;
- il nome del file del documento, del file dei parametri di conservazione e del file di indice, e le rispettive impronte;
- il tempo di creazione (timestamp) del file IpdA.

4.2. File di parametri di conservazione

Il file di parametri contiene le seguenti informazioni

Tag	Descrizione
parameters	Tag radice per la richiesta di conservazione
policy_id	Il codice della Policy con cui si vuole conservare il documento
index_file	Tag contenente le informazioni sul file di indici che si vuole conservare
index_name	Il nome del file di indice che si vuole conservare. E' il nome con cui verrà conservato il file in LegaldDoc
index_hash	E' l'hash calcolato con metodo SHA-256 del file di indice
index_mimetype	Indica il mimetype del file di indice che si vuole conservare
data_file	Tag contenente le informazioni sul file di dati che si vuole conservare
data_name	Il nome del file di dati che si vuole conservare. E' il nome con cui verrà conservato il file in LegaldDoc
data_hash	E' l'hash calcolato con metodo SHA-256 del file di dati
data_mimetype	Indica il mimetype del file di dati che si vuole conservare
path	E' il percorso logico dove si vuole salvare il proprio file di dati

4.3 Classi documentali e policy

Le tipologie documentali oggetto di conservazione sono individuate dal Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi d'intesa con il Responsabile della conservazione. Ai fini della conservazione, i documenti sono organizzati in un unica classe documentale, individuata con la sigla "ae_gen".
Sono esclusi dal processo di conservazione i documenti informatici rilevanti a fini tributari e i documenti analogici originali unici. I documenti vengono conservati per un periodo di 10 anni dalla data di acquisizione del documento da parte del sistema LegalDoc.

4.4 Metadati

Per la classe documentale "ae_gen" vengono definiti i seguenti metadati

Label	Indice	Controllo obbligatorietà
data documento	__data_documento_dt	si
oggetto	oggetto_s	no
numero di protocollo	numero_protocollo_i	no
data di protocollo	data_protocollo_dt	no
soggetto interessato	denominazione_s	no
codice fiscale	codice_fiscale_s	no
partita IVA	partita_iva_s	no
data inizio periodo di imposta	__data_ inizio_numerazione_dt	no
periodo di imposta	__anno_fiscale_i	no
data_fattura	data_fattura_dt	no
numero fattura	numero_fattura_s	no
numero di registrazione	__numero_documento_l	no
data di registrazione	data_registrazione_dt	no
progressivo inizio	__progr_inizio_l	no
progressivo fine	__progr_fine_l	no
numero documento	numero_documento_s	no
data inizio	data_inizio_dt	no
data fine	data_fine_dt	no
periodo di competenza	periodo_comp_s	no
anno	anno_i	no
anno scolastico	anno_scolastico_s	no
id documento	id_documento_s	no
sede	sede_s	no
classe	classe_s	no
materia	materia_s	no
progetto	progetto_s	no
codice ipa	cod_ipa_s	no
codice aoo	cod_aoo_s	no
codice registro	cod_registro_s	no
tipo documento	tipo_documento_s	no
descrizione file	des_allegato_s	no
nome file	des_nomefile_s	no
note	note_s	no
indice fascicolo	__indice_fascicolo_s	no

L'indicizzazione dei documenti è fatta in automatico dal sistema di gestione documentale GECODOC, sulla base dei dati associati ai documenti - in fase di caricamento degli stessi al sistema - da parte degli utenti della Scuola.

I documenti conservati e i relativi metadati non possono essere oggetto di successive modifiche.

5. Esibizione dei documenti

La procedura di esibizione permette di estrarre dal sistema LegalDoc un pacchetto di distribuzione per cui sia stata completata correttamente la procedura di conservazione, 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 restituisce il documento in un unico pacchetto di distribuzione in formato zip.

6. Allegati

Si fornisce di seguito l' elenco dei documenti contrattuali relativi al servizio di conservazione.

1. Affidamento del procedimento di conservazione sostitutiva: formalizza l'affidamento ad InfoCert del processo di conservazione, delineandone l'ambito di applicazione;
2. Allegato A - Condizioni Generali di Contratto LegalDoc: regola il rapporto tra InfoCert e la Scuola;
3. Documentazione tecnica e contrattuale stipulata con ARGO Software.

Data:08/09/2016

Firmato digitalmente da

ROBERTO MANISCALCO

Data e ora della firma: 06/10/2016 08:45:16