ISTITUTO COMPRENSIVO STATALE VIA MANIAGO

Via Maniago, n. 30

20134 Milano (MI)

Codice Meccanografico: MIIC8D4005– C.F. 97154750158

Sito web istituzionale: www.icsbuzzati.gov.it

Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi (artt. 3 e 5 dPCM 03/12/13)

INDICE

Sezione 12 *Accesso*

Sezione 13 *Approvazione, revisione e pubblicazione*

Allegati

1 *Disposizioni generali*

1.1[1] *Ambito di applicazione*

Il presente manuale è adottato ai sensi degli articoli 3 e 5 del DPCM 3 dicembre 2013 per la gestione delle attività di formazione, registrazione, classificazione, fascicolazione, gestione e conservazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti del dell'Amministrazione.
Esso descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la gestione documentale.
Regolamenta inoltre le fasi operative per la gestione informatica dei documenti, nel rispetto della normativa vigente in materia di trasparenza degli atti amministrativi, di tutela della *privacy* e delle politiche di sicurezza.

1.2 *Definizioni dei termini*

Per quanto riguarda la definizione dei termini, che costituisce la corretta interpretazione del dettato del presente manuale, si rimanda al glossario (Allegato n. 1) [2].

1.3 *Storia delle versioni del documento*[3]

Versione	**Data**	**Descrizione**
1.0	24/08/2017	Versione iniziale

[1] La numerazione degli articoli del manuale è autonoma per sezione.
[2] Quando nell'articolato del manuale si rimanda, per specificazioni ulteriori, a un altro documento allegato, è necessario indicare chiaramente gli estremi dell'allegato, come nel testo del documento citato deve essere fatto rimando al manuale.
[3] Indicare sotto forma di tabella la storicizzazione delle varie versione.

1.4 *Differenze rispetto alla versione precedente*[4]

Versione	**Changelog**
1.0	Versione iniziale

1.5 *Area organizzativa omogenea*

Ai fini della gestione dei documenti è individuata una sola area organizzativa omogenea denominata Istituto Comprensivo Statale Via Maniago[5] composta dall'insieme di tutte le sue unità organizzative come da elenco allegato (Allegato n. 2). Il codice identificativo dell'area è istsc_miic8d4005 [6].

1.6 *Servizio per la gestione documentale e i suoi responsabili*

Nell'ambito dell'area organizzativa omogenea, ai sensi della normativa vigente sono istituiti, con atti **(**Allegati nn. 3, 4 e 5**)**, il Servizio di gestione documentale; il Servizio per la sicurezza informatica[7]. Ai servizi sono preposti dei responsabili e dei vicari espressamente nominati. È altresì nominato il Responsabile della Conservazione[8], che d'intesa con il Responsabile della gestione documentale e il Responsabile dei sistemi informativi svolge le funzioni definite all'art. 7 delle regole tecniche sulla conservazione, tra cui la predisposizione e l'aggiornamento del Manuale della Conservazione, garantendo la conservazione integrata dei documenti e delle informazioni di contesto generale, prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi.

---

[4] Indicare sotto forma di tabella le differenze rispetto all'ultima versione.

[5] Inserire il nome dell'ente/Istituzione/Organizzazione: es. Amministrazione comunale di; Comune di; Azienda Ospedaliera ecc.

[6] Indicare l'eventuale codice identificativo dell'area organizzativa. Un'amministrazione può avere una o più Aree Organizzative Omogenee (AOO). Ai sensi dell'art.12, comma 2, lett. g, viene trasmesso presso l'Indice delle Pubbliche Amministrazioni l'elenco degli uffici utente per ciascuna area organizzativa omogenea. A ciascun ufficio utente è assegnato automaticamente dall'Indice delle Amministrazioni il codice identificativo associato, che lo identifica univocamente all'interno dell'Indice stesso. Inserire nell'organigramma gli uffici utente e i relativi codici assegnati dall'Indice delle PA.

[7] Qualora un ente abbia più Aree Organizzative Omogenee (AOO) sono identificati in ciascuna delle area i servizi di cui all'articolo. L'ente ha inoltre la facoltà di nominare il *Coordinatore della gestione documentale* e un suo vicario per i casi di vacanza, assenza o impedimento del primo. La nomina del sostituto o vicario può essere effettuata contestualmente a quella del Responsabile, con un atto successivo oppure ogni volta se ne presenti la necessità. In un ente/organizzazione di piccole-medie dimensioni le figure sopra citate potranno coincidere con un'unica persona.

[8] Questa figura può coincidere con quella del Responsabile della gestione documentale o con il Responsabile dei sistemi informativi. Nel caso in cui il Conservatore è esterno all'ente/organizzazione il conservatore sarà individuato nel soggetto esterno.

Il Responsabile della conservazione, di concerto con il Responsabile dei sistemi informativi dell'ente/organizzazione, provvede altresì alla conservazione degli strumenti di descrizione, ricerca, gestione e conservazione dei documenti.

1.7 *Unicità del protocollo informatico*

La numerazione delle registrazioni di protocollo è unica, progressiva, corrisponde all'anno solare ed è composta da almeno sette numeri, tuttavia a norma dell'articolo 53, comma 5 del dPR 445/00 sono possibili registrazioni particolari. Il sistema informatico di gestione del protocollo è sincronizzato per il calcolo dell'ora con i server su cui risiede l'applicativo, a loro volta sincronizzati con un orologio atomico. L'Amministrazione non riconosce validità a registrazioni particolari che non siano quelle individuate nell'elenco allegato (Allegato n. 6).
Ad ogni documento è dato un solo numero, che non può essere utilizzato per la registrazione di altri documenti anche se correlati allo stesso.

1.8 *Modello operativo adottato per la gestione dei documenti*

Per la gestione dei documenti è adottato un modello operativo decentrato[9] che prevede la partecipazione attiva di più soggetti ed uffici utenti abilitati a svolgere soltanto le operazioni di loro competenza di cui all'elenco allegato (Allegato n. 7), le abilitazioni sono rilasciate/revocate dal responsabile del servizio di gestione documentale[10]. L'archivio storico e di deposito analogico sono conservati presso l'Archivio Generale dell'Istituto, situato nei locali denominati Archivio ubicati nella sede dell'Istituto [11], quello corrente è conservato presso le unità organizzative. La documentazione informatica è gestita secondo le modalità descritte nel Piano per la sicurezza informatica (Allegato n. 8) e conservata presso il suddetto archivio. [12].

[9] Sono due prevalentemente i modelli di protocollo decentrato: uno prevede il totale decentramento della registrazione dei documenti sia in entrata sia in uscita; l'altro prevede la gestione centralizzata delle entrate e decentralizzata delle uscite; con gestione mista, per entrambi i modelli, delle registrazioni particolari: a esempio, gestione centralizzata delle delibere di giunta e consiglio, decentralizzata di altre tipologie documentarie legate a specifici procedimenti amministrativi: edilizia, commercio, polizia locale, ecc. Le postazioni di protocollo decentralizzato, coordinate dal servizio di gestione documentale dell'ente, svolgono ciascuna le funzioni previste dal manuale e pertanto dovranno essere dotate delle varie attrezzature (timbri, etichettatrici ecc.) relative alla gestione documentale: per esempio nel caso di gestione cartacea delle uscite, il timbro di segnatura/etichetta dovrà essere apposto sulla minuta dal responsabile/operatore della postazione decentrata ecc. Il decentramento può essere anche pensato come abilitazione alla protocollazione data ad ogni responsabile di procedimento. In questo caso i problemi organizzativi relativi alla gestione dei documenti analogici e le attrezzature (timbri, etichettatrici ecc.) si moltiplicano, a meno che non si voglia procedere con la gestione manuale delle operazioni di segnatura e classificazione.
In alternativa al modello decentrato è possibile istituire un modello centralizzato dove tutte le operazioni di amministrazione e protocollazione dei documenti sono gestite dal servizio di gestione documentale.

[10] Il sistema di gestione documentale e di protocollo informatico deve prevedere una acces control list per l'assegnazione differenziata di profili di abilitazione per la gestione dei documenti sulla base dei ruoli svolti dagli utenti.

[11] Indicare il luogo/i di conservazione, se lo stesso è a norma, i metri lineari della documentazione, gli estremi cronologici della stessa, se esistono inventari ecc.

[12] Indicare il o i conservatori. Si fa qui riferimento a varie tipologie di documentazione come per esempio i mandati di pagamento ecc. Per tutte le altre specificazioni si rimanda alla sezione apposita del manuale.

2 Formazione dei documenti

2.1 *Requisiti minimi del documento*

Indipendentemente dal supporto su cui sono formati i documenti prodotti dall'ente/organizzazione devono riportare le seguenti informazioni:

- denominazione dell'ente/organizzazione
- indirizzo (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, indirizzo di posta elettronica istituzionale dell'ente/organizzazione, **PEC**)
- indicazione del settore, servizio o ufficio che ha prodotto il documento
- luogo e data
- destinatario
- classificazione
- numero di protocollo
- oggetto del documento: un solo oggetto per documento
- testo
- numero degli allegati (se presenti)
- indicazione dello scrittore del documento
- sottoscrizione autografa o elettronico/digitale del responsabile
- indicazione del Responsabile del procedimento

2.2 *Formazione dei documenti informatici*

L'ente/organizzazione forma gli originali dei propri documenti con mezzi informatici secondo le regole tecniche di cui all'articolo 71 del CAD, mediante l'utilizzo di appositi strumenti software[13]. Le tipologie particolari di documenti per i quali si stabiliscono modalità di trattamento specifiche e/o prodotti mediante modelli standard sono indicati nell'allegato (Allegato n. 9).

2.3 *Formato dei documenti informatici*

I documenti informatici prodotti dall'ente/organizzazione, indipendentemente dal *software* utilizzato, prima della loro sottoscrizione con firma elettronico/digitale, sono convertiti in uno dei formati *standard* previsti dalla normativa vigente in materia di conservazione[14]. L'ente/organizzazione per la formazione

[13] Il documento informatico assume la caratteristica di immodificabilità quando forma e contenuto non sono alterabili durante le fasi di tenuta e accesso e sia garantita la staticità nella fase di conservazione. Gli atti formati con strumenti informatici, i dati e i documenti informatici dell'ente costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, copie e duplicati per gli usi consentiti dalla legge.
La copia o l'estratto di uno o più documenti informatici può essere sottoscritta con firma digitale o firma elettronica qualificata da chi effettua la copia. Affinché la copia non sia disconoscibile essa deve essere firmata da un pubblico ufficiale. I duplicati informatici di un documento informatico sono prodotti mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine. Nella formazione dei documenti informatici effettuata nei diversi gestionali, viene attuato un controllo delle versioni degli stessi, tenendo traccia dei loro passaggi e trasformazioni fino alla versione definitiva inviata alla registrazione e, ove richiesto, vengono conservate le versioni stesse.

[14] L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'allegato 2 delle regole tecniche di cui al DPCM 3 dicembre 2013 in modo da assicurare l'indipendenza dalle piattaforme

dei documenti informatici, delle copie e degli estratti informatici adotta i seguenti formati: (elencare i formati, ad esempio PDF, PDF/A, TIFF, XML, OOXML, ODF, TXT ecc.)[15].

2.4 *Metadati dei documenti informatici*

Al documento informatico è associato l'insieme minimo dei metadati, con riferimento all'allegato 5 delle regole tecniche del CAD[16].
L'insieme minimo dei metadati è il seguente:

- identificativo univoco e persistente e/o numero di protocollo;
- data di chiusura e/o di protocollazione;
- oggetto;
- soggetto produttore, identificazione/codice univoco che identifica l'ente/organizzazione;
- destinatario;
- numero allegati e descrizione;
- impronta digitale.

I metadati dei documenti informatici soggetti a registrazione particolare sono individuati nell'allegato (Allegato n. 10).

2.5 *Sottoscrizione dei documenti informatici*

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma elettronico/digitale conforme alle disposizioni di legge. L'ente/organizzazione utilizza:[17]

- firma digitale.

tecnologiche, l'interoperabilità tra sistemi informatici e la durata nel tempo dei dati in termini di accesso e di leggibilità.

[15] Indicare eventuali ulteriori formati utilizzati per la formazione del documento informatico in relazione a specifici contesti operativi esplicitati e motivati; oppure fare riferimento agli standard di legge senza citarli.

[16] Al documento amministrativo informatico sono inoltre associati i metadati indicati nell'art. 53 del D.P.R. 445/2000 e quelli previsti dall'art. 9 del DPCM 3 dicembre 2013.

[17] Indicare per ciascuna tipologia di firma gli strumenti tecnologici utilizzati.

3 *Ricezione dei documenti*

3.1 *Ricezione dei documenti su supporto analogico*

I documenti su supporto analogico possono arrivare all'ente/organizzazione attraverso:
- il servizio postale;
- la consegna diretta agli uffici, ai funzionari, o agli uffici utente/sportelli URP abilitati presso l'amministrazione al ricevimento della documentazione.

I documenti, esclusi quelli non soggetti a registrazione di protocollo, devono pervenire al protocollo per la loro registrazione. Le buste dei documenti analogici pervenuti non si inoltrano agli uffici destinatari e non si conservano; le buste di assicurate, corrieri, espressi, raccomandate ecc. si inoltrano insieme ai documenti[18].

Non è presente una gestione associata di servizi[19].

3.2 *Ricezione dei documenti informatici*

Le comunicazioni e i documenti informatici sono valide ai fini del procedimento amministrativo una volta che ne sia accertata la loro provenienza e siano prodotti con formati *standard* previsti dalla normativa vigente[20].
I documenti ricevuti in un formato diverso da quelli prescritti dalla normativa e dal presente manuale, nonché cartelle o documenti in formati di compressione (es: .zip, .rar, .7-zip, .ace, ecc.), sono recepiti dal sistema e non convertiti in uno dei formati standard previsti.

Il certificato di firma è verificato da parte delle postazioni abilitate alla registrazione dei documenti in ingresso e/o dal responsabile del procedimento. In caso di certificati scaduti o revocati si rimanda alla Sezione 5.

3.3 *Ricezione dei documenti informatici attraverso PEC (Posta Elettronica Certificata)*

Gli indirizzi di posta elettronica certificata sono pubblicati sul sito web dell'ente/organizzazione[21].

3.4 *Ricezione dei documenti informatici attraverso posta elettronica ordinaria*

La ricezione dei documenti informatici soggetti alla registrazione di protocollo trasmessi da posta elettronica ordinaria è garantita dalle caselle di posta elettronica ordinaria istituzionale.
Gli indirizzi di posta elettronica ordinaria abilitati alla ricezione di documenti informatici soggetti a protocollazione sono resi pubblici sul sito web istituzionale[22].

---

[18] Verificare la possibilità di introdurre un articolo sulla apertura dei documenti analogici.
[19] La gestione associata di servizi interessa principalmente i comuni che, associandosi in unione, associazione intercomunale o consorzio ecc., trasferiscono funzioni agli enti associativi al fine di garantirne un migliore funzionamento.
[20] Indicare se il controllo degli standard viene effettuato in automatico dal sistema di gestione documentale, se di competenza delle postazioni di protocollo in ingresso o ai responsabili di procedimento.
[21] Qualora l'ente utilizzi la PEC anche per la ricezione di documenti informatici provenienti da indirizzi di posta elettronica ordinaria, sarà necessario integrare l'articolo.
[22] Questo articolo va inserito qualora l'ente abbia legato al protocollo più di una casella di posta elettronica ordinaria. Per quanto

3.5 *Ricezione dei documenti informatici attraverso fax management*

L'ente/organizzazione riceve i documenti informatici attraverso un sistema di fax management come descritto nella sezione 7.

3.6 *Ricezione dei documenti informatici attraverso moduli, formulari e altri sistemi*

L'ente/organizzazione riceve i documenti informatici creati dall'utente attraverso i moduli e i formulari resi disponibili mediante gli applicativi *web* elencati nell'allegato n. 7 e tramite trasmissioni telematiche, sistemi di cooperazione applicativa e altri supporti[23].

3.7 *Acquisizione dei documenti analogici o tramite copia informatica*

L'ente/organizzazione può acquisire i documenti analogici attraverso la copia per immagine su supporto informatico di un documento originale analogico e/o attraverso la copia informatica di un documento originale analogico.
Le copie per immagine sono prodotte mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto. Le copie per immagine di uno o più documenti analogici possono essere sottoscritte con firma digitale o firma elettronica qualificata da chi effettua la copia. Affinché le copie non siano disconoscibili esse devono essere firmate da un pubblico ufficiale.
Dei documenti analogici ricevuti viene effettuata copia conforme digitale e il documento originale viene trattenuto presso la postazione di protocollo[24].
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.
Il processo di scansione della documentazione cartacea è descritto nella Sezione 10.
La copia informatica di un documento analogico, è acquisita nel sistema mediante processi e strumenti che assicurino che il documento informatico abbia contenuto identico a quello del documento analogico da cui è tratto.
L'unitarietà è garantita dal sistema mediante il numero di protocollo, l'indice di classificazione e il numero di repertorio del fascicolo.

3.8 *Ricevute attestanti la ricezione dei documenti*

La ricevuta della consegna di un documento analogico può essere prodotta con qualsiasi mezzo che ne attesti il giorno della consegna. Alla registrazione di protocollo vengono associate le ricevute generate dal sistema di gestione documentale e, nel caso di registrazione di messaggi posta elettronica certificata spediti, anche i dati relativi alla consegna rilasciati dal sistema di posta certificata correlati al messaggio oggetto di registrazione.

---

riguarda la gestione della posta elettronica vedi quanto descritto nella Sezione 8.
[23] Indicare i sistemi in uso. Con altri supporti si intendono quelli rimovibili.
[24] Una gestione diversa dei documenti analogici a seguito di scansione sostitutiva dovrà essere descritta. Se un ente non effettua scansione sostitutiva dovrà dichiararlo e indicare come gestisce i documenti analogici nella sezione 5.

3.9 *Orari di apertura per il ricevimento della documentazione*

Gli uffici abilitati al ricevimento dei documenti sono delegati dal Responsabile della gestione documentale all'apertura di tutta la corrispondenza analogica e informatica pervenuta all'ente/organizzazione, salvo i casi particolari specificati nella Sezione 7 .
L'apertura di peculiari tipologie documentali, anche oggetto di registrazione particolare, è delegata ai Responsabili di procedimento. Gli orari di apertura degli uffici sono indicati sul sito web.

4 *Registrazione dei documenti*

4.1 *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. È cura del Responsabile del procedimento verificarne le caratteristiche.

4.2 *Documenti non soggetti a registrazione di protocollo*

Sono esclusi dalla registrazione di protocollo: gazzette ufficiali, bollettini ufficiali, notiziari della pubblica amministrazione, note di ricezione delle circolari e di altre disposizioni, materiale statistico ricevuto, atti preparatori interni, giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti quei documenti già soggetti a registrazione particolare da parte dell'ente/organizzazione il cui elenco è allegato al presente manuale (Allegato n. 11)[25].

4.3 *Registrazione di protocollo dei documenti ricevuti e spediti*

La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione[26]. I requisiti necessari di ciascuna registrazione di protocollo sono:

- numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e numero di protocollo dei documenti ricevuti, se disponibili;
- impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
- classificazione: categoria, classe, fascicolo (si veda titolario);

  assegnazione.

Inoltre possono essere aggiunti:

- data di arrivo;
- allegati (numero e descrizione);
- estremi del provvedimento differimento dei termini di registrazione;
- mezzo di ricezione/spedizione (PE, PEC, altre modalità di ricezione informatica e analogica);
- ufficio di competenza;
- tipo di documento;
- livello di riservatezza;
- elementi identificativi del procedimento amministrativo, se necessario;
- numero di protocollo e classificazione: categoria, classe, fascicolo, del documento ricevuto.

[25] L'elenco delle registrazioni particolari varia a seconda della tipologia dell'ente: comune, provincia, camera di commercio ecc. e dalle varie disposizioni di leggi o regolamenti.

[26] Di norma, i documenti interni sono protocollati in arrivo, a meno che il software di protocollo non preveda una voce specifica.

4.4 *Formazione dei registri e repertori informatici particolari*

L'ente/organizzazione forma i propri registri e repertori informatici particolari mediante la generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.
I registri, i repertori, gli albi e gli elenchi e le raccolte di dati concernenti stati, qualità personali e fatti sono indicati (Allegato n. 12).
Periodicamente il Responsabile della gestione documentale, di concerto con il Responsabile dei sistemi informativi provvede ad effettuare il censimento delle banche dati e dei software di gestione documentale in uso all'interno dell'ente/organizzazione.
Ogni registrazione deve riportare necessariamente:

- dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile);
- dati di classificazione;
- numero di repertorio progressivo e annuale (generato in modo non modificabile).

4.5 *Registrazione degli allegati*

Il numero e la descrizione degli allegati sono elementi essenziali per l'efficacia di una registrazione. Nella registrazione di protocollo/particolare si riporta la descrizione della tipologia degli allegati e, se significativi, anche dei loro estremi (data, numero, ecc).
Tutti gli allegati devono pervenire con il documento principale alle postazioni abilitate alla protocollazione al fine di essere inseriti nel sistema di gestione documentale. In presenza di allegati analogici su ciascuno è riportata la segnatura di protocollo.
Il sistema di gestione documentale gestisce in forma automatizzata gli allegati, come descritto nel manuale operativo del software (Allegato n. 13).

4.6 *Segnatura di protocollo*

La segnatura di protocollo apposta o associata al documento è effettuata contemporaneamente alla registrazione di protocollo o di altra registrazione cui esso è soggetto[27].
I requisiti necessari di ciascuna segnatura di protocollo sono:

- codice identificativo dell' ente/organizzazione
- codice identificativo dell'area organizzativa omogenea
- codice identificativo del registro
- data di protocollo
- progressivo di protocollo

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 comprendono anche:

[27] La segnatura dei documenti analogici può avvenire con il classico timbro o con l'utilizzo di etichette (specificare che tipo di mezzo si utilizza). In un sistema di protocollo decentrato tutte le postazioni di protocollo dovranno avere il timbro o

- oggetto del documento
- mittente
- destinatario/i

Inoltre possono essere aggiunti:

- persona o ufficio destinatari
- classificazione e fascicolazione di competenza
- identificazione degli allegati
- informazioni sul procedimento e sul trattamento

4.7 *Annullamento delle registrazioni di protocollo*

Le registrazioni di protocollo/particolare, tutte o in parte, possono essere annullate/modificate con una specifica funzione del sistema di gestione informatica dei documenti, a seguito di motivata richiesta scritta al responsabile del servizio o per iniziativa dello stesso. Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema. Il sistema durante la fase di annullamento registra gli estremi del provvedimento autorizzativo redatto dal responsabile del servizio. Le richieste di annullamento dei numeri di protocollo devono pervenire in forma scritta al responsabile del servizio. Sui documenti cartacei è apposto un timbro che riporta gli estremi del verbale di annullamento; il documento è conservato, anche fotoriprodotto, a cura del responsabile del servizio di gestione documentale insieme al verbale.
Non è possibile annullare il solo numero di protocollo e mantenere valide le altre informazioni della registrazione.
Le registrazioni annullate/modificate rimangono memorizzate nel data base e sono evidenziate dal sistema, il quale registra l'iter che ha portato all'annullamento.

4.8 *Differimento dei termini di protocollazione*

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.

4.9 *Registro giornaliero e annuale di protocollo*

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto secondo quanto previsto nel Manuale di conservazione.
Delle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.

4.10 *Registro di emergenza*

Le procedure adottate dal Responsabile della gestione documentale per l'attivazione, la gestione e il recupero dei dati contenuti nel registro di emergenza sono descritte (Allegato n. 14).

---

l'etichettatrice.

5 *Documentazione particolare*

5.1 *Deliberazioni di giunta e consiglio, determinazioni dirigenziali, decreti, ordinanze, contratti, verbali sanzioni amministrative polizia locale e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti, pubblicazioni all'albo online e notifiche.*

Le deliberazioni di giunta e consiglio, le determinazioni dirigenziali, i decreti, le ordinanze, i contratti, i verbali della polizia locale e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti, se sono documenti già soggetti a registrazione particolare da parte dell'ente/organizzazione possono non essere registrati al protocollo. Il software di produzione e conservazione di questa tipologia particolare di documentazione deve consentire di eseguire su di essi tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico[28]. Ogni registrazione deve riportare necessariamente:

- dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile);
- dati di classificazione e fascicolazione;

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

Per le pubblicazioni all'albo online e per le notifiche si rimanda alle apposite linee guida pubblicate dall'AGID (Allegati n. 15).

5.2 *Documentazione di gare d'appalto*

Per la documentazione delle gare telematiche l'ente/organizzazione utilizza le piattaforme del mercato elettronico in uso, secondo la normativa vigente.
Per la documentazione relativa a gare gestite al di fuori del mercato elettronico, per ragioni di sicurezza, si riceve di norma per via telematica solo la registrazione del partecipante alla gara e la documentazione che non faccia esplicito riferimento all'offerta economica, che invece dovrà essere inviata in cartaceo o tramite sistemi informatici di criptazione dell'offerta. Le buste contenenti le offerte sono registrate al protocollo senza effettuarne l'apertura. Dopo l'apertura a cura dell'ufficio che gestisce la gara dovranno essere riportati su ciascun documento la data e il numero di protocollo assegnato alla busta[29].

5.3 *Documenti con mittente o autore non identificabile, posta personale*

I documenti, analogici o digitali, ricevuti e indirizzati al personale dell'ente/organizzazione e quelli di cui non sia identificabile l'autore sono regolarmente aperti e registrati al protocollo, salvo diversa valutazione[30]. Non si registra la posta indirizzata nominalmente sulla busta sia indicata la dicitura "personale" o "riservata personale". Il destinatario di posta elettronica su indirizzo personale rilasciato dall'ente/organizzazione potrà richiederne la registrazione inoltrando il messaggio al protocollo.

[28] In un sistema di protocollo informatico anche le registrazioni particolari devono essere prodotte da un sistema informatico e non più cartaceo.
[29] Per la gestione di gare d'appalto ecc. svolte su sistemi gestionali di altri enti SINTEL, MEPA ecc. devono essere indicate le modalità di conservazione dei documenti prodotti, tenendo conto di quanto dichiarato dei gestori di tali sistemi a riguardo della conservazione documentale.
[30] Indicare eventuali procedure diverse.

5.4 *Documenti informatici con certificato di firma scaduto o revocato*[31]

Nel caso in cui l'ente/organizzazione riceva documenti informatici firmati digitalmente il cui certificato di firma risulta scaduto o revocato prima della sottoscrizione, questi verranno protocollati e inoltrati al responsabile di procedimento che farà opportuna comunicazione al mittente[32].

5.5 *Documenti inviati via fax*

La normativa vigente prevede l'esclusione della corrispondenza via fax fra pubbliche amministrazioni. La trasmissione di documenti via *fax* con cittadini o altri soggetti privati non aventi l'obbligo di comunicazione in forma telematica con la pubblica amministrazione richiede la registrazione di protocollo. L'ente/organizzazione utilizza per la ricezione e l'invio di fax un sistema di *fax management,* che consente l'acquisizione dei documenti in formato elettronico tramite la/le casella/e di posta elettronica integrate nel sistema di gestione documentale[33].
Di norma al *fax* non segue mai l'originale. Qualora successivamente arrivasse anche l'originale del documento, a questo sarà attribuito lo stesso numero di protocollo.

5.6 *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 necessita la distribuzione interna all'ente/organizzazione, si faranno copie immagine degli stessi.

5.7 *Allegati*

Tutti gli allegati devono essere trasmessi con i documenti a cui afferiscono all'ufficio/postazioni decentrate di protocollo per la registrazione. Su ogni allegato analogico è riportato il timbro della segnatura di protocollo. Il sistema informatico provvede automaticamente a registrare gli allegati come parte integrante di un documento elettronico. Nel caso in cui una PEC contenga allegati illeggibili si dovrà chiedere chiarimenti al mittente in merito al documento allegato.

5.8 *Documenti di competenza di altre amministrazioni*

Qualora pervengano all'ente/organizzazione documenti di competenza di altre amministrazioni, questi vanno inviati al destinatario. Nel caso in cui il destinatario non sia individuabile, il documento deve essere rimandato al mittente.

5.9 *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

[31] Nella definizione dell'articolo è necessario considerare quanto indicato per la ricezione dei documenti informatici.
[32] Indicare eventuali altre procedure.
[33] Qualora un ente/organizzazione non abbia integrato tali caselle di posta elettronica al sistema di gestione documentale dovrà indicare le modalità per l'inoltro dei documenti alle caselle di posta elettronica deputate alla registrazione di protocollo.

successivamente registrare, classificare e fascicolare indipendentemente una dall'altra. Ciascun documento in uscita avrà un unico oggetto.

5.10 *Gestione della documentazione relativa al Servizio associato*[34]

L'ente/organizzazione non è capofila né ha aderito a un Servizio associato.

Nel caso in cui l'ente/organizzazione sia capofila di un Servizio associato[35]*:*
I documenti relativi ai procedimenti afferenti al servizio[36] *sono ricevuti tramite l'indirizzo di posta elettronica certificata indicato nel sito web dell'ente/organizzazione e/o tramite*[37]*. I documenti sono registrati nel sistema di protocollo informatico*[38]*.*
I documenti ricevuti e prodotti sono trattati secondo le modalità previste nel presente Manuale e secondo quanto specificato nella Convenzione (allegato n.)[39]*.*
Nel caso in cui un ente/organizzazione abbia aderito ad un Servizio associato[40]*:*
I documenti relativi ai procedimenti afferenti al servizio[41] *sono ricevuti tramite l'indirizzo di posta elettronica certificata indicato nel sito web dell'ente/organizzazione e/o tramite*[42]*. I documenti sono registrati nel sistema di protocollo informatico*[43]*. La gestione di questi documenti è descritta nel Manuale di gestione dell'ente/organizzazione capofila e secondo quanto specificato nella Convenzione in allegato n.*[44]*.*
Nel caso di Gestione associata di servizi nell'Unione/Consorzio:
Tutte le attività relative alla gestione della documentazione in entrata e in uscita dei servizi (indicare quali) sono esercitate in forma associata per conto dei comuni partecipanti dall'unità organizzativa/ufficio, individuata dall'Unione/Consorzio.
La registrazione dei documenti avviene all'interno del software di gestione documentale, secondo quanto indicato nel manuale dell'Unione/Consorzio e con riferimento alla Convenzione in Allegato n[45].

---

[34] L'ente dovrà indicare il nome del servizio associato. Se sono presenti più servizi associati che prevedono gestioni della documentazione differenti, sarà necessario descriverli in diversi articoli (esempio: un articolo per SUAP Associato, un articolo per il SUE Associato, ecc.).
[35] Questo articolo riguarda la AOO che ha istituito al proprio interno uno o più Servizi Associati (con altre Amministrazioni), di cui ne ricopre il ruolo di ente capofila. L'ente capofila dovrà descrivere le procedure di gestione dei documenti che vengono prodotti nell'ambito del Servizio associato.
[36] Indicare il servizio.
[37] Inserire altre modalità di ricezione dei documenti se presenti.
[38] Indicare se sono registrati nel protocollo dell'ente o se è stato istituito apposito registro (a seguito dell'istituzione di una AOO apposita) per la gestione del servizio.
[39] Qualora non sia specificato nella convenzione la gestione documentale l'ente dovrà descrivere le procedure nel dettaglio.
[40] Questo articolo riguarda l'ente che ha aderito ad uno o più Servizi Associati (con altre Amministrazioni), la cui documentazione prodotta e ricevuta nell'ambito del servizio associato in oggetto è gestita direttamente dall'ente capofila.
[41] Indicare il servizio.
[42] Inserire l'indirizzo pec al quale pervengono i documenti e altre modalità di ricezione, se presenti.
[43] Indicare se sono registrati nel protocollo dell'ente capofila o se è stata istituita apposita AOO.
[44] Qualora non sia specificato nella convenzione la gestione documentale, l'ente dovrà descrivere le procedure nel dettaglio
[45] L'ente dovrà descrivere in forma dettagliata la gestione della documentazione afferente all'Unione/Consorzio, se non previsto nella Convezione.

5.11 *Documentazione prodotta e registrata in appositi gestionali*[46]

L'ente/organizzazione non è al momento dotato di software gestionali in grado di acquisire automaticamente la registrazione di protocollo, mediante specifico collegamento tra i sistemi, nell'ambito di procedimenti riguardanti determinate attività.

5.12 *Modelli pubblicati*

Tutti i modelli di documenti prodotti dall'ente/organizzazione e pubblicati sul sito internet o sulla rete intranet dell'ente/organizzazione sono classificati secondo il piano di classificazione in uso[47]. Non possono essere pubblicati modelli, formulari ecc. che non siano classificati.

5.13 *Trasmissioni telematiche e procedimenti amministrativi online*

I documenti di cui all'allegato (Allegato n. 16) [48] sono trasmessi/ricevuti dall'ente/organizzazione con immissione diretta dei dati nel sistema dell'ente/organizzazione destinatario. I documenti possono essere trasmessi senza firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate ed a identificazione univoca attivati con i singoli destinatari. Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione. L'ente/organizzazione è dotato di software gestionali dedicati alla produzione, ricevimento, registrazione e gestione di tipologie documentali anche via web: il sistema Axios in uso permette lo scambio di tipologie documentali direttamente con i portali governativi interessati.

5.14 *Gestione delle password*

Il sistema garantisce la gestione e conservazione delle password di accesso al sistema stesso e ai servizi online degli utenti interni e esterni secondo le modalità descritte nel piano per la sicurezza informatica (Allegato n. 8)[49].

[46] Alcuni esempi di software gestionali che possono essere legati al sistema di protocollo riguardano la gestione SUAP, SUE. Altri esempi di software gestionali non necessariamente legati al sistema di protocollo informatico possono riguardare: documenti del personale (ferie, permessi, ecc.) o, per gli enti del "Sistema Socio Sanitario Regionale" i documenti che vengono registrati nel SISS.

[47] Ogni volta che verrà inserito un nuovo modello questo dovrà essere classificato. Il responsabile del servizio di gestione documentale dovrà provvedere alla classificazione di tutti i modelli già pubblicati.

[48] Ad esempio: DURC on-line denunce di infortunio, certificati di malattia ecc.

[49] Specificare le tipologie di trattamento delle password: censimento dei servizi che registrano in chiaro le password, se le password vengono trasmesse via mail, dove si conservano ecc.

6 Posta elettronica

6.1 *Gestione della posta elettronica*

La posta elettronica viene utilizzata per l'invio di comunicazioni, informazioni e documenti sia all'interno dell'ente/organizzazione, sia nei rapporti con i cittadini e altri soggetti privati, sia con altre Pubbliche Amministrazioni.

Le comunicazioni formali e la trasmissione di documenti informatici, il cui contenuto impegni l'ente/organizzazione verso terzi, avvengono tramite le caselle di posta elettronica istituzionali e PEC, secondo quanto descritto nella Sezione 3.

I documenti informatici eventualmente pervenuti agli uffici non abilitati alla ricezione, devono essere inoltrati all'indirizzo di posta elettronica istituzionale indicato dall'ente/organizzazione come deputato alle operazioni di registrazione, secondo quanto previsto negli articoli seguenti.

Le semplici comunicazioni informali ricevute o trasmesse per posta elettronica, che consistano in scambio di informazioni che non impegnano l'ente/organizzazione verso terzi, possono non essere protocollate.

A chi ne fa richiesta deve sempre essere data la risposta dell'avvenuto ricevimento. Non è possibile inviare messaggi dalla casella di posta elettronica nominativa quando il contenuto di questi impegni l'amministrazione verso terzi. Nel formato dei messaggi di posta elettronica non certificata è inserito automaticamente il seguente testo: "*Questo messaggio non impegna (nome ente/organizzazione) e contiene informazioni appartenenti al mittente, che potrebbero essere di natura confidenziale, esclusivamente dirette al destinatario sopra indicato. Qualora Lei non sia il destinatario indicato, Le comunichiamo che, ai sensi dell'articolo 616 Codice penale e del D. Lgs 196/03, sono severamente proibite la revisione, divulgazione, rivelazione, copia, ritrasmissione di questo messaggio nonché ogni azione correlata al contenuto dello stesso"*.

La posta elettronica nominativa non può essere utilizzata per la ricezione o la spedizione di documenti a firma digitale per i quali si utilizzano le caselle istituzionali.

6.2 *La posta elettronica per le comunicazioni interne*

Le comunicazioni tra l'ente/organizzazione e i propri dipendenti, nonché tra le varie strutture, avvengono, di norma, mediante l'utilizzo della casella di posta elettronica ordinaria dei rispettivi uffici/ servizi/dipartimenti/articolazioni aziendali o le caselle di posta elettronica nominative[50], nel rispetto delle norme in materia di protezione dei dati personali, nonché previa informativa agli interessati circa il grado di riservatezza degli strumenti utilizzati.

La posta elettronica viene utilizzata per:

1 convocare riunioni (interne all'ente/organizzazione);

2 inviare comunicazioni di servizio o notizie, dirette ai dipendenti in merito a informazioni generali di organizzazione;

3 diffondere circolari, ordini di servizio, copie di documenti (gli originali si conservano nel fascicolo specifico debitamente registrati).

[50] Tutti i dipendenti sono dotati di una casella di posta elettronica nominativa rilasciata dell'Ente/Organizzazione oppure hanno comunicato un indirizzo privato

6.3 *La posta elettronica ricevuta da cittadini o altri soggetti privati*

Le istanze e le dichiarazioni trasmesse per via telematica all'indirizzo istituzionale devono ritenersi valide a tutti gli effetti di legge qualora:

- siano trasmesse via posta elettronica o via posta elettronica certificata, regolarmente sottoscritte con firma elettronica/digitale dotata di certificato valido rilasciato da un certificatore accreditato;
- l'autore del documento è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della Carta Regionale dei Servizi (CRS) oppure attraverso altri strumenti informatici messi a disposizione dall'ente/organizzazione, che consentano l'individuazione certa del soggetto richiedente;
- siano inviate utilizzando una casella di Posta Elettronica Certificata, le cui credenziali di accesso siano state rilasciate previa identificazione del titolare attestata da parte del gestore del sistema;
- si tratti di istanze o dichiarazioni sostitutive di atto di notorietà trasmesse secondo le modalità di cui all'art. 38 comma 3 del DPR 445/2000.

Al di fuori delle predette ipotesi, le comunicazioni di posta elettronica che pervengono all'indirizzo istituzionale, dei singoli servizi o a quelli nominativi, sono valutate in ragione della loro rispondenza a ragionevoli criteri di attendibilità e riconducibilità al mittente dichiarato, e successivamente soggette, se del caso, a protocollazione/registrazione secondo le seguenti modalità:

a) Messaggi di posta elettronica con allegate rappresentazioni digitali di documenti originali cartacei: nel caso in cui via posta elettronica pervengano rappresentazioni digitali di documenti originali cartacei in uno dei seguenti formati standard TIFF, PDF, PDF-A, JPEG, la rappresentazione digitale e il messaggio che la trasmette verranno inoltrati alla casella di posta elettronica istituzionale[51], con richiesta di protocollazione/registrazione da parte del responsabile del procedimento;

b) Messaggi di posta elettronica:[52] qualora si volessero registrare al protocollo semplici messaggi di posta elettronica ordinaria/nominativa, il Responsabile del procedimento dovrà fare richiesta di protocollazione/registrazione; poiché le istanze e le dichiarazioni presentate con tale modalità non sono valide ai sensi dell'art.65 del CAD, la richiesta di protocollazione dovrà contenere la dichiarazione della certezza della provenienza.

In ogni caso, spetterà al Responsabile del procedimento, ove ne rilevi la necessità, richiedere al mittente la regolarizzazione dell'istanza o della dichiarazione, acquisendo ogni utile documentazione integrativa.

6.4 *La posta elettronica ricevuta da altre Pubbliche Amministrazioni*

Le comunicazioni e i documenti ricevuti da altre Pubbliche Amministrazioni sono valide ai fini del procedimento una volta che ne sia verificata la provenienza, ovvero quando:

- sono sottoscritti con firma elettronica/digitale;
- sono dotati di segnatura di protocollo;
- sono trasmessi attraverso sistemi di posta elettronica certificata.

[51] Indicare l'indirizzo di posta elettronica abilitata alla protocollazione/registrazione.

[52] L'ente/organizzazione può dichiarare di non protocollare semplici messaggi di posta elettronica.

7 *Assegnazione dei documenti*

7.1 *Assegnazione*

Le postazioni abilitate al ricevimento/protocollazione/registrazione provvedono ad assegnare i documenti tramite il sistema di gestione documentale sulla base dell'organigramma (Allegato n. 2), agli uffici/strutture competenti.
L'assegnatario può a sua volta smistare i documenti a unità organizzative afferenti attraverso apposita funzione del software di gestione documentale.
Qualora sia necessario consegnare un documento analogico originale, questo dovrà essere consegnato all'ufficio che risulta assegnatario nel sistema di gestione documentale.
Le assegnazioni per conoscenza devono essere effettuate tramite il sistema di gestione documentale.
Le abilitazioni all'assegnazione dei documenti sono rilasciate dal responsabile della gestione documentale. Qualora si tratti di documenti originali analogici viene assegnata per conoscenza l'immagine acquisita secondo le stesse modalità indicate per l'assegnazione tramite il sistema di gestione documentale[53].

7.2 *Modifica delle assegnazioni*

Nel caso di un'assegnazione errata, la struttura che riceve il documento provvederà ad assegnare lo stesso alla struttura effettivamente competente o restituirla all'unità di protocollazione.

Il sistema di gestione informatica dei documenti tiene traccia dei passaggi di cui sopra, memorizzando per ciascuno di essi l'identificativo dell'operatore agente, data e ora di esecuzione.

[53] Integrare l'articolo con la descrizione delle proprie modalità/procedure di assegnazione, smistamento e condivisione dei documenti.

8 *Classificazione e fascicolazione dei documenti*

8.1 *Classificazione dei documenti*

Tutti i documenti ricevuti o prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al piano di classificazione (titolario)[54]. Le abilitazioni alla classificazione dei documenti in arrivo, effettuate dalle postazioni di protocollo decentrato, sono rilasciate dal responsabile del servizio di gestione documentale. Sono classificati anche gli atti preparatori interni, le minute dei documenti spediti o altri documenti che non vengono protocollati o siano soggetti a registrazione particolare. I documenti prodotti dall'ente/organizzazione sono classificati da chi li scrive, pertanto perverranno alle postazioni di protocollo già classificati. I dati di classificazione sono riportati su tutti i documenti. Il programma di protocollo informatico non permette la registrazione in uscita di documenti non classificati[55].

8.2 *Formazione e identificazione dei fascicoli*

Tutti i documenti[56], indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli o serie documentarie[57]. L'apertura di un nuovo fascicolo è effettuata dal servizio di gestione documentale, su richiesta dei responsabili di servizio/procedimento[58], o dagli stessi se abilitati a questa funzione (l'elenco è allegato al manuale). La formazione di un nuovo fascicolo avviene attraverso l'operazione di apertura, con richiesta scritta oppure, se informatica, regolata dal manuale operativo del sistema, che prevede la registrazione sul repertorio/elenco dei fascicoli o nel sistema informatico delle seguenti informazioni:

- categoria e classe del titolario;
- numero del fascicolo;
- oggetto del fascicolo;
- data di apertura;
- ufficio a cui è assegnato;
- responsabile del procedimento;
- livello di riservatezza eventualmente previsto;
- tempo previsto di conservazione[59].

Il sistema di protocollo informatico aggiorna automaticamente il repertorio/elenco dei fascicoli

[54] Nel caso in cui l'Ente/Organizzazione sia strutturato in più AA:OO il titolario dovrà essere unico e valido per tutte le AOO.

[55] Se l'ente ha attivato il modello operativo parzialmente decentrato, la classificazione dei documenti in entrata sarà effettuata dall'ufficio protocollo consultando il piano di classificazione. Se il modello operativo invece è quello totalmente decentrato, ogni postazione dovrà classificare i documenti sia in entrata, sia in uscita, sia interni. In ogni caso il responsabile del servizio di gestione documentale deve attivare all'interno del software di protocollo informatico l'inibizione alla generazione di numeri di protocollo se non sono stati inseriti gli estremi di classificazione (categoria e classe). Nell'articolo deve essere specificato a quale modello ci si riferisce, esplicitando che non è possibile generare numeri di protocollo in uscita senza classificazione.

[56] In un fascicolo confluiscono documenti protocollati e non (documentazione preparatoria e di corredo), ma tutti i documenti devono essere classificati.

[57] Si riuniscono in serie documentarie i documenti standard: delibere, determinazioni, verbali ecc.

[58] Si deve decidere chi, e con quale responsabilità, ha facoltà di richiedere o aprire i fascicoli. In alcune amministrazioni la richiesta di apertura è formulata dal dirigente. In un sistema di gestione decentrata, l'apertura di un nuovo fascicolo può essere effettuata direttamente dal funzionario/responsabile di procedimento. In questo caso sarà adottato un sistema di password di accesso che consentirà di aggiornare l'elenco dei fascicoli, il cui criterio di formazione, aggiornamento e controllo sarà comunque dettato dal responsabile del servizio di gestione documentale.

[59] Il tempo di conservazione è determinato dal responsabile del servizio di gestione documentale, che si basa, per esprimere la sua valutazione, sul massimario per la selezione e conservazione dei documenti.

[60].

8.3 *Processo di formazione dei fascicoli*

In presenza di un documento da inserire in un fascicolo, il responsabile del servizio di gestione documentale o i responsabili di servizio/procedimento stabilisce/ono, consultando le funzioni del protocollo informatico, o il repertorio dei fascicoli, se esso si colloca nell'ambito di un affare o procedimento in corso, oppure se dà avvio ad un nuovo procedimento; se il documento deve essere inserito in un fascicolo già aperto, dopo la classificazione e protocollazione viene rimesso al responsabile del procedimento che ha cura di inserirlo fisicamente nel fascicolo, nel caso di documenti informatici il sistema provvede automaticamente, dopo l'assegnazione del numero di fascicolo, a inserire il documento nel fascicolo informatico stesso. Se invece dà avvio a un nuovo affare, apre/ono un nuovo fascicolo (con le procedure sopra descritte). I documenti prodotti dall'ente/organizzazione sono fascicolati da chi li scrive, pertanto perverranno alle postazioni di protocollo già con l'indicazione del numero/identificativo di fascicolo[61]. I dati di fascicolazione sono riportati su tutti i documenti. Ai documenti informatici prodotti nei *software* gestionali tramite l'utilizzo di modelli *standard* o creati dall'utente attraverso moduli e formulari, resi disponibili mediante applicativi *web*, sono associati automaticamente dal sistema di gestione documentale i metadati minimi del fascicolo informatico o aggregazione documentale informatica cui appartengono o a cui danno avvio.

Nel caso di gestione associata di servizi aggiungere:
Ciascun affare, gestito dall'Unione/Consorzio per conto dei propri comuni, deve essere organizzato/sottofascicolato con distinzione per comune. Verranno inoltre creati fascicoli autonomi per ogni Comune relativamente alla cessione di fabbricato, denunce di infortuni e notifiche[62].

8.4 *Modifica delle assegnazioni dei fascicoli*

La riassegnazione di un fascicolo è effettuata, su istanza scritta dell'ufficio o dell'unità organizzativa che ha in carico il fascicolo, dal servizio di gestione documentale 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, e degli estremi del provvedimento di autorizzazione, è lasciata traccia nel sistema informatico di gestione dei documenti o sul repertorio/elenco cartaceo dei fascicoli[63].

8.5 *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 e il numero di repertorio che dovrà essere apposto identico su entrambe le unità

[60] Ogni anno si costituiscono fascicoli standard all'interno di ogni classe del titolario (es. il fascicolo del bilancio preventivo, il bilancio consuntivo; l'acquisto della cancelleria ecc.). Il fascicolo raccoglie i documenti prodotti durante l'esercizio di effettive funzioni; pertanto potrà capitare che alcune classi rimarranno vuote di fascicoli se in quell'anno non si sarà verificato alcun evento in quel settore di attività.
[61] Il responsabile del servizio di gestione documentale deve attivare all'interno del software di protocollo informatico l'inibizione alla generazione di numeri di protocollo se non sono stati inseriti gli estremi di fascicolazione, per impedire la registrazione in uscita di documenti non fascicolati. Nell'articolo deve essere specificato a quale modello operativo di protocollo ci si riferisce, dando anche l'indicazione che non è possibile generare numeri di protocollo in uscita senza classificazione.
[62] E altre tipologie di procedimenti e affari.
[63] In un sistema totalmente decentrato anche la gestione delle riassegnazioni è demandata al responsabile del procedimento.

archivistiche. In presenza di documenti cartacei da inserire in fascicoli informatici, dovrà essere prodotta copia per immagine degli stessi secondo la normativa vigente.
L'originale cartaceo sarà conservato presso gli archivi cartacei dell'ufficio Protocollo dell'Istituto[64].

8.6 *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[65]. Per quanto riguarda i fascicoli informatici, vedi Sezione 10.

[64] L'ente deve indicare se si tratta dell'ufficio protocollo o delle unità organizzative
[65] Indicare eventuali altri modelli gestionali in uso presso l'ente.

9 *Invio dei documenti destinati all'esterno*

9.1 *Spedizione dei documenti informatici mediante l'utilizzo della posta elettronica*

Per la spedizione dei documenti informatici soggetti alla registrazione di protocollo/particolare mediante l'utilizzo della posta elettronica l'ente/organizzazione si avvale di indirizzi di posta elettronica certificata e/o ordinaria.
I documenti vengono trasmessi, dopo essere stati classificati, fascicolati e protocollati, secondo le procedure previste dal manuale operativo del *software* di gestione documentale (Allegato n.), all'indirizzo di posta elettronica dichiarato dai destinatari abilitati alla ricezione della posta per via telematica ovvero:

- in caso di spedizione di un documento al cittadino/utente, all'indirizzo di posta elettronica certificata comunicato in qualità di domicilio digitale e inserito all'interno dell'ANPR
- in caso di PA all'indirizzo pubblicato su indicepa.gov.it
- in caso di imprese e professionisti all'indirizzo pubblicato sull'Indice Nazionale degli Indirizzi PEC delle imprese e dei professionisti (INI PEC).

Le postazioni deputate ad effettuare l'invio telematico verificano l'avvenuto recapito dei documenti e il collegamento delle ricevute elettroniche alle registrazioni di protocollo.
I corrispondenti destinatari dell'ente/organizzazione sono descritti in appositi elenchi costituenti l'anagrafica unica dell'ente/organizzazione.
In assenza del domicilio digitale l'ente/organizzazione può predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o forma elettronica avanzata ed inviare ai cittadini stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia analogica di tali documenti secondo la normativa vigente.
L'ente/organizzazione dovrà conservare l'originale digitale nei propri archivi; all'interno della copia analogica spedita al cittadino, deve essere riportata la dicitura che la copia originale del documento è conservata dall'ente/organizzazione.

La spedizione di documenti informatici, attraverso posta elettronica, al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni senza che a queste l'ente/organizzazione riconosca un carattere giuridico-amministrativo che la impegni verso terzi.
Per l'uso della posta elettronica si rimanda alla Sezione 8.

9.2 *Trasmissione dei documenti informatici in interoperabilità e in cooperazione applicativa (trasmissioni telematiche)*

L'ente/organizzazione effettua lo scambio di informazioni, dati e documenti soggetti a registrazione di protocollo attraverso messaggi trasmessi in cooperazione applicativa.
I documenti di cui all'(Allegato n. 16) sono trasmessi dall'ente/organizzazione con immissione diretta dei dati nel sistema informatico dell'ente/organizzazione destinatario, senza la produzione e conservazione dell'originale cartaceo.
I documenti possono essere trasmessi senza firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate ed ad identificazione univoca attivati con i singoli enti destinatari.

Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione

9.3 *Spedizione dei documenti cartacei*

Qualora sia necessario spedire documenti originali analogici questi devono essere completi della firma autografa del responsabile del procedimento, della classificazione e del numero di fascicolo nonché delle eventuali indicazione necessarie a individuare il procedimento amministrativo di cui fanno parte. La spedizione avviene a cura degli uffici produttori, tramite passaggio della documentazione completa all'ufficio Protocollo, che ne effettua la protocollazione in uscita e successivamente predispone la spedizione tramite Raccomandata R/R del servizio postale nazionale.[66]
Nel caso di spedizione che utilizzi pezze di accompagnamento (raccomandate, posta celere, corriere 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 e autorizzate dal responsabile del Servizio di gestione documentale.
I corrispondenti destinatari dell'ente/organizzazione sono descritti in appositi elenchi costituenti l'anagrafica unica dell'ente/organizzazione.

[66] Descrivere le procedure adottate dall'ente per la spedizione dei documenti analogici. Nel caso di un modello operativo di protocollo accentrato la documentazione definita in tutti i propri elementi deve essere messa a disposizione dell'Ufficio protocollo per essere protocollata e spedita. L'ente dovrà indicare le procedure operative per la protocollazione e la spedizione.

10 *Scansione dei documenti su supporto cartaceo*

10.1 *Documenti soggetti a scansione*

I documenti su supporto cartaceo, dopo le operazioni di registrazione, classificazione e segnatura, possono essere acquisiti, all'interno del sistema di protocollo informatico, in formato immagine con l'ausilio di scanner[67].

10.2 *Processo di scansione*

Il processo di scansione si articola di massima nelle seguenti fasi:

- acquisizione delle immagini in modo che a ogni documento, anche composto da più fogli, corrisponda un unico file in un formato standard abilitato alla conservazione;
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- collegamento delle rispettive immagini alla registrazione di protocollo, in modo non modificabile;
- memorizzazione delle immagini, in modo non modificabile;
- autenticazione, attraverso sottoscrizione digitale, di ogni singolo file, o comunque secondo quanto previsto dalla legge.

Nel caso di produzione di fascicoli ibridi, il processo di scansione dei documenti avviene alla chiusura del procedimento amministrativo a cui afferiscono; fino a quel momento il fascicolo è composto da due supporti, quello cartaceo e quello informatico; l'unitarietà del procedimento stesso è garantita dal sistema mediante l'indice di classificazione e il numero di repertorio del fascicolo; vedi articolo n. 8.6.

I documenti analogici soggetti a riproduzione sostitutiva si conservano nell'archivio dell'ente/organizzazione fino a procedimento legale di scarto.

[67] Il processo di scansione descritto è pensato ai fini della "dematerializzazione" della documentazione prodotta e ricevuta in corrente, a fini di riproduzione sostitutiva legale. Un modello operativo può essere esemplificato secondo questo schema:
1) l'ente produce solamente documentazione informatica a firma elettronico/digitale; vedi punto 6;
2) tutta la documentazione è classificata e fascicolata (non è possibile produrre documenti se non sono classificati e fascicolati); il sistema può presentare modelli documentari pre-classificati e, al momento della loro registrazione a protocollo/particolare, non genera il numero se non sono indicati gli estremi della classificazione e fascicolazione;
3) i documenti ricevuti dall'esterno su formato cartaceo vengono registrati al protocollo/particolare e classificati, etichettati con codice a barre e successivamente scansionati; al momento dell'etichettatura è indicato il contenitore nel quale è inserito l'originale cartaceo; successivamente alla scansione la copia immagine del documento è resa disponibile sulla postazione di lavoro del responsabile del procedimento, il quale per accedere al documento deve indicare, nel profilo di registrazione del documento stesso, il numero di fascicolo; se il responsabile del procedimento non fascicola non può accedere alla copia immagine del documento;
4) al momento della scansione i file immagine di ogni singolo documento, o di serie giornaliera degli stessi, sono autenticati con firma digitale;
5) i documenti originali sono collocati in appositi contenitori e inviati in archivio; il nesso giuridico archivistico del fascicolo, fra l'originale cartaceo e la copia immagine, è ricostruibile tramite l'indicazione del contenitore nel quale si trova l'originale, vedi punto 3;
6) i documenti sono spediti all'esterno agli indirizzi di posta elettronica oppure in copie cartacee tramite servizi di postalizzazione (escluse le eccezioni documentate); sulla copia cartacea è apposta la dichiarazione di conformità della stessa all'originale informatico.

11 Sistema informatico, *conservazione e tenuta dei documenti*

11.1 *Sistema informatico*

Il sistema informatico, le misure di sicurezza fisica e logica, le procedure comportamentali adottate per la gestione del sistema documentale e del sistema informatico sono descritte nel Piano della sicurezza informatica (Allegato n. 8). Il piano per la sicurezza informatica e predisposto e aggiornato annualmente[68]. All'interno del Piano della sicurezza informatica sono dichiarati i servizi e le aziende che si occupano della sicurezza informatica e i loro responsabili.

11.2 *Conservazione e memorizzazione dei documenti analogici, informatici e delle rappresentazioni digitali dei documenti cartacei*

I documenti dell'amministrazione, su qualsiasi formato prodotti, sono conservati a cura del Servizio di gestione documentale che svolge anche le funzioni di Responsabile della conservazione (vedi articolo n. 1.6)[69]. La documentazione corrente è conservata a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.
I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo, e conservati nell'archivio informatico.
Le rappresentazioni digitali dei documenti originali su supporto cartaceo, acquisite con l'ausilio dello scanner, sono memorizzate nel sistema, in modo non modificabile, al termine del processo di scansione.

11.3 *Conservazione dei documenti informatici*

Il Responsabile del servizio di gestione documentale provvede, in collaborazione con il servizio di gestione dei servizi informativi e con il supporto della tecnologia disponibile, a conservare i documenti informatici e a controllare periodicamente a campione (almeno ogni sei mesi) la leggibilità dei documenti stessi. L'intervento del Responsabile del servizio di gestione documentale deve svolgersi in modo che si provveda alla conservazione integrata dei documenti e delle informazioni di contesto generale, prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi. Il servizio di gestione documentale, di concerto con i sistemi informativi dell'ente/organizzazione, provvede altresì alla conservazione degli strumenti di descrizione, ricerca, gestione e conservazione dei documenti[70]. Il sistema deve inoltre fornire la documentazione del software di gestione e conservazione, del sistema di sicurezza, delle responsabilità per tutte le fasi di gestione del sistema documentario, delle operazioni di conservazione dei documenti.
La documentazione prodotta nell'ambito del manuale di gestione e dei relativi aggiornamenti deve essere conservata integralmente e perennemente nell'archivio dell'ente/organizzazione[71].

11.4 *Censimento depositi documentari delle banche dati e dei software*

[68] Indicare il servizio/struttura che si occupa della sicurezza informatica e il suo responsabile.
[69] Le varie responsabilità sono descritte nella Sezione 1, le articolazioni di responsabilità diverse da quella citata nell'articolo andranno descritte in sostituzione della presente. Se presso l'ente non è presente una figura di riferimento per la gestione dei sistemi informatici, ma questa è affidata in servizio esterno, andranno specificati in questo articolo gli estremi del contratto che verrà allegato al manuale di gestione.
[70] Indici, inventari, quadri di classificazione (titolari) e relativi massimari di selezione e scarto, repertori.
[71] Nel caso in cui il servizio di gestione e conservazione della memoria informatica dell'ente sia dato in gestione esterna devono essere indicati chiaramente gli estremi del contratto o convenzione e gli obblighi del conservatore, e la descrizione dell'articolo deve essere modificata tenendo conto di quanto indicato..

Ogni anno il responsabile del servizio di gestione documentale provvede ad effettuare il censimento dei depositi documentari[72], dei registri particolari (vedi sezione 5), delle banche dati[73] e dei software di gestione documentale in uso all'ente/organizzazione, per programmare i versamenti dei documenti cartacei all'archivio di deposito, dei documenti informatici sui supporti di memorizzazione e per predisporre, di concerto con il responsabile dei sistemi informativi, il Piano per la continuità operativa, il disaster recovery e gli aggiornamenti del Piano per la sicurezza informatica (Allegati n. 8 e 17).

11.5 *Trasferimento delle unità archivistiche analogiche negli archivi di deposito e storico*

All'inizio di ogni anno gli uffici individuano i fascicoli da versare all'archivio di deposito dandone comunicazione al responsabile del servizio di gestione documentale, il quale provvede al loro trasferimento e compila o aggiorna il repertorio/elenco dei fascicoli. Delle operazioni di trasferimento deve essere lasciata traccia documentale o attivata l'apposita funzione all'interno del sistema informatico di gestione dei documenti. Il responsabile del servizio della gestione documentale provvede, sentiti i responsabili delle unità organizzative, a rimuovere/trasferire i fascicoli informatici e a versarli nelle unità informatiche di conservazione. Di norma sono versati all'archivio storico tutti i documenti anteriori all'ultimo quarantennio. E' tuttavia possibile depositare anche documentazione successiva al quarantennio purché non rivesta più un preminente carattere giuridico-amministrativo per l'ente/organizzazione.

11.6 *Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica*

I dati e i documenti informatici sono memorizzati nel sistema di gestione documentale al termine delle operazioni di registrazione. Le procedure di memorizzazione sono le seguenti[74]:

- caricamento del documento informatico nel sistema di gestione documentale
- archiviazione del documento informatico tramite attribuzione di ID univoco e calcolo dell'HASH del documento
- definitiva memorizzazione presso i server Cloud del fornitore del sistema di gestione documentale

Alla fine di ogni giorno sono create, a cura dei servizi informativi, copie di *backup* della memoria informatica dell'ente/organizzazione, che verranno poi riversate su supporti di memorizzazione tecnologicamente avanzati e conservati secondo quanto previsto dai Piano di Continuità Operativa e Disaster Recovery (Allegato n. 17) e dalle procedure di salvataggio dati descritte all'interno del Piano per la sicurezza informatica dell'ente/organizzazione (Allegato n. 8).

11.7 *Pacchetti di versamento*

Il Responsabile della gestione documentale/conservazione assicura la trasmissione del contenuto del pacchetto di versamento al sistema di conservazione secondo le modalità operative definite nel Manuale di conservazione /Allegato n. 18).

Il Responsabile della conservazione genera il rapporto di versamento relativo ad uno o più pacchetti di versamento e una o più impronte relative all'intero contenuto del pacchetto, secondo le modalità descritte nel Manuale di conservazione.

---

[72] Per deposito documentario si intende ogni luogo dove è conservata la documentazione dell'ente, dal singolo ufficio al deposito d'archivio vero e proprio.

[73] L'elenco delle banche dati sarà allegato al Piano per la sicurezza informatica.

[74] L'ente deve specificare le procedure adottate e gli strumenti utilizzati per la memorizzazione dei dati e dei documenti informatici

11.8 *Conservazione dei documenti informatici, dei fascicoli informatici e delle aggregazioni documentali informatiche*

I documenti informatici, i fascicoli informatici e le aggregazioni documentali informatiche sono versati nel sistema di conservazione con i metadati ad essi associati di cui all'(Allegato n. 20) delle regole tecniche sulla conservazione, in modo non modificabile, nei tempi previsti dal Manuale di conservazione (Allegato n. 18). Tutti i documenti destinati alla conservazione utilizzano i formati previsti nell'allegato 2 delle regole tecniche sulla conservazione.
In caso di migrazione dei documenti informatici la corrispondenza fra il formato originale e quello migrato è garantita dal Responsabile della conservazione.

11.9 *Conservazione in outsourcing*[75]

L'ente/organizzazione, per la conservazione di tutto l'archivio documentale[76] si avvale del sistema di conservazione fornito da Axios Italia SPA e 2C Solution[77], come da convenzione/contratto (Allegati n. 19) [78].
Le modalità di conservazione e accesso ai documenti, analogici o digitali, sono specificate con riferimento al Manuale di conservazione dell'outsourcer (Allegato n. 20).
Il Responsabile della conservazione dell'ente/organizzazione vigila affinché il soggetto individuato come conservatore esterno provveda alla conservazione integrata dei documenti e delle informazioni di contesto generale, prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi.

11.10 *Trasferimento delle unità archivistiche analogiche nell'archivio di deposito*

Il Responsabile della gestione documentale cura il versamento nell'archivio di deposito delle unità archivistiche non più utili per la trattazione degli affari in corso, individuate dagli uffici produttori.
Le procedure di versamento sono descritte nell'(Allegato n. 21) "Linee Guida per la gestione degli archivi analogici".
Delle operazioni di trasferimento deve essere lasciata traccia documentale o attivata l'apposita funzione all'interno del sistema informatico di gestione dei documenti.
La documentazione analogica corrente è conservata a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.

---

[75] Se l'ente si avvale di diversi conservatori esterni, questi devono essere indicati
[76] L'ente dichiara se utilizza un servizio di conservazione in outsourcing solo per una parte del proprio archivio, specificandone le tipologie documentali interessate.
[77] Indicare conservatore.
[78] In outsourcing possono essere conservati documenti analogici e informatici, è possibile che alcuni enti/organizzazioni abbiano più outsourcer e/o conservatori (indicarli tutti). Relativamente alla conservazione informatica bisognerà allegare al manuale:
1 Mandato di affidamento delle attività del procedimento do conservazione (documento nel quale si declinano le attività di conservazione, le condizioni dell'affidamento e le clausole di accettazione);
2 Manuale di Conservazione dell'ente/organizzazione;
3 Accordi di versamento dei documenti informatici nel sistema di conservazione: tipologie dei pacchetti, flussi, sistemi di archiviazione, sistema di conservazione, regole e canali di versamento e archiviazione;
4 Il manuale di conservazione del Conservatore outsourcer.

11.11 *Conservazione dei documenti analogici*

I documenti analogici dell'ente/organizzazione sono conservati nei locali di archivio siti presso la sede dell'ente/organizzazione.[79]
Le procedure adottate per la corretta conservazione sono descritte (Allegato n. 21) "Linee Guida per la gestione degli archivi analogici".
Il loro aggiornamento compete al Responsabile per la gestione documentale.
I fascicoli non soggetti a operazioni di scarto sono conservati nell'archivio di deposito secondo i termini di legge e quindi trasferiti nell'archivio storico per la conservazione permanente[80].

11.12 *Selezione dei documenti*

Periodicamente, in base al Massimario di scarto (Allegato n. 22), viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale con l'invio della proposta alla competente Soprintendenza Archivistica. Le modalità di selezione e scarto per i documenti informatici sono descritte nel Manuale di Conservazione (Allegato n. 18).

[79] Specificare se i documenti sono conservati nei locali dell'ente produttore o se si tratta di Servizio esternalizzato. Nel caso di esternalizzazione è necessario allegare la convenzione/contratto, e far riferimento al nulla osta preventivo da parte della competente Soprintendenza Archivistica.
[80] Se l'ente ha un regolamento per l'accesso e la consultazione dell'archivio storico, deve allegarlo al Manuale di gestione.

12 Accesso ai dati, informazioni e documenti - Pubblicità legale e trasparenza amministrativa

12.1 *Accessibilità da parte degli utenti appartenenti all'Amministrazione*

La sicurezza e 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.
Il controllo degli accessi è assicurato utilizzando le credenziali di accesso[81] ed un sistema di autorizzazione basato sulla profilazione degli utenti.
Sulla base della struttura organizzativa e funzionale dell'ente/organizzazione, il responsabile della gestione documentale attribuisce, in coordinamento con il responsabile della sicurezza informatica, almeno i seguenti livelli di autorizzazione:

a) abilitazione alla consultazione
b) abilitazione all'inserimento
a) abilitazione alla cancellazione e alla modifica delle informazioni[82].

L'elenco degli utenti abilitati all'accesso al sistema, con i diversi livelli di autorizzazioni, è riportato nell'allegato (Allegato n. 23).

12.2 *Accesso esterno*

L'accesso ai documenti è disciplinato dal Regolamento per l'accesso agli atti (Allegato n. 24) e secondo le modalità di seguito descritte[83].
L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con i seguenti strumenti tecnologici[84]:

- sistema di autenticazione al portale web con credenziali fornite dall'AOO. Le credenziali e la relativa profilatura danno accesso ai soli documenti di pertinenz

L'ente/organizzazione provvede a pubblicare sul sito istituzionale, all'interno della sezione "*Amministrazione Trasparente"* i dati, i documenti e le informazioni secondo quanto previsto dalla normativa di settore e come specificato nel "*Programma triennale per la trasparenza e l'integrità*" (Allegato n. 25).
I documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria sono pubblicati in formato di tipo aperto[85].
I dati, le informazioni e i documenti oggetto di pubblicazione obbligatoria sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di

[81] Specificare quali sono le modalità di accesso al sistema di gestione documentale (es. *username e password*).
[82] Qualora fosse necessario l'ente/organizzazione indica le eventuali altre abilitazioni.
[83] Solo in caso di gestione associata di servizi specificare che durante la permanenza nell'Archivio dell'Unione/Consorzio ecc. dei documenti spettanti ai singoli enti, il capofila ha l'obbligo di espletare quanto previsto dalla Legge 241/1990, dal dlgs. 196/03, dal Codice Civile e dalla legislazione italiana in materia di documenti, accesso e trasparenza.
[84] Indicare quali dei seguenti strumenti utilizza: firme elettroniche, firme digitali, Carta Nazionale dei Servizi (CNS), sistemi di autenticazione riconosciuti dall'AOO ecc.

pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti, fatti salvi i diversi termini previsti dalla normativa in materia di trattamento dei dati personali. Alla scadenza del termine di durata dell'obbligo di pubblicazione, i documenti, le informazioni e i dati sono comunque conservati e resi disponibili, all'interno di distinte sezioni del sito istituzionale e segnalate nell'ambito della sezione "*Amministrazione trasparente*".

L'obbligo previsto dalla normativa vigente di pubblicare documenti, informazioni o dati comporta il diritto di chiunque a richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione (accesso civico).

Lo scambio dei documenti informatici tra le varie amministrazioni[86], e con i cittadini, avviene attraverso meccanismi di "interoperabilità" e "cooperazione applicativa".

[85] Indicare i tipi di formato aperto.

[86] Qualora ci siano amministrazioni esterne che accedono alle banche dati, l'ente deve dichiarare se tali accessi sono disciplinati da specifiche convenzioni.

13 *Approvazione, revisione e pubblicazione*

13.1 *Approvazione*

Il presente manuale è adottato da Istituto Comprensivo Statale Via Maniago[87], su proposta del Responsabile del servizio di gestione documentale.

13.2 *Revisione*

Il presente manuale è rivisto, ordinariamente, ogni due anni[88] su iniziativa del Responsabile del servizio di gestione documentale. Qualora se ne presenti la necessità, si potrà procedere a revisione o integrazione del manuale anche prima della scadenza prevista.

13.3 *Pubblicazione e divulgazione*

Il Manuale di gestione è reso pubblico tramite la sua diffusione sul sito internet dell'Amministrazione, secondo le modalità previste dalla normativa vigente.

[87] Specificare la denominazione dell'organo di governo.
[88] I due anni sono indicativi.

Allegato 1 – Glossario dei termini

Oggetto/Soggetto	
AMMINISTRAZIONI CERTIFICANTI	Le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni procedenti (*art. 1, comma 1, lett. p) del DPR n. 445/2000*);
AMMINISTRAZIONI PROCEDENTI	Le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi che ricevono le dichiarazioni sostitutive ovvero provvedono agli accertamenti d'ufficio (*art. 1, comma 1 lett. o) DPR n. 445/2000*);
AMMINISTRAZIONI PUBBLICHE	Per amministrazioni pubbliche si intendono quelle indicate nell'art. 1, comma 2 del d. lgs. 30 marzo 2001, n. 165;
AMMINISTRAZIONI PUBBLICHE CENTRALI	Le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300 (*art. 1, comma 1 lett. z) del d. lgs.7 marzo 2005, n. 82*);
ARCHIVIO	L'archivio è la raccolta ordinata degli atti spediti, inviati o comunque formati dell'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'Amministrazione o dalla Area Organizzativa Omogenea sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico. L'archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, l'archivio viene suddiviso in tre sezioni: corrente, di deposito e storica;
ARCHIVIO CORRENTE	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale;
ARCHIVIO DI DEPOSITO	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento del procedimento amministrativo o comunque verso i quali sussista un interesse sporadico;
ARCHIVIO STORICO	Costituito da complessi di documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto, alla conservazione perenne;
ARCHIVIAZIONE ELETTRONICA	Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione *(art. 1 della Deliberazione CNIPA 19 febbraio 2004 n. 11);*
AREA ORGANIZZATIVA OMOGENEA (**AOO**)	Un insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato *(art. 2, lett. n) del DPCM 31 ottobre 2000*);
ASSEGNAZIONE	L'operazione d'individuazione dell'Ufficio Utente (UU) competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
AUTENTICAZIONE DI SOTTOSCRIZIONE	L'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive (*art. 1, comma 1, lett. i) del DPR 28 dicembre 2000, n. 445*);
AUTENTICAZIONE INFORMATICA	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso; (*art. 1, comma 1 lett. b) del d. lgs.7 marzo 2005, n. 82*);

BANCA DI DATI	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti (*art. 4 comma 1 lett. o) del d. lgs. 30 giugno 2003 n. 196*);
BLOCCO	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento (*art. 4, comma 1, lett. d) del d. lgs. 30 giugno 2003 n. 196*);
CARTA NAZIONALE DEI SERVIZI	Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni (*art. 1 del d. lgs.7 marzo 2005, n. 82*);
CARTA D'IDENTITÀ ELETTRONICA	Il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare (*art. 1 comma 1, lett. c) del d. lgs.7 marzo 2005, n. 82*);
CASELLA DI POSTA ELETTRONICA ISTITUZIONALE	La casella di posta elettronica istituita da una AOO, attraverso la quale vengono ricevuti i messaggi da protocollare (ai sensi del DPCM 31 ottobre 2000, articolo 15, comma 3). (*art. 1 dell'allegato A alla circolare AIPA 7 maggio 2001 n. 28*);
CERTIFICATI ELETTRONICI	Gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi (*art. 1, comma 1 lett. e) del d. lgs.7 marzo 2005, n. 82*);
CERTIFICATO QUALIFICATO	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (*art. 1 comma 1 lett. f) del d. lgs.7 marzo 2005, n. 82*);
CERTIFICATO	Il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione o partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche (*art. 1 comma 1 lett. f) del DPR 28 dicembre 2000, n. 445*);
CERTIFICATORE	Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (*art. 1, comma 1 lett. g) del d. lgs. 7 marzo 2005, n. 82*);
CLASSIFICAZIONE	L'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione;
COMUNICAZIONE	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (*art. 4 comma 1 lett. l) del d. lgs. 30 giugno 2003 n. 196*);
CONSERVAZIONE A NORMA	Processo effettuato con le modalità di cui agli articoli 3 e 4 della deliberazione CNIPA 19 febbraio 2004, n.11;
CREDENZIALI DI AUTENTICAZIONE	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (*art. 4 comma 3 lett. d) del d. lgs. 30 giugno 2003 n. 196*);
DATI GIUDIZIARI	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (*art. 4, comma 1 lett. e) del d. lgs. 30 giugno 2003 n. 196*);
DATI IDENTIFICATIVI	I dati personali che permettono l'identificazione diretta dell'interessato (*art. 4, comma 1 lett. c) del d. lgs. 30 giugno 2003 n. 196*);
DATI SENSIBILI	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 religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (*art. 4 comma 1, lett. ddd) del d. lgs. 30 giugno 2003 n. 196*);
DATO ANONIMO	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (*art. 4 comma 1 lett. n) del d. lgs. 30 giugno 2003 n. 196*);

DATO PERSONALE	Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (*art. 4 comma 1 lett. b) del d. lgs. 30 giugno 2003 n. 196*);
DATO PUBBLICO	Il dato conoscibile da chiunque (*art. 1 comma 1 lett. n) del d. lgs. 7 marzo 2005, n. 82)*;
DATO A CONOSCIBLITÀ LIMITATA	Il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti (*art. 1 comma 1 lett. l) del d. lgs.7 marzo 2005, n. 82*);
DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETÀ	Il documento sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dall' *art. 1 comma 1 lett. h) del DPR 28 dicembre 2000, n. 445;*
DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE	Il documento, sottoscritto dall'interessato, prodotto in sostituzione del certificato (*art. 1 comma 1 lett. g) del DPR 28 dicembre 2000, n. 445*);
DIFFUSIONE	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (*art. 4 del d. lgs. 30 giugno 2003 n. 196*);
DOCUMENTO	Rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica (*art. 1 comma 1 lett. a) Deliberazione CNIPA del 19 febbraio 2004 n.11*);
DOCUMENTO AMMINISTRATIVO	Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa (*art. 1 comma 1 lett. a) del DPR 28 dicembre 2000, n. 445*);
DOCUMENTO ANALOGICO	Documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia (*art. 1 comma 1 lett. b) Deliberazione CNIPA del 19 febbraio 2004, n.11);*
DOCUMENTO ANALOGICO ORIGINALE	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (*art. 1 Deliberazione CNIPA del 19 febbraio 2004 n. 11);*
DOCUMENTO ARCHIVIATO	Documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica (*art. 1 comma 1 lett. h) Deliberazione CNIPA del 19 febbraio 2004 n. 11);*
DOCUMENTO CONSERVATO	Documento sottoposto al processo di conservazione a norma (*art. 1 Deliberazione CNIPA del 19 febbraio 2004 n. 11);*
DOCUMENTO DI RICONOSCIMENTO	Ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare. (*art. 1 comma 1 lett. c) del DPR 28 dicembre 2000, n. 445*);
DOCUMENTO D'IDENTITÀ	La carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare (*art. 1 comma 1 lett. d) del DPR 28 dicembre 2000, n. 445*);
DOCUMENTO D'IDENTITÀ ELETTRONICO	Il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età (*art. 1 comma 1 lett. e) del DPR 28 dicembre 2000, n. 445*);
DOCUMENTO INFORMATICO	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (*art. 1 comma 1 lett. t) del d. lgs.7 marzo 2005, n. 82*);
DOSSIER	È una aggregazione di più fascicoli che può essere costituita a seguito di esigenze operative dell'Amministrazione, *come ad esempio, dossier riferiti ad un Ente o ad una persona che contengono fascicoli relativi a diversi procedimenti che riguardano lo stesso Ente o la stessa persona;*
ESIBIZIONE	Operazione che consente di visualizzare un documento conservato e di ottenerne copia (*art. 1 comma 1 lett. n) della deliberazione AIPA 19 febbraio 2004 n. 11*);
EVIDENZA INFORMATICA	Una sequenza di simboli binari (bit) che può essere elaborata da

	una procedura informatica (*art. 1 comma 1, lett. f) del DPCM 13 gennaio 2004*);
FASCICOLAZIONE	L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi.
FASCICOLO	Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento/processo amministrativo, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se è non è infrequente la creazione di fascicoli formati di insieme di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc.). I fascicoli costituiscono il tipo di unità archivistica più diffusa degli archivi contemporanei e sono costituiti, in base alle esigenze di servizio, secondo criteri che sono stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento;
FIRMA DIGITALE	Un particolare tipo di firma elettronica qualificata basata 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 lett. s) del d. lgs.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 autenticazione informatica (*art. 1, comma 1, lett. q) del d. lgs.7 marzo 2005, n. 82*);
FIRMA ELETTRONICA QUALIFICATA	La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica (*art. 1 comma 1 lett. r) del d. lgs.7 marzo 2005, n. 82*);
FORMAZIONE DEI DOCUMENTI INFORMATICI	Il processo di generazione del documento informatico al fine di rappresentare atti, fatti e dati riferibili con certezza al soggetto e all'amministrazione che lo hanno prodotto o ricevuto. Esso reca la firma digitale, quando prescritta, ed è sottoposto alla registrazione del protocollo o ad altre forme di registrazione previste dalla vigente normativa (*art. 2 della deliberazione AIPA 23 novembre 2000 n. 51*);
FUNZIONE DI HASH	Una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali (*art. 1 comma 1 lett. e) del DPCM 13 gennaio 2004*);
GARANTE (della Privacy)	L'autorità di cui all'articolo 153 del d. lgs. 30 giugno 2003 n. 196, istituita dalla legge 31 dicembre 1996, n. 675 (*art. 4 comma 1 lett. q) del d. lgs. 30 giugno 2003 n. 196*);
GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici (*art. 1 comma 1 lett. l) del d. lgs. 7 marzo 2005, n. 82*);
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash (art. 1 del DPCM 13 geo 2004);*
INCARICATI DEL TRATTAMENTO DEI DATI	Le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal responsabile;

PERSONALI	
INSERTO	È un sottoinsieme omogeneo del sottofascicolo che può essere costituito a seguito di esigenze operative dell'Amministrazione;
LEGALIZZAZIONE DI FIRMA	L'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa (*art. 1 comma 1 lett. l) del DPR 28 dicembre 2000, n. 445*);
LEGALIZZAZIONE DI FOTOGRAFIA	L'attestazione, da parte di una pubblica amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato (*art. 1 comma 1 lett. n) del DPR 28 dicembre 2000, n. 445*);
MARCA TEMPORALE	Un'evidenza informatica che consente la validazione temporale (*art. 1 comma 1 lett. i) del DPCM 31 gennaio 2004*);
MASSIMARIO DI SELEZIONE E SCARTO DEI DOCUMENTI/PIANO DI CONSERVAZIONE	Il massimario di selezione e scarto è lo strumento che consente di effettuare razionalmente lo scarto archivistico dei documenti prodotti e ricevuti dalle pubbliche amministrazioni. Il massimario riproduce l'elenco delle partizioni e sottopartizioni del titolario con una descrizione più o meno dettagliata dei procedimenti/procedure attivate per le funzioni a cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascun procedimento/procedura, quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nei competenti archivi di Stato per gli uffici dello Stato o per la sezione degli archivi storici per gli Enti pubblici) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc. o secondo le esigenze dell'Amministrazione/AOO. Ne consegue il PIANO DI CONSERVAZIONE periodica o permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;
MEMORIZZAZIONE	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi dell'articolo 10, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 così come modificato dall'articolo 6 del decreto legislativo 23 gennaio 2002, n. 10 (*art 1, comma 1, lett. f) Deliberazione CNIPA del 19 febbraio 2004 n.11);*
MISURE MINIME DI SICUREZZA	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del d. lgs. 30 giugno 2003 n. 196 (*art. 4 comma 3 lett. a) del d. lgs. 30 giugno 2003 n. 196*);
PAROLA CHIAVE	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica (*art. 4, comma 3, lett. e) del d. lgs. 30 giugno 2003, n. 196*);
ORIGINALI NON UNICI	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (*art. 1, comma 1, lett. v) del d. lgs. 7 marzo 2005, n. 82*);
PIANO DI CONSERVAZIONE DEGLI ARCHIVI	Vedi MASSIMARO DI SELEZIONE E SCARTO
PROFILO DI AUTORIZZAZIONE	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti (*art. 4, comma 3, lett. f) del d. lgs. 30 giugno 2003 n. 196*);
PUBBLICO UFFICIALE	Il notaio, salvo quanto previsto dall'art. 5, comma 4 della Deliberazione CNIPA del 19 febbraio 2004, n. 11 e nei casi per i quali possono essere chiamate in causa le altre figure previste dall'art. 18, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (*art. 1 Deliberazione CNIPA del 19 febbraio 2004, n. 11);*
RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (*art. 4, comma 1, lett. g) del d. lgs. 30 giugno 2003 n. 196*);
RESPONSABILE DEL SERVIZIO DI PROTOCOLLO	Il responsabile del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi di cui all'articolo 62, comma 2, del DPR 28 dicembre 2000, n. 445;
RESPONSABILI DEI PROCEDIMENTI AMMINISTRATIVI (**RPA**)	È la persona, alla quale è stata affidata la trattazione di un affare amministrativo ivi compresa la gestione/creazione del relativo fascicolo dell'archivio corrente;

RIFERIMENTO TEMPORALE	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (*art 1, comma 1, lett. g) del DPCM 13 gennaio 2004*) o ad un messaggio di posta elettronica certificata (*art. 1, comma 1, lett. i), del DPR 11 febbraio 2005, n. 68*);
RIVERSAMENTO DIRETTO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica (*art. comma 1, lett. l) Deliberazione CNIPA del 19 febbraio 2004, n. 11);*
RIVERSAMENTO SOSTITUTIVO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica (*art. 1, comma 1, lett. o) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);*
SCOPI SCIENTIFICI	Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore (*art. 4, comma 4, lett. c) del d. lgs. 30 giugno 2003 n. 196*);
SCOPI STATISTICI	Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici (*art. 4, comma 4, lett. b) del d. lgs. 30 giugno 2003 n. 196*);
SCOPI STORICI	Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato (*art. 4, comma 4, lett. a) del d. lgs. 30 giugno 2003 n. 196*);
SEGNATURA INFORMATICA	L'insieme delle informazioni archivistiche di protocollo, codificate in formato XML ed incluse in un messaggio protocollato, come previsto dall'articolo 18, comma 1, del DPCM 31 ottobre 2000 (*art. 1 dell'allegato A della circolare AIPA 7 maggio 2001 n. 28);*
SEGNATURA DI PROTOCOLLO	L'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso (*Glossario dell'IPA Indice delle Pubbliche Amministrazioni*);
SISTEMA DI CLASSIFICAZIONE	Lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata *(art. 2, comma 1, lett. h) del DPCM 31 ottobre 2000);*
SISTEMA DI AUTORIZZAZIONE	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente (*art. 4, comma 3, lett. g) del d. lgs. 30 giugno 2003 n. 196*);
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti (*art. 1, comma 1, lett. r) del DPR 28 dicembre 2000 n. 445*);
STRUMENTI ELETTRONICI	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento di dati.

Allegato 2 – Elenco unità organizzative

Denominazione dell'Amministrazione	**Istituto Comprensivo Statale Via Maniago**
Codice identificativo assegnato all'Amministrazione	MIIC8D4005
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	Via Maniago 30 20134 Milano
Elenco delle AREE ORGANIZZATIVE OMOGENEE – AOO	istsc_miic8d4005

Allegato 3 - Atto di nomina del responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

Determinazione n. prot. 10591 del 15/12/2017

Oggetto: **Nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi e del suo Vicario.**

In data odierna, nell'amministrazione di

ISTITUTO COMPRENSIVO STATALE VIA MANIAGO
VIA MANIAGO 30
20134 MILANO (MI)

<< IL DIRIGENTE >>

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi e delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

VISTO in particolare l'articolo 61, comma 2, il quale tra l'altro, stabilisce che presso il servizio gratuito del protocollo informatico, è preposto un dirigente, ovvero un funzionario, comunque in possesso di idonei requisiti professionali e di professionalità tecnico archivistica;

VISTO il Decreto ministeriale 14 ottobre 2003 "Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi", nel quale sono indicati gli adempimenti delle amministrazioni relativamente al protocollo informatico ed alla gestione dei procedimenti amministrativi con tecnologie informatiche;

RITENUTO di individuare nel/nella signor/signora Anita Talarico, in servizio presso l'Ufficio di Segreteria di questa istituzione scolastica, la figura professionale più idonea ad espletare i compiti di seguito indicati:

• predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
• provvedere alla pubblicazione del Manuale anche su Internet;
• proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax, e, più in generale, dei protocolli diversi dal protocollo informatico;
• predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il:
– Responsabile dei sistemi informativi automatizzati,
– Referente della pianificazione delle attività,
– Responsabile della sicurezza dei dati personali, se nominato, o direttamente con il Titolare dei

trattamenti dei dati di cui al d. lgs. 196/03,
– Responsabile del servizio archivistico,
– Responsabile della conservazione a norma;
• attribuire il livello di autorizzazione di ciascun addetto all'accesso alle funzioni delle procedure applicative di gestione del protocollo informatico e gestione documentale distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento, alla modifica e alla cancellazione delle informazioni;
• garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
• garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
• garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalla normativa corrente, ovvero altri formati non proprietari;
• curare, anche attraverso altri responsabili, le funzionalità del sistema di gestione informatica del protocollo e della gestione documentale affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
• conservare le copie di salvataggio delle informazioni del sistema e del registro di emergenza in luoghi sicuri differenti;
• garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso esterno o da altre Amministrazioni e le attività di gestione degli archivi, quali, trasferimento dei documenti all'archivio di deposito, disposizioni per la conservazione degli archivi e Archivi storici;
• autorizzare le operazioni di annullamento della registratura di protocollo;
• vigilare sull'osservanza delle disposizioni delle norme correnti da parte del personale autorizzato e degli incaricati.

<< DETERMINA >>

1. di nominare il/la signore/a Anita Talarico, quale Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi ai sensi dell'articolo 61 comma 2 del DPR n. 445/2000 con i compiti specificati nelle premesse.
2. di nominare vicario del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, per i casi di vacanza, assenza o impedimento del Responsabile, viene nominato il/la signor/signora Rinaldi Umberto in servizio presso la Segreteria di questa Istituzione.

Allegato 4 – Nomina a Amministratore di Rete

All'atto della pubblicazione del presente documento, la figura di Amministratore di Rete è rappresentata dal sig. BASSI FERDINANDO, in qualità di Amministratore / Responsabile Reparto Tecnico della società:

Easyteam.org SRL
Via Walter Tobagi 2
20067 Tribiano (MI)

Con la quale codesta amministrazione ha in essere un contratto di assistenza informatica, regolarmente pubblicato agli atti dell'Albo On Line dell'Istituto.

Allegato 5

Determinazione n. prot. 10591 del 15/12/2017

Oggetto: **Nomina del Responsabile del Servizio di conservazione a norma**

In data odierna, nell'amministrazione di

ISTITUTO COMPRENSIVO STATALE VIA MANIAGO
VIA MANIAGO 30
20134 MILANO (MI)

<< IL DIRIGENTE>>

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

CONSIDERATO che il sistema di gestione informatica dei documenti deve garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalla normativa corrente, ovvero altri formati non proprietari;

VISTO l'art. 62 comma 1 del DPR n. 445/2000 concernente le procedure di salvataggio e conservazione delle informazioni del sistema di gestione elettronica dei documenti;

CONSIDERATO che Il Responsabile intende delegare le attività operative di conservazione a norma dei documenti digitali dell'Amministrazione/AOO a soggetto diverso da se medesimo;

RITENUTO di individuare nel/nella signor/signora Anita Talarico, in servizio presso la Segreteria di questa Istituzione, la figura professionale più idonea ad espletare i compiti di seguito indicati:
• rendere le informazioni trasferite sempre consultabili;
• provvedere alla conservazione degli strumenti hardware e software atti a garantire la consultabilità dei documenti conservati;
• eseguire, in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno quinquennale, la riproduzione delle informazioni del protocollo informatico su nuovi supporti informatici.

<< DETERMINA >>

di nominare il/la signore/a Anita Talarico, quale Responsabile del Servizio di conservazione a norma con i compiti assegnati nelle premesse. Il Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, mantiene la responsabilità della corretta esecuzione delle operazioni.

Determinazione n. prot. 10590 del 15/12/2017

Oggetto: **Nomina del responsabile della conservazione delle copie di riserva del registro di protocollo informatico**

In data odierna, nell'amministrazione di

ISTITUTO COMPRENSIVO STATALE VIA MANIAGO
VIA MANIAGO 30
20134 MILANO (MI)

<< IL DIRIGENTE >>

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

CONSIDERATO che, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della giornata lavorativa, deve essere riversato su supporti informatici non riscrivibili e deve essere conservato da soggetto diverso dal responsabile del servizio appositamente nominato da ciascuna amministrazione ai sensi dell'art. 7, comma 7 del DPCM 31 0ttobre 2000;

VISTA la determinazione numero prot. 10591 del 15/12/2017 relativa alla nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi;

CONSIDERATA l'esigenza di conservare in luogo sicuro le copie del registro di protocollo che quotidianamente vengono generate dal sistema informativo di protocollo;

RITENUTO di individuare nel/nella signor/signora Rinaldi Umberto, in servizio presso la Segreteria di questa Istituzione, la figura professionale più idonea ad espletare i compiti di seguito indicati:

- definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o digitali) da conservare, dei quale tiene evidenza;
- organizzare, conseguentemente, il contenuto dei supporti ottici e gestire le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
- archiviare e rendere disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
  a. descrizione del contenuto dell'insieme dei documenti;
  b. estremi identificativi del responsabile della conservazione;
  c. estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione, con l'indicazione dei compiti alle stesse assegnati;
  d. indicazione delle copie di sicurezza;
- mantenere e rendere accessibile un archivio del software dei sistemi operativi e dei programmi in

gestione nelle eventuali diverse versioni per la leggibilità dei documenti conservati;
- verificare la corretta funzionalità del sistema e dei programmi in gestione;
- adottare, su indicazione del Responsabile del servizio di gestione del protocollo informatico, le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione a norma e delle copie di sicurezza dei supporti di memorizzazione;
- richiedere la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- definire e documentare le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale sui supporti informativi di propria pertinenza;
- verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

<< DETERMINA >>

di nominare il/la signore/a Rinaldi Umberto, quale Responsabile della conservazione delle copie di riserva del registro di protocollo informatico con i compiti specificati nelle premesse, ai sensi dell'art. 7, comma 5 del DPCM 31 ottobre 2000.

Allegato 6 – Titolario di classificazione

I. AMMINISTRAZIONE

1. Normativa e disposizioni attuative
2. Organigramma e funzionigramma
3. Audit, statistica e sicurezza di dati e informazioni
4. Archivio, accesso, privacy, trasparenza e relazioni con il pubblico
5. Qualità, carta dei servizi, valutazione e autovalutazione
6. Elezioni e nomine
7. Eventi, cerimoniale, patrocini, concorsi, editoria e stampa

II. ORGANI E ORGANISMI

1. Consiglio di istituto, Consiglio di circolo
2. Consiglio di classe e di interclasse
3. Collegio dei docenti
4. Giunta esecutiva
5. Dirigente scolastico DS
6. Direttore dei servizi generali e amministrativi DSGA
7. Comitato di valutazione del servizio dei docenti
8. Comitato dei genitori, Comitato studentesco e rapporti scuola-famiglia
9. Reti scolastiche
10. Rapporti sindacali, contrattazione e Rappresentanza sindacale unitaria (RSU)

III. ATTIVITÀ GIURIDICO-LEGALE

1. Contenzioso
2. Violazioni amministrative e reati
3. Responsabilità civile, penale e amm.va
4. Pareri e consulenze

IV. DIDATTICA

1. Piano dell'offerta formativa POF
2. Attività extracurricolari
3. Registro di classe, dei docenti e dei profili
4. Libri di testo
5. Progetti e materiali didattici
6. Viaggi di istruzione, scambi, stage e tirocini
7. Biblioteca, emeroteca, videoteca e sussidi
8. Salute e prevenzione
9. Attività sportivo-ricreative e rapporti con il Centro Scolastico Sportivo

V. STUDENTI E DIPLOMATI

1. Orientamento e placement
2. Ammissioni e iscrizioni
3. Anagrafe studenti e formazione delle classi
4. Cursus studiorum
5. Procedimenti disciplinari

6. Diritto allo studio e servizi agli studenti (trasporti, mensa, buoni libro, etc.)
7. Tutela della salute e farmaci
8. Esoneri
9. Prescuola e attività parascolastiche
10. Disagio e diverse abilità – DSA

VI. FINANZA E PATRIMONIO

1. Entrate e finanziamenti del progetto
2. Uscite e piani di spesa
3. Bilancio, tesoreria, cassa, istituti di credito e verifiche contabili
4. Imposte, tasse, ritenute previdenziali e assistenziali
5. Assicurazioni
6. Utilizzo beni terzi, comodato
7. Inventario e rendiconto patrimoniale
8. Infrastrutture e logistica (plessi, succursali)
9. DVR e sicurezza
10. Beni mobili e servizi
11. Sistemi informatici, telematici e fonia

VII. PERSONALE

1. Organici, lavoratori socialmente utili, graduatorie
2. Carriera
3. Trattamento giuridico-economico
4. Assenze
5. Formazione, aggiornamento e sviluppo professionale
6. Obiettivi, incarichi, valutazione e disciplina
7. Sorveglianza sanitaria
8. Collaboratori esterni

VIII. OGGETTI DIVERSI

Allegato 7 – Profili di accesso

Vengono individuati i seguenti profili di accesso.

Ruolo amministrativo. **Responsabile PdP**
Ruolo funzionale: **Amministratore PdP**

Funzione	**C**	**I**	**M**	**A**
Protocollo	X	X	X	X
Registro di Protocollo	X	X	X	X
Cambio Anno	X	X	X	X
Registro Protocollo	X	X	X	X
Istruttoria Protocollo	X	X	X	X
Registro Istruttoria Protocollo	X	X	X	X
Stampe Archivi Complementari	X	X	X	X
Stampe Archivi Complementari	X	X	X	X
Stampa Etichette	X	X	X	X
Stampa Etichette	X	X	X	X
Stampe Registro Protocollo	X	X	X	X
Stampa Registro Istruttoria Protocollo	X	X	X	X
Stampe Registro Protocollo	X	X	X	X
Tabelle	X	X	X	X
Aree Organizzative Omogenee	X	X	X	X
Attuali Destinatari	X	X	X	X
Fonti	X	X	X	X
Gestione Amministrazione	X	X	X	X
Mezzi di Trasmissione	X	X	X	X
Mittenti Destinatari	X	X	X	X
Oggetti	X	X	X	X
Parametri Generali	X	X	X	X
Parametri generali registro riservato	X	X	X	X
Soggetti	X	X	X	X
Tipo di evasione	X	X	X	X
Tipi di atto	X	X	X	X
Titolario	X	X	X	X
Uffici	X	X	X	X
Utilità	X	X	X	X
Server Info	X	X	X	X
Verifica Archivio Protocollo	X	X	X	X
Verifica Integrità Numero di Protocollo	X	X	X	X
Registro di Emergenza	X	X	X	X
Registro di Emergenza	X	X	X	X
Registro Protocollo Giornaliero	X	X	X	X
Registro Protocollo Giornaliero	X	X	X	X
Registro Protocollo Riservato	X	X	X	X
Registro Protocollo Riservato	X	X	X	X
Segreteria Digitale	X	X	X	X

Connetti SD	X	X	X	X
Disconnetti SD	X	X	X	X
Richiesta Documenti da Protocollare	X	X	X	X

Ruolo amministrativo. **Operatore PdP**
Ruolo funzionale: **Operatore PdP**

Funzione	**C**	**I**	**M**	**A**
Protocollo	X	X		X
Registro di Protocollo	X	X		X
Cambio Anno				
Registro Protocollo	X	X		X
Istruttoria Protocollo	X	X		X
Registro Istruttoria Protocollo	X	X		X
Stampe Archivi Complementari	X	X		X
Stampe Archivi Complementari	X	X		X
Stampa Etichette	X	X		X
Stampa Etichette	X	X		X
Stampe Registro Protocollo	X	X		X
Stampa Registro Istruttoria Protocollo	X	X		X
Stampe Registro Protocollo	X	X		X
Tabelle				
Aree Organizzative Omogenee				
Attuali Destinatari				
Fonti				
Gestione Amministrazione				
Mezzi di Trasmissione				
Mittenti Destinatari				
Oggetti				
Parametri Generali				
Parametri generali registro riservato				
Soggetti				
Tipo di evasione				
Tipi di atto				
Titolario				
Uffici				
Utilità				
Server Info				
Verifica Archivio Protocollo	X	X		X
Verifica Integrità Numero di Protocollo	X	X		X
Registro di Emergenza	X	X		X
Registro di Emergenza	X	X		X
Registro Protocollo Giornaliero	X	X		X
Registro Protocollo Giornaliero	X	X	X	X
Registro Protocollo Riservato				
Registro Protocollo Riservato				

Segreteria Digitale	X	X	X	X
Connetti SD	X	X	X	X
Disconnetti SD	X	X	X	X
Richiesta Documenti da Protocollare	X	X	X	X

Legenda:

C = Consultazione
I = Inserimento
M = Modifica
A = Accesso

Allegato 8 – Piano di sicurezza informatica

1 Politiche accettabili di uso del sistema informativo

1.1 Premessa

1. L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.
2. Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.
3. L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

1.2 Scopo

1. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.
2. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.
3. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

1.3 Ambito di applicazione

1. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato) e agli impiegati della/e ditta/e Axios Italia di Roma e suoi rappresentanti sul territorio nazionale, includendo tutto il personale affiliato con terze parti.
2. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

1.4 Politiche – Uso generale e proprietà

1. Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.
2. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.
3. Le singole aree o settori o Divisioni o Direzioni, sono responsabili della creazione di linee guida per

l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare il loro Dirigente.

4. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.
5. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

1.5 Politiche - Sicurezza e proprietà dell'informazione

1. Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.
2. Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password devono essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi. Le password devono rispondere ai requisiti di complessità così come previsto dal D.lgs 196/2003.
   Al momento della redazione del presente documento non sono presenti sistemi che registrano in chiaro le password; tutti i servizi web sono dotati di protocollo HTTPS e tutti i sistemi locali utilizzano sistemi di archiviazione crittografata delle credenziali.
3. Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico.
4. Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.
5. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.
6. Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "new group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.
7. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.
8. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.
9. Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

2 Politiche accettabili di uso del sistema informativo

2.1 Premessa

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.
I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.
I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

2.2 Scopo
Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

2.3 Ambito di applicazione
Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

2.4 Politiche per le azioni preventive
- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.
- Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.
- Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
- Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
- Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
- Non scaricare mai messaggi da siti o sorgenti sospette.
- Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
- Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
- Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
- Evitare collegamenti diretti ad Internet via modem.
- Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.
- Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura.
- Non utilizzare i server di rete come stazioni di lavoro.
- Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.
- Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.

- Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno.
- Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.
- Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.
- I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
- Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico… [omissis]…che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
- Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
- È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

2.5 Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

- verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
- verificare se il virus ha diffuso dati;
- identificare il virus;
- attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
- diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

3 Politiche – uso non accettabile

1. Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).
2. In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.
3. L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

3.1 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che

non sono espressamente licenziati per essere usati dall'Amministrazione.

2. Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
5. Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
6. Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
    a. accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
    b. attività di "sniffing";
    c. disturbo della trasmissione;
    d. spoofing dei pacchetti;
    e. negazione del servizio;
    f. le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
    g. attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

3.2 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
3. Uso non autorizzato delle informazioni della testata delle e-mail,
4. Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare

servizi erogati dall'Amministrazione e fruibili via Intranet stessa.

6. Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

4 Linee telefoniche commutate (analogiche e digitali)

4.1 Scopo

2. Di seguito vengono illustrate le linee guida per un uso corretto delle linee telefoniche commutate (analogiche convenzionali) e digitali (ISDN, ADSL).
3. Queste politiche coprono due diversi usi distinti: linee dedicate esclusivamente ai telefax e linee di collegamento alle risorse elaborative dell'Amministrazione.

4.2 Ambito di applicazione

1. Queste politiche sono relative solo a quelle linee che sono terminate all'interno della/e sede/i dell'Amministrazione. Sono pertanto escluse le eventuali linee collegate con le abitazioni degli impiegati che operano da casa e le linee usate per gestire situazioni di emergenza.

4.3 Politiche – Scenari di impatto sull'Amministrazione

1. Esistono due importanti scenari che caratterizzano un cattivo uso delle linee di comunicazione che tentiamo di tutelare attraverso queste politiche.
2. Il primo è quello di un attaccante esterno che chiama un gruppo di numeri telefonici nella speranza di accedere alle risorse elaborative che hanno un modem collegato. Se il modem è predisposto per la risposta automatica, allora ci sono buone probabilità di accesso illecito al sistema informativo attraverso un server non monitorato. In questo scenario, al minimo possono essere compromesse solo le informazioni contenute sul server.
3. Il secondo scenario è la minaccia di una persona esterna che può accedere fisicamente alle risorse dell'Amministrazione e utilizza illecitamente un PC da tavolo o portatile corredato di un modem connesso alla rete. In questo caso l'intruso potrebbe essere capace di connettersi, da un lato, alla rete sicura dell'Amministrazione attraverso la rete locale e, dall'altro, simultaneamente di collegarsi con il modem ad un sito esterno sconosciuto (ma precedentemente predisposto). Potenzialmente potrebbe essere possibile trafugare tutte le informazioni dell'Amministrazione, comprese quelle vitali.

4.4 Politiche – Telefax

1. Dovrebbero essere adottate le seguenti regole:
    a. le linee fax dovrebbero essere approvate solo per uso istituzionale;
    b. nessuna linea dei telefax dovrebbe essere usata per uso personale;
2. Le postazioni di lavoro che sono capaci di inviare e ricevere fax non devono essere utilizzate per svolgere questa funzione.
3. Eventuali deroghe a queste politiche possono essere valutate ed eventualmente concesse dal Responsabile della sicurezza caso per caso dopo una attenta valutazione delle necessità dell'Amministrazione rispetto ai livelli di sensitività dei dati.

4.5 Politiche – Collegamento di PC alle linee telefoniche analogiche

1. La politica generale è quella di non approvare i collegamenti diretti dei PC alle linee telefoniche commutate.
2. Le linee commutate rappresentano una significativa minaccia per l'Amministrazione di attacchi esterni. Le eccezioni alle precedenti politiche dovrebbero essere valutate caso per caso dal

responsabile della sicurezza.

4.6 Politiche – Richiesta di linee telefoniche analogiche

Una volta approvata la richiesta individuale di linea commutata dal responsabile dell'incaricato all'uso della linea medesima, questa deve essere corredata dalle seguenti informazioni da indirizzare al responsabile della sicurezza di rete:

- una chiara e dettagliata relazione che illustri la necessità di una linea commutata dedicata in alternativa alla disponibilità di rete sicura dell'Amministrazione;
- lo scopo istituzionale per cui si rende necessaria la linea commutata;
- il software e l'hardware che deve essere collegato alla linea e utilizzato dall'incaricato;
- che cosa la connessione esterna richiede per essere acceduta.

5 Politiche per l'inoltro automatico di messaggi di posta elettronica

5.1 Scopo

1. Lo scopo di queste politiche è prevenire rivelazioni non autorizzare o involontarie di informazioni confidenziali o sensitive dell'Amministrazione

5.2 Ambito di applicazione

1. Queste politiche riguardano l'inoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

5.3 Politiche

1. Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio all'esterno dell'Amministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati all'esterno dell'Amministrazione.
2. Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario.

6 Politiche per le connessioni in ingresso su rete commutata

6.1 Scopo

1. Proteggere le informazioni elettroniche dell'Amministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dall'esterno su rete commutata.

6.2 Ambito di applicazione

1. Lo scopo di queste politiche è definire adeguate modalità di accesso da remoto ed il loro uso da parte di personale autorizzato.

6.3 Politiche

1. Il personale dell'Amministrazione e le persone terze autorizzate (clienti, venditori, altre amministrazioni, cittadini, etc.) possono utilizzare la linea commutata per guadagnare l'ingresso alla Intranet dell'Amministrazione. Tale accesso dovrebbe essere rigidamente controllato usando sistemi di autenticazione forte, quali: password da usare una sola volta (one time password), sistemi di firma digitale o tecniche di sfida/risposta (challenger/response).

2. È responsabilità del personale con i privilegi di accesso dall'esterno alla rete dell'Amministrazione garantire che personale non autorizzato possa accedere illecitamente alla Intranet dell'Amministrazione ed alle sue informazioni. Tutto il personale che può accedere al sistema informativo dell'Amministrazione dall'esterno deve essere consapevole che tale accesso costituisce "realmente" una estensione del sistema informativo che potenzialmente può trasferire informazioni sensitive.
3. Il personale e le persone terze devono, di conseguenza, porre in essere tutte le ragionevoli misure di sicurezza in loro possesso per proteggere il patrimonio informativo ed i beni dell'Amministrazione.
4. Solo la linea commutata convenzionale può essere utilizzata per realizzare il collegamento.
5. Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un re instradamento della connessione.

7 Politiche per l'uso della posta istituzionale dell'amministrazione

7.1 Scopo

1. Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.

7.2 Ambito di applicazione

1. La politica di seguito descritta intende illustrare l'uso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dell'Amministrazione stessa.

7.3 Politiche – Usi proibiti

1. Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

7.4 Politiche – Uso personale

1. Non è ammesso l'uso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

8 Politiche per le comunicazioni wireless

8.1 Scopo

1. Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura.
2. Solo i sistemi wireless che si adattano a queste politiche o hanno la garanzia di sicurezza certificata dal responsabile della sicurezza, possono essere utilizzati per realizzare i collegamenti all'Amministrazione.

8.2 Ambito di applicazione

1. La politica riguarda tutti i dispositivi di comunicazione dati senza fili collegati (PC e cellulari telefonici) alla Intranet dell'Amministrazione, ovvero qualunque dispositivo di comunicazione wireless capace di trasmettere "pacchetti" di dati.

2. Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

8.3 Politiche – Registrazione delle schede di accesso

1. Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
2. Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing).
1. Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate tramite l'attribuzione di specifiche credenziali di accesso.

8.4 Politiche – Approvazione delle tecnologie

1. Tutti i dispositivi di accesso alle LAN dell'Amministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.

9. Piano di sicurezza

Il presente capitolo riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

9.1 Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'amministrazione/AOO 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.

9.2 Generalità

Il RSP ha predisposto il piano di sicurezza (o lo ha fatto predisporre sotto la sua guida e responsabilità) in collaborazione con il responsabile del sistema informativo ed il responsabile del trattamento dei dati personali e/o altri esperti di sua fiducia.
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 stabilite dal vertice dell'amministrazione, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- 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 decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, 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.

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.
Il RSP ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'Amministrazione/AOO;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno trimestrale durante la fase di esercizio;

Axios prevede il tempo massimo di validità della password impostabile dall'RSP. Il controllo quindi di tempo massimo per la validità della password può anche essere gestito in modalità automatica.
Questa Amministrazione ha deciso che è opportuno, al fine di evitare rallentamenti nel lavoro di tutti i giorni, che sia responsabilità di ogni UOP modificare la propria password di accesso secondo quanto stabilito dal presente manuale.

- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;

Il PdP Axios essendo completamente in cloud provvede in maniera autonoma ad effettuare copie di sicurezza giornaliere e garantire un ripristino delle funzionalità, in caso di malfunzionamento, entro le 24/48 ore.

- conservazione, a cura del RsP, delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

9.3 Formazione dei documenti – aspetti di sicurezza

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

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di

riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad 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 all'interno della stessa AOO e con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, XML e TIFF.
I documenti informatici prodotti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.
L'intero sistema gestionale in uso presso questa Amministrazione/AOO consente l'elaborazione e la produzione automatica di praticamente qualsiasi documento utile al corretto funzionamento della segreteria.
I documenti possono essere prodotti direttamente in formato PDF/A e firmati digitalmente nello stesso momento.
Sempre all'interno del sistema gestionale in uso è possibile anche effettuare la firma massiva di diversi documenti in un'unica soluzione.
Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).
L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.
L'amministrazione si è dotata di un sistema di marcatura temporale certificata e, sempre grazie al sistema gestionale adottato, può marcare temporalmente i documenti in modo automatico nel momento stesso in cui vengono prodotti dal sistema dando così alla marca temporale una valore di immediatezza rispetto alla produzione del documento stesso.
E' ovviamente anche possibile marcare temporalmente e massivamente una serie di documenti.

9.4 Gestione dei documenti informatici

Il sistema operativo del PdP utilizzato dall'amministrazione/AOO, è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).

- Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il PdP in uso presso questa Amministrazione ha un sistema di scrittura automatica del log delle operazioni eseguite.

Le informazioni che vengono memorizzate, sia nel log della parte client/server, sia che nelle applicazioni CLOUD sono le seguenti:

Area Indica l'area di competenza (protocollo, personale, ecc. ecc.)
Menu Sigla della maschera video utilizzata
Utente Nome utente che ha effettuato l'operazione
Data e ora operazione Data e ora (hh:mm:ss) dell'operazione
Percorso Percorso del menu seguito
Operazione Nome specifico dell'operazione
Nome del pc della rete interna Nome del pc della rete interna dell'Amministrazione/AOO
Nome del logon Nome del logon Windows
SQL eseguito (dove possibile) Istruzione SQL eseguita
Versione dell'area Versione dell'area (vedi primo campo)
Utente cloud Eventuale nome dell'utente cloud

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;

L'accesso alla base dati locale è possibile solo tramite login e password inseriti nel gestionale.
In nessun caso è possibile accedere alla base dati fuori dalla procedura sopra indicata.
La base dati è protetta e non può essere in alcun modo modificato il suo contenuto.
Il server dove è custodito il DB locale è locato in ambiente sicuro non raggiungile e l'accesso è consentito solo tramite password.

- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- La procedura interna stabilita dall'Amministrazione/AOO prevede l'immediata registrazione del protocollo prima di qualsiasi altra operazione venga effettuata sul documento.
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;

Il PdP in uso presso questa Amministrazione/AOO consente la completa gestione del ciclo del documento ivi compresa, ovviamente, la sua collocazione logica in tutti i fascicoli ove necessaria.
Ad esempio un certificato di servizio sarà legato logicamente al fascicolo generico del personale/sottofascicolo certificati di servizio, al fascicolo personale della singola utenza, al fascicolo dei documenti emessi in un certa data e, perché no, anche al fascicolo legato alla UOP che ha emesso il documento.

- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

9.4.1 Componente organizzativa della sicurezza

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione/AOO.
Nella conduzione del sistema informativo Il piano di sicurezza garantisce che:
- i documenti e le informazioni trattati dall'Istituto siano resi disponibili, autentici e integri;
- i dati personali, i dati sensibili e quelli 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..

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:
• Il piano di sicurezza, basato sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:
- le politiche generali e particolari di sicurezza da adottare all'interno dell'Istituto
- le modalità di accesso al sistema di protocollo e gestione documentale
- le misure di sicurezza operative adottate sotto il profilo organizzativo, procedurale e tecnico
- le modalità con le quali deve essere effettuato il monitoraggio periodico
dell'efficacia e dell'efficienza delle misure di sicurezza

Al fine di garantire la sicurezza dell'impianto tecnologico, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, l'Istituto ha adottato le misure tecniche e organizzative di seguito specificate:
- protezione periferica della Intranet dell'amministrazione;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno trimestrale durante la fase di esercizio
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e lontani da quelli in cui è installato il sistema di elaborazione di esercizio;
- impiego e manutenzione di un adeguato sistema antivirus;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultabili in caso di necessità dalle forze dell'ordine.
In relazione alla componente fisica della sicurezza sono stati definiti i seguenti ruoli:
• E' messo in atto ai sensi della normativa vigente6 il Piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi.

9.4.2 Componente fisica della sicurezza

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:
• Si garantisce la sicurezza fisica degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico attraverso locali dotati di:
- porte blindate
- impianti elettrici dedicati
- sistemi di raffreddamento delle apparecchiature
- la continuità elettrica è garantita dal Gruppo di continuità
- estintori
- un controllo dell'attuazione del piano di verifica periodica sull'efficacia dei sistemi di sorveglianza e degli estintori
- impianto antincendio

9.4.3 Componente logica della sicurezza

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.
Tale componente, nell'ambito del PdP, è stata realizzata attraverso:
• Login specifico per ogni utenza con password a scadenza trimestrale.
• Profilazione dei diversi utenti con accessibilità ai dati in base a stringenti criteri di sicurezza e di necessità di utilizzo degli stessi
• Richiesta conferma di tutte le operazioni di aggiornamento/cancellazione
• In caso di operazioni particolarmente delicate, il messaggio di richiesta conferma di tale operazione, viene richiesto per 2 volte
• In altri casi la funzione non viene eseguita se le copie di sicurezza non sono aggiornate alla stessa data di richiesta dell'operazione
In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza come di seguito descritto:
La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente, nell'ambito del sistema di protocollo informatico e di gestione documentale Axios, è stata realizzata attraverso:
- identificazione e autenticazione utente
- profilazione degli accessi (ACL)
- politica antivirus
- firma digitale
- monitoraggio sessioni di lavoro
- disponibilità del software e dell'hardware
L'utilizzo delle PdL e della rete intranet è garantito ai soli utenti dotati di apposite credenziali d'accesso (user ID + password) al sistema informatico dell'Istituto.
L'operatore può accedere unicamente al livello "interfaccia utente" e solamente se dotato di specifiche credenziali e autorizzazioni al sistema Axios.
L'interfaccia viene generata in funzione delle autorizzazioni in possesso dell'utente connesso; funzioni e dati ai quali l'utente non è autorizzato ad accedere non vengono resi disponibili.
Agli utenti "generici" dell'Istituto non è quindi consentito:
- interrogare direttamente il DBMS

- interagire direttamente con il repository dei file
- accedere direttamente ai server fisici e virtualizzati

Le precedenti operazioni sono possibili ai soli soggetti autorizzati ed appartenenti al Settore Servizi Informatici e Telematici per le sole attività sistemistiche di amministrazione, aggiornamento e manutenzione delle componenti di sistema.

9.4.4 Componente infrastrutturale della sicurezza

Il sistema informatico utilizza i seguenti impianti:
- scrittura su database in modalità sincrona (scrittura logica che coincide con scrittura fisica sul disco)
- copie di backup realizzate su dischi RAID in mirroring e/o RAID 5
- consegna di una copia di sicurezza dei back up in un locale diverso come previsto dalla normativa

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul PdP - 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 PdP.
Le registrazioni di sicurezza sono soggette alle seguenti misure:
• Le registrazioni del log delle operazioni effettuate dal PdP è memorizzato nella medesima base dati e la copia avviene quindi insieme alla normale copia di backup giornaliero.
• La struttura della tabella di log del PdP è stata precedentemente illustrata
• I log di sistema rimangono automaticamente residenti all'interno del sistema
• I log del firewall sono salvati all'interno del firewall stesso
• La scuola, per ora, non intende avvalersi di sistemi particolarmente sofisticati come, ad esempio, IDS.
In questa sede viene espressamente richiamato quanto indicato nell'ultimo capoverso del paragrafo 9.2 del presente Manuale.

9.5 Trasmissione ed interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.
Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'amministrazione, (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/AOO) oltre alle funzioni di un server

SMTP tradizionale, svolge anche le seguenti operazioni:
• accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
• tracciamento delle attività nel file di log della posta;
• gestione automatica delle ricevute di ritorno.
Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.
Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, dove possibile, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

9.5.1 All'esterno della AOO (Interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).
Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.
Ai sensi del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.
La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28.

9.5.2 All'interno della AOO (Interoperabilità dei sistemi di protocollo informatico)

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.
Gli Uffici dell'amministrazione (UOR) si scambiano documenti informatici attraverso l'utilizzo del sistema di posta interno completamente gestito dal software in possesso dell'Amministrazione/AOO.
L'intero scambio di informazioni all'interno del sistema viene completamente tracciato e memorizzato in una tabella di log non modificabile e non accessibile dall'esterno.
Il sistema consente anche lo scambio di informazioni all'interno dell'Amministrazione anche tramite l'utilizzo di normali caselle di posta elettronica (in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione le tecnologie concernente l'impiego della posta elettronica nelle pubbliche amministrazioni) o misto.

9.6 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata o PIN nel caso di un dispositivo rimovibile in uso esclusivo all'utente) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere

effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.
Il software Axios adottato dall'Amministrazione consente di definire per ogni utente ed ogni funzione, anche in base alla funzione stessa, se l'utente ha i diritti necessari a:
Creazione
Lettura
Aggiornamento
Cancellazione
Stampa
Duplicazione
Download
Autorizzazione speciale

Composizione della password:
La password di accesso al sistema è generata in automatico la prima volta con una lunghezza, a scelta dell'Amministrazione da 8 a 16 caratteri, con caratteri alfabetici maiuscoli, minuscoli e numeri.

Blocco delle utenze:
Il sistema utilizzato dall'Amministrazione è completamente integrato e questo consente una gestione dinamica delle utenze ed il relativo blocco delle stesse.
Se ad esempio un dipendente viene sospeso o è in malattia per un periodo, registrando l'evento all'interno dell'area personale, automaticamente l'utenza viene sospesa per il periodo necessario.
Ovviamente è possibile sospendere un'utenza in qualsiasi momento tramite la gestione dell'archivio utenze.

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password, in parte riportate di seguito, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.

Il PdP adottato dall'amministrazione/AOO:
• 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.
Il PdP in uso dall'Amministrazione/AOO consente la gestione dei gruppi di utenti e, per ogni tipo di documento è possibile associare il gruppo che lo deve lavorare e la fase del processo di cui si deve occupare.
All'interno del gruppo sono presenti poi i diversi utenti ognuno con diversi livelli di accesso e di operatività sul documento.
Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.
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.

9.6.1 Utenti interni all'AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RSP dell'amministrazione/AOO. Tali livelli si distinguono in: abilitazione alla

consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.
La gestione delle utenze rispetta i seguenti criteri operativi:
Vengono creati gruppi di utenti corrispondenti ai diversi UOR.
Vengono create le diverse tipologie di documento.
Vengono creati i flussi operativi per ogni tipologia di documento
Assegnazione dei documenti ai gruppi con specifiche funzioni in base al flusso operativo
Definizione dei livelli di accesso e competenza di ogni utente nell'ambito del singolo gruppo

9.6.2 Accesso al registro di protocollo per utenti interni alla AOO

L'autorizzazione all'accesso ai registri di protocollo è regolata tramite i seguenti strumenti:
L'accesso al registro di protocollo è regolamentato da una procedura di accesso tramite programma con login e password. In nessun altro modo è possibile accedere a tale registro.
La visibilità completa sul registro di protocollo è consentita solo al personale autorizzato secondo i criteri di sicurezza prima illustrati. In particolare ai soli utenti aventi un livello di sicurezza tale da poter avere la visibilità completa sul registro.
L'utente assegnatario dei documenti protocollati è invece abilitato sempre secondo i criteri di sicurezza sopra indicati, ad assegnare un numero di protocollo al documento e, se previsto, inviarlo in conservazione a norma. Può anche effettuare la scannerizzazione dello stesso se il documento giunge in forma cartacea.
A questo punto il documento continuerà il suo iter, completamente digitale ed automatizzato, secondo il flusso stabilito per la sua tipologia.
L'operatore che gestisce lo smistamento dei documenti può scannerizzare il documento se giunto in forma cartacea, scaricare la posta elettronica, marcare il documento secondo le regole tipologiche stabilite ed avviarlo al flusso al documento stesso assegnato. Può anche segnalare l'eventuale mancanza di una specifica tipologia di documento al RSP.
Nel caso in cui sia effettuata la registrazione di un documento sul protocollo particolare, la visibilità completa sul documento stesso è possibile solo all'utente abilitato alla gestione del registro particolare di protocollo, ad esempio il registro dei protocolli riservati.
Tutti gli altri utenti possono accedere solo ai dati di registrazione e visualizzazione del documento sempre in formato digitale, solo con determinate autorizzazioni l'utente può anche stampare o memorizzare il documento in oggetto.

9.6.3 Utenti esterni alla AOO – Altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 49.
Le AOO che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzano funzioni di accesso per ottenere le seguenti informazioni:
• numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
• identificazione dell'UU di appartenenza del RPA.

9.6.4 Utenti esterni alla AOO – Privati

Per l'esercizio del diritto di accesso ai documenti, sono possibili due alternative: l'accesso diretto per via telematica e l'accesso attraverso l'Ufficio Relazioni con il Pubblico (URP).
L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente, quali: firme elettroniche, firme digitali, Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE), sistemi di autenticazione riconosciuti dall'AOO.
L'accesso attraverso l'URP prevede che questo ufficio sia direttamente collegato con il sistema di protocollo informatico e di gestione documentale sulla base di apposite abilitazioni di sola consultazione concesse al personale addetto.
Se la consultazione avviene allo sportello, di fronte all'interessato, a tutela della riservatezza delle registrazioni di protocollo, l'addetto posiziona il video in modo da evitare la diffusione di informazioni di carattere personale.
Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

9.7 Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nella deliberazione CNIPA 19 febbraio 2004, n. 11.

9.7.1 Servizio archivistico

Il responsabile del sistema archivistico dell'AOO ha individuato nella sede centrale della scuola la sede dell'archivio dell'amministrazione.
Il responsabile del servizio in argomento ha effettuato la scelta a seguito della valutazione dei fattori di rischio che incombono sui documenti (ad es. rischi dovuti all'ambiente in cui si opera, rischi nelle attività di gestione, rischi dovuti a situazioni di emergenza) e del fatto che gli archivi fossero già presenti ed organizzati in tale sede.
Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha predisposto e reso noto, un piano individuando i soggetti incaricati di ciascuna fase.
Sono state pure regolamentate minutamente le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.
Il responsabile del servizio di gestione archivistica è a conoscenza, in ogni momento, della collocazione del materiale archivistico e ha predisposto degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.
Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalle regole tecniche vigenti, (ovvero altri formati non proprietari eventualmente di seguito indicati).

9.7.2 Servizio di conservazione a norma

Il responsabile della conservazione a norma dei documenti fornisce le disposizioni, in sintonia con il piano generale di sicurezza e con le linee guida tracciate dal RSP, per una corretta esecuzione delle operazioni di salvataggio dei dati su supporto informatico rimovibile.
Per l'archiviazione ottica dei documenti sono utilizzati i supporti di memorizzazione digitale che consentono registrazioni non modificabili nel tempo Questa Amministrazione ha scelto di avvalersi dei servizi della società Axios Italia come software e dei servizi della società 2C Solution come tenutari dello

spazio per l'archiviazione ottica a norma. Si fa inoltre presente che è stato verificato nell'elenco dell'AGID che la società 2C Solution è accreditata come CA.
Il responsabile della conservazione digitale:
• adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza dei supporti di memorizzazione, utilizzando gli strumenti tecnologici e le procedure descritte nelle precedenti sezioni;
• assicura il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti in caso di aggiornamento del sistema di conservazione;
• definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;
• verifica periodicamente, con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento del contenuto dei supporti.

9.7.3 Conservazione dei documenti informatici e delle registrazioni di protocollo

I luoghi di conservazione previsti per i supporti contenenti le registrazioni di protocollo e le registrazioni di sicurezza sono differenziati in base al livello di sicurezza loro attribuito: le registrazioni di protocollo cosi come le registrazioni del log di sicurezza sono entrambi presenti all'interno della base dati della scuola.
Il log delle operazioni effettuate viene esportato con cadenza mensile e conservato su supporti removibili da parte dell'RSP che provvede alla archiviazione di tali supporti in un luogo sicuro e distante dal server della scuola. Le registrazioni di protocollo invece, o meglio il registro delle stesse, viene conservato giornalmente in maniera a norma.

È compito dell'ufficio che si occupa del servizio di sicurezza del sistema informativo (Bassi Ferdinando, responsabile tecnico Easyteam.org SRL) l'espletamento delle seguenti procedure atte ad assicurare la corretta archiviazione, la disponibilità e la leggibilità dei supporti stessi.
L'archiviazione di ogni supporto viene registrata in un specifico file di cui è disponibile la consultazione per le seguenti informazioni:
• descrizione del contenuto;
• responsabile della conservazione;
• lista delle persone autorizzate all'accesso ai supporti, con l'indicazione dei compiti previsti;
• indicazione dell'ubicazione di eventuali copie di sicurezza;
• motivi e durata dell'archiviazione.
Tale tabella è stata creata come foglio Excel protetto da password a conoscenza solo dell'RSP e del responsabile AOO.
È stato implementato e viene mantenuto aggiornato un archivio dei prodotti software (nelle eventuali diverse versioni) necessari alla lettura dei supporti conservati con lo stesso sistema del precedente.
Presso il sistema informativo sono altresì mantenuti i sistemi con la configurazione hardware necessaria al corretto funzionamento del software.
Nell'archivio di cui al terzo capoverso del presente paragrafo, viene quindi indicato anche:
• il formato del supporto rimovibile;
• il prodotto software col quale è stato generato e la versione della release;
• la configurazione hardware e software necessaria per il suo riuso.
Deve essere inoltre indicata l'eventuale necessità di refresh periodico dei supporti, che questa AOO ha stabilito essere annuale. Annualmente quindi si farà una verifica di tali supporti decidendo, in base al loro stato, la necessità o meno di un refresh degli stessi.

Il personale addetto alla sicurezza del sistema informativo verifica la corretta funzionalità del sistema e dei programmi in gestione e l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento sostitutivo del contenuto su altri supporti.

9.7.4 Conservazione delle registrazioni di sicurezza

Un operatore addetto alla sicurezza dell'amministrazione/AOO, con periodicità settimanale, provvede alla memorizzazione su supporto non riscrivibile dei seguenti file di sicurezza: LOG di sistema.
Viene salvato su tali supporti sia l'esportazione del file di log delle operazioni svolte sul sistema e gestito dall'applicazione sia il file di log gestito dal database.
I supporti così realizzati sono conservati in Come previsto dal Dlgs 192/2003, conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e lontani da quelli in cui è installato il sistema di elaborazione di esercizio per un periodo minimo di cinque anni ove specifiche disposizioni di legge non ne prevedano la conservazione per un più lungo periodo.

9.7.5 Riutilizzo e dismissione dei supporti rimovibili

Non è previsto il riutilizzo dei supporti rimovibili. Al termine del previsto periodo di conservazione i supporti sono distrutti secondo una specifica procedura operativa.
Qualora però alcuni di questi, magari residui di vecchie procedure di salvataggio, debbano essere riutilizzati, questi vengono formattati a basso livello in modo tale da non consentire la lettura di vecchie informazioni prima memorizzate sui supporti stessi.

9.8 Politiche di sicurezza adottate dalla AOO

Le politiche di sicurezza, riportate nell'allegato 15.9 stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.
Le politiche illustrate sono corredate dalle procedure sanzionatorie che l'AOO intende adottare in caso di riscontrata violazione delle prescrizioni dettate in materia di sicurezza da parte di tutti gli utenti che, a qualunque titolo, interagiscono con il servizio di protocollo, gestione documentale ed archivistica.
È compito del RSP, assistito dal il DSGA Anita Talarico, procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza.
Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dal CNIPA o a seguito dei risultati delle attività di audit.
In ogni caso, tale attività è svolta almeno con cadenza annuale.

Allegato 9: Modalità di trattamento specifiche per documenti di tipologia particolare

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati nell'allegato 11.
Tale tipo di registrazione consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertoriazione.

Allegato 10 – Metadati particolari per documenti soggetti a registrazione particolare

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati nell'allegato 11.
Tale tipo di registrazione consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertoriazione.
Questi documenti costituiscono comunque delle serie di interesse archivistico, ciascuna delle quali deve essere corredata da un repertorio contenente le seguenti informazioni:
• dati identificativi di ciascun atto (persona fisica o giuridica che adotta il documento, data di adozione, oggetto, ….);
• numero di repertorio, un numero progressivo;
• dati di classificazione e di fascicolazione.

Allegato 11 - Elenco registrazioni particolari escluse dalla protocollazione

Sono escluse dalla protocollazione, ai sensi dell'art. 53. c. 5 del DPR n. 445/2000 le seguenti tipologie documentarie:

- Gazzette ufficiali, Bollettini ufficiali PA
- Notiziari PA
- Giornali, Riviste, Libri
- Materiali pubblicitari
- Note di ricezione circolari
- Note di ricezione altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Offerte o preventivi di terzi non richiesti
- Inviti a manifestazioni che non attivino procedimenti amministrativi
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a registrazione particolare (es. fatture, vaglia, assegni)
- Atti preparatori interni
- Certificazioni non meccanizzate
- Certificati di servizio personale docente di ruolo e non di ruolo
- Certificati di servizio personale tecnico amministrativo (a tempo determinato o indeterminato)
- Certificati situazioni retributive e contributive personale strutturato e non strutturato
- Certificazioni studenti
- Estratti conto bancario
- Report (o registro) delle presenze
- Visite fiscali (si protocollano solo quelle "sfavorevoli" al dipendente, ad es. per assenza)
- Cambio banca – comunicazioni
- Lettere di accompagnamento di fatture
- Progetti formativi e di orientamento – stage
- Richiesta conferma conseguimento titolo di studio
- Restituzioni dei buoni mensa da parte dei ristoratori o ditte convenzionate
- 730, 770, IRAP corrispondenza e modelli (come sopra)
- Avvisi di pagamento – comunicazioni di bonifici bancari

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto all'interno dell'Amministrazione/AOO un registro di protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati.
Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto.

Elenco dei documenti soggetti a registrazione particolare per tutte le amministrazioni

- Documenti relativi a vicende di persone o a fatti privati o particolari;
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare

il raggiungimento degli obbiettivi prefissati;

- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- I documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
- Corrispondenza legata a vicende di persone o a fatti privati o particolari;
- Le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241; dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

Allegato 12 - Elenco registri

- Registri di classe
- Registri dei docenti
- Registri dei contratti
- Registri delle determine
- Registri delle circolari
- Graduatorie

Allegato 13 - Manuale operativo software Protocollo

Il manuale operativo del software Protocollo WEB di Axios Italia è reperibile al link:

https://protocollo.axioscloud.it/Help/PRO_WEB_Manuale_Operativo.pdf

Di seguito sono elencate le funzionalità, le specifiche e le modalità operative.

1. Modalità di produzione e di conservazione delle registrazioni di protocollo informatico

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

1.1 Unicità del protocollo informatico

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica in base al modello organizzativo centralizzato adottato da questa Amministrazione/AOO.
La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.
Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.
Il numero di protocollo è costituito da almeno sette cifre numeriche.
Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.
Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.
La documentazione che non è stata registrata presso una UOP viene considerata giuridicamente inesistente presso l'amministrazione.
Non è consentita la protocollazione di un documento già protocollato.
Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.
Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

1.2 Registro giornaliero di protocollo

Il RSP provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. La produzione di tale registro viene effettuata in automatico dal sistema informatico di questa Amministrazione.
Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è inviato, al termine della giornata lavorativa, al supporto per la conservazione a norma al fine di garantirne la completa immodificabilità (2C Solution per questa

Amministrazione).
Questa operazione è eseguita dall'RSP.

1.3 Registrazione di protocollo

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).
Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.
Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.
Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:
• il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
• la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
• il mittente che ha prodotto il documento, registrato in forma non modificabile;
• il destinatario del documento, registrato in forma non modificabile;
• l'oggetto del documento, registrato in forma non modificabile;
• la classificazione.
Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.
Tali dati facoltativi sono descritti nei paragrafi seguenti.

1.3.1 Documenti informatici

I documenti informatici sono ricevuti e trasmessi in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'amministrazione.
La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma.
Nel caso di documenti informatici in partenza, l'operatore esegue anche la verifica della validità amministrativa della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto o inviato.
La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati.
I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.
Le UOP ricevono i documenti informatici interni di tipo formale da protocollare all'indirizzo di posta elettronica interno preposto a questa funzione o tramite il sistema di messaggistica interna utilizzato dall'applicazione gestita in questa Amministrazione.

1.3.1 Documenti analogici (cartacei e supporti rimovibili)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza, (il servizio postale pubblico e/o privato o con consegna diretta alla UOP).
La registrazione di protocollo di un documento analogico cartaceo ricevuto, così come illustrato nel

seguito, viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.
Nel caso di corrispondenza in uscita o interna formale, l'UOP esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

1.4 Elementi facoltativi delle registrazioni di protocollo

Il RSP, con proprio provvedimento e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può modificare e integrare gli elementi facoltativi del protocollo.
La registrazione degli elementi facoltativi del protocollo, con determinazione del RSP può essere modificata, integrata e cancellata in base alle effettive esigenze delle UOR o degli UOP.
I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.
Di seguito vengono riportati gli elementi facoltativi finalizzati alla conservazione e gestione della documentazione:

- ora e minuto di registrazione;
- luogo di provenienza o di destinazione del documento;
- tipo di documento;
- mezzo di ricezione/spedizione (ordinaria, espressa, corriere, raccomandata con ricevuta di ritorno, telefax, ecc.);
- collegamento a documenti precedenti e susseguenti;
- numero degli allegati;
- riferimenti agli allegati su supporto informatico;
- nominativo dei destinatari delle copie per conoscenza;
- UOR/UU competente;
- identificativo del RPA;
- termine di conclusione del procedimento amministrativo o di lavorazione del documento;
- indicazione del livello di sicurezza se diverso da quello standard applicato dal sistema di protocollazione;
- stato e tempi parziali delle procedure del procedimento amministrativo;
- classificazione del documento (titolo, categoria e fascicolo; eventuale sottofascicolo e inserto);
- data di istruzione del fascicolo;
- numero del fascicolo;
- numero del sottofascicolo;
- numero dell'inserto;
- data di chiusura del fascicolo;
- repertorio dei fascicoli;
- identificativo del fascicolo e/o del documento;
- numero di repertorio della serie (delibere, determinazioni, verbali, circolari e contratti);
- tipologia del documento con l'indicazione dei termini di conservazione e di scarto;
- scadenzario.

1.5 Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.
La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.
Essa consente di individuare ciascun documento in modo inequivocabile.

1.5.1 Documenti informatici

I dati della segnatura di protocollo di un documento informatico 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) reso disponibile dalla procedura software in dotazione a questa Amministrazione e comunque personalizzabile dall'utenza o direttamente dalla società Axios in base ad eventuali e sopraggiunte necessità anche per migliorare la fruibilità del prodotto.
Le informazioni minime incluse nella segnatura sono quelle di seguito elencate:
• codice identificativo dell'amministrazione;
• codice identificativo dell'area organizzativa omogenea;
• data e numero di protocollo del documento.
È facoltativo riportare anche le seguenti informazioni:
• denominazione dell'amministrazione;
• indice di classificazione;
• il codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
• numero di fascicolo.
Per i documenti informatici in partenza, possono essere specificate, in via facoltativa, anche le seguenti informazioni:
• persona o ufficio destinatario;
• identificazione degli allegati;
• informazioni sul procedimento e sul trattamento.
La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.
Quando il documento è indirizzato ad altre AOO la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.
L'AOO che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.
Qualora l'AOO decida di scambiare con altre AOO informazioni non previste tra quelle definite come facoltative, può estendere il file di cui sopra, nel rispetto delle regole tecniche dettate dal CNIPA, includendo le informazioni specifiche stabilite di comune accordo con l'AOO con cui interagisce.

1.5.2 Documenti cartacei

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un "segno" grafico sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:
• codice identificativo dell'amministrazione,
• codice identificativo dell'AOO;
• data e numero di protocollo del documento;
Facoltativamente possono essere riportate anche le seguenti informazioni:
• denominazione dell'amministrazione;
• indice di classificazione;
• il codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
• numero di fascicolo;
• ogni altra informazione utile o necessaria, se già disponibile al momento della registrazione di

protocollo.
Il “segno” grafico di norma è realizzato con una etichetta autoadesiva corredata di codice a barre o, in alternativa, con un timbro tradizionale.
L’AOO ha optato per il “segno” riportato nell’allegato 15.22.
L’operazione di segnatura dei documenti in partenza viene effettuata dall’UOR/UU/RPA competente che redige il documento se è abilitata, come UOP, alla protocollazione dei documenti in uscita; in alternativa l’operazione viene integralmente eseguita dalla UOP.
L’operazione di acquisizione dell’immagine dei documenti cartacei è eseguibile solo dopo che l’operazione di segnatura è stata eseguita, in modo da “acquisire” con l’operazione di scansione, come immagine, anche il “segno” sul documento.
Se è prevista l’acquisizione del documento cartaceo in formato immagine, il “segno” della segnatura di protocollo deve essere apposto sulla prima pagina dell’originale; in caso contrario il “segno” viene apposto sul retro della prima pagina dell’originale.

1.6 Annullamento delle registrazioni di protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrati in forma non modificabile - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l’interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l’obbligo di annullare l’intera registrazione di protocollo.
Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l’ora e l’autore dell’annullamento e gli estremi dell’autorizzazione all’annullamento del protocollo rilasciata dal RSP.
In tale ipotesi la procedura riporta la dicitura “annullato” in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l’avvenuta rettifica, la data ed il soggetto che è intervenuto.
Solo il RSP è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.
L’annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RSP.
A tal fine è istituito un registro (informatico o cartaceo) per le richieste di annullamento delle registrazioni e dei dati obbligatori delle registrazioni.
Il registro riporta i motivi dell’annullamento e, se il documento è stato protocollato nuovamente, il nuovo numero di protocollo assegnato.

1.7 Livello di riservatezza

L’operatore che effettua la registrazione di protocollo di un documento attribuisce allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal sistema.
In modo analogo, il RPA che effettua l’operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza.
Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti che invece hanno un livello di riservatezza superiore lo mantengono.

1.8 Casi particolari di registrazioni di protocollo

1.8.1 Registrazioni di protocollo particolari (riservate)

All'interno dell'AOO è istituito il protocollo riservato - sottratto alla consultazione da parte di chi non sia espressamente abilitato - nel quale sono riportati:
• documenti relativi a vicende di persone o a fatti privati o particolari;
• documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
• documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
• le tipologie di documenti individuati dalla normativa vigente richiamati nell'allegato 15.17.
La registrazione nel protocollo particolare, quando non sia palesemente evidente la necessità, può essere disposta dal RSP con l'apposizione, sul documento, della seguente dicitura: "Da registrare sul protocollo particolare".
I documenti (informatici o cartacei) anonimi, come tali individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale, vengono inviati al RSP che ne effettua una valutazione:
• se ritiene che contengano dati o informazioni di interesse dell'amministrazione/AOO, provvede ad inviarli agli uffici competenti per le ulteriori eventuali determinazioni. Questi decidono se registrarli, farli registrare nel protocollo generale;
• se ritiene che non contengano dati rilevanti dal punto di vista amministrativo, il documento viene registrato nel protocollo particolare.

1.8.2 Circolari e disposizioni generali

Le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale.
I destinatari sono indicati in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo secondo le modalità previste dalla gestione anagrafica del sistema.

1.8.3 Documenti cartacei in partenza con più destinatari

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica e viene riportata solo sul documento originale con la dicitura "Questa registrazione di protocollo viene riportata sui documenti degli altri destinatari - Vedi elenco allegato alla minuta/copia presso l'UOR/UU/RPA.
Tale elenco, in formato cartaceo, viene allegato alla minuta dell'originale.

1.8.4 Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma inoltrati al servizio protocollo come documenti senza firma, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

1.8.5 Documenti cartacei ricevuti a mezzo telefax

Il documento ricevuto a mezzo telefax è un documento analogico a tutti gli effetti.
Il documento trasmesso da chiunque ad una pubblica AOO tramite telefax, qualora ne venga accertata la fonte di provenienza, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale.

L'accertamento della fonte di provenienza spetta al RPA e avviene, di norma, per le vie brevi o con l'uso di sistemi informatici.
Qualora non sia possibile accertare la fonte di provenienza, sul telefax viene apposta la dicitura "Documento ricevuto via telefax" e successivamente il RPA provvede ad acquisire l'originale.
Nel caso che al telefax faccia seguito l'originale, poiché ogni documento viene individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione, l'addetto alla registrazione a protocollo, dopo aver registrato il telefax, deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax ed apporre la seguente dicitura: "Già pervenuto via fax il giorno…".
Il RSP accerta comunque che si tratta del medesimo documento ricevuto via fax: qualora dovesse riscontrare una differenza, anche minima, deve procedere alla registrazione con un nuovo numero di protocollo in quanto si tratta di un documento diverso.
Il fax ricevuto con un terminale telefax dedicato (diverso da un PC) è fotocopiato dal ricevente qualora il supporto cartaceo non fornisca garanzie per una corretta e duratura conservazione.
Su di esso o sulla sua foto-riproduzione va apposta, a cura del ricevente, la dicitura "Documento ricevuto via telefax".
Il documento in partenza reca una delle seguenti diciture:
• "Anticipato via telefax" se il documento originale viene successivamente inviato al destinatario;
• "La trasmissione via fax del presente documento non prevede l'invio del documento originale» nel caso in cui l'originale non venga spedito. Il RPA è comunque tenuto a spedire l'originale qualora il destinatario ne faccia motivata richiesta;
La segnatura viene apposta sul documento e non sulla copertina di trasmissione.
La copertina del telefax ed il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.
Il fax ricevuto direttamente su una postazione di lavoro (esempio un PC con l'applicativo per invio e ricezione di fax) è la rappresentazione informatica di un documento che può essere, sia stampato e trattato come un fax convenzionale come è stato descritto nei paragrafi precedenti, sia visualizzato e trattato interamente con tecniche informatiche.
In questo secondo caso il "file" rappresentativo del fax, viene inviato al protocollo generale, per essere sottoposto alle operazioni di protocollazione e segnatura secondo gli standard XML vigenti e poi, trattato secondo le regole precedentemente specificate per la gestione dei documenti informatici.

1.8.6 Protocollazione di un numero consistente di documenti cartacei

Quando si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso (es. scadenza gare o concorsi) che in uscita, deve esserne data comunicazione all'ufficio protocollo con almeno due giorni lavorativi di anticipo, onde concordare tempi e modi di protocollazione e di spedizione.

1.8.7 Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio

La corrispondenza ricevuta con rimessa diretta dall'interessato o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.
Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta.
Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, essi saranno accantonati e protocollati successivamente (come di seguito descritto). In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli

estremi del protocollo.

1.8.8 Fatture, assegni ed altri valori di debito o credito

Le buste contenenti fatture, assegni o altri valori di debito o credito sono immediatamente separate dall'altra posta in arrivo, protocollate su un registro diverso da quello generale e inviate quotidianamente all'UOR competente.

1.8.9 Protocollazione di documenti inerenti a gare di appalto confezionati su supporti cartacei

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo" o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata all'UOR competente.
È compito dello stesso UOR provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi idonei, sino all'espletamento della gara stessa.
Dopo l'apertura delle buste l'UOR che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.
Per motivi organizzativi tutti gli UOR sono tenuti ad informare preventivamente il RSP dell'amministrazione in merito alle scadenze di concorsi, gare, bandi di ogni genere.

1.8.10 Protocolli urgenti

La richiesta di protocollare urgentemente un documento è collegata ad una necessità indifferibile e di tipo straordinario.
Solo in questo caso il RSP si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale o cartaceo da spedire.
Tale procedura viene osservata sia per i documenti in arrivo che per quelli in partenza, raccomandando, per questi ultimi, che non devono essere protocollati anticipatamente documenti diversi dall'originale (ad esempio bozze del documento), fatti pervenire all'UOP.

1.8.11 Documenti non firmati

L'operatore di protocollo, conformandosi alle regole stabilite dal RSP attesta la data, la forma e la provenienza per ogni documento.
Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "Mittente sconosciuto o anonimo" e "Documento non sottoscritto".
Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.
È poi compito dell'UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

1.8.12 Protocollazione dei messaggi di posta elettronica convenzionale

Considerato che l'attuale sistema di posta elettronica non certificata non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata nei seguenti modi:
• in caso di invio, come allegato, di un documento scansionato e munito di firma autografa, quest'ultimo

è trattato come un documento inviato via fax fermo restando che l'RPA deve verificare la provenienza certa dal documento; in caso di mittente non verificabile, l'RPA valuta caso per caso l'opportunità di trattare il documento inviato via e-mail;
• in caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale, il documento e/o il messaggio sono considerati come un documento elettronico inviato con qualunque mezzo di posta;
• in caso di invio di una e-mail contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

1.8.13 Protocollo di documenti digitali pervenuti erroneamente

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all'amministrazione non competente, l'addetto al protocollo provvede o ad annullare il protocollo stesso o provvede a protocollare il documento in uscita indicando nell'oggetto "protocollato per errore" e rispedisce il messaggio al mittente.

1.8.14 Ricezione di documenti cartacei pervenuti erroneamente

Nel caso in cui sia protocollato un documento cartaceo erroneamente inviato all'amministrazione, l'addetto al protocollo provvede o ad annullare il protocollo stesso o provvede a protocollare il documento in uscita indicando nell'oggetto "protocollato per errore"; il documento oggetto della rettifica viene restituito al mittente con la dicitura "protocollato per errore".

1.8.15 Copie per conoscenza

Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nel paragrafo 1.8.3. In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, inserisce nel registro di protocollo i nominativi di coloro ai quali sono state inviate le suddette copie per conoscenza.
Tale informazione è riportata anche sulla segnatura di protocollo.

1.8.16 Differimento delle registrazioni

Le registrazioni di protocollo dei documenti pervenuti presso l'amministrazione destinataria sono effettuate nella giornata di arrivo e comunque non oltre le 48 ore dal ricevimento di detti documenti.
Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del RSP, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.
Il protocollo differito consiste nel differimento dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento sopra citato.

1.8.17 Registrazioni di documenti temporaneamente riservati

Quando si è in presenza di documenti che per la loro natura richiedono una temporanea riservatezza delle informazioni in essi contenute (ad esempio gare e appalti, verbali di concorso, etc.), è prevista una forma di accesso riservato al protocollo generale.
Il responsabile dell'immissione dei dati provvede alla registrazione di protocollo indicando contestualmente l'anno, il mese e il giorno, nel quale le informazioni temporaneamente riservate

saranno accessibili nelle forme ordinarie.

1.8.18 Corrispondenza personale o riservata

La corrispondenza personale è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale".
In quest'ultimo caso, la corrispondenza con la dicitura "riservata" o "personale" non è aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli al più vicino ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

1.8.19 Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.
Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.
I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel fascicolo relativo.

1.9 Gestione delle registrazioni di protocollo con il PDP

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono effettuate attraverso il PdP.
Il sistema di sicurezza adottato dall'AOO garantisce la protezione di tali informazioni sulla base dell'architettura del sistema informativo, sui controlli d'accesso e sui livelli di autorizzazione previsti.

1.10 Registrazioni di protocollo

1.10.1 Attribuzione del protocollo

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il servizio di protocollo è realizzato dall'applicativo PdP attraverso l'apposizione di un riferimento temporale come previsto dalla normativa vigente.
Il sistema informativo assicura in tal modo la precisione del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.
• Come previsto dalla normativa in materia di tutela dei dati personali, gli addetti al protocollo adottano tutti gli accorgimenti necessari per la tutela dei dati sensibili. E giudiziari non inserendoli nel campo "oggetto" del registro di protocollo.

1.10.2 Registro informatico di protocollo

Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo generale della AOO si provvede, in fase di chiusura dell'attività di protocollo, ad effettuare le seguenti operazioni:
• estrazione delle registrazioni del giorno corrente (o precedente) dal file del registro generale di

protocollo;
• applicazione della firma digitale e di un riferimento temporale al file così realizzato;
• copia del file estratto, del file di firma e del riferimento temporale su supporto rimovibile non riscrivibile;
• salvataggio del file di firma e del riferimento temporale sul sistema di esercizio del PdP.
L'ufficio o l'addetto incaricato di eseguire l'operazione di riversamento dei file in parola su due supporti rimovibili non riscrivibili è stato individuato nel RSP o in chi da lui delegato.
L'uso combinato dei meccanismi permette di conferire validità e integrità ai contenuti del file del registro di protocollo (Le copie giornaliere generali di backup dell'intero sistema informativo dell'amministrazione/AOO esulano dai meccanismi di sicurezza qui richiamati).
È inoltre disponibile, all'occorrenza, per i gestori del PdP una funzione applicativa di "stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.
Al termine delle operazioni giornaliere o, comunque entro il giorno successivo sono effettuate le seguenti operazioni di garanzia:
• Invio in conservazione a norma del registro di protocollo giornaliero

1.10.3 Tenuta delle copie del registro di protocollo

È compito del responsabile della conservazione dei documenti provvedere alla verifica del contenuto dei supporti prodotti dall'ufficio o dall'addetto incaricato.
Una copia dei supporti è conservata nei supporti di backup in dotazione del responsabile della AOO, mentre la seconda copia è custodita nel relativo servizio cloud acquistato appositamente e che consente anche la completa gestione del dystaster recovery.
Le modalità di gestione di tali supporti sono definite e regolamentate direttamente dal RSP dell'AOO.
I dati contenuti su tali supporti sono conservati con le modalità previste dalla normativa vigente.
Procedendo alle operazioni di riversamento con la periodicità prevista dalla deliberazione CNIPA n. 11/2004.

2. Descrizione funzionale ed operativa del sistema di protocollo informatico

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'amministrazione con particolare riferimento alle modalità di utilizzo dello stesso.

2.1 Descrizione funzionale ed operativa

L'area Protocollo è lo strumento che permette di registrare, assegnando un numero identificativo e la classificazione in un titolario, la posta in entrata e in uscita della segreteria scolastica.
Permette quindi di gestire il Registro di Protocollo composto da: Registro Giornaliero Protocollo, Registro protocollo Riservato e dal registro di Emergenza.
La gestione del Protocollo permette la gestione dei mittenti e destinatari collegata ad un archivio interno, prevede la gestione di allegati digitali con possibilità di pubblicazione in Albo on-line e in Amministrazione trasparente. Prevede inoltre un Registro di Istruttoria Protocollo e la possibilità di inviare il Registro Protocollo Giornaliero in conservazione a norma.
All'interno dell'area protocollo sono presenti varie funzioni per effettuare le stampe dei vari registri

Le modalità operative perché quest'ultime sono trattate dettagliatamente nel Manuale utente del PdP.
Il manuale utente operativo è disponibile direttamente da programma tramite il tasto F1.
Tale tasto consente l'accesso all'help on line che, pur essendo organizzato come un vero e proprio

manuale, si posiziona direttamente sulla pagina di argomento di contesto.
E' inoltre possibile accedere, sempre direttamente tramite programma, ad un archivio di FAQ con motore di ricerca integrato.

Allegato 14 – Procedure per la gestione del registro di emergenza

1. Modalità di utilizzo del registro di emergenza

Il presente documento illustra le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente, prevista dal PdP.

1.1 Il registro di emergenza

Qualora non fosse disponibile fruire del PdP per una interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza.
Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.
Qualora nel corso di un anno non venga utilizzato il registro di emergenza, il RSP annota sullo stesso il mancato uso.
Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite su registro di protocollo generale.
Il registro di emergenza si configura come un repertorio del protocollo generale.
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

1.2 Modalità di apertura del registro di emergenza

Il RSP assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica, le operazioni di protocollo sono svolte manualmente sul registro di emergenza, sia esso cartaceo o informatico, su postazioni di lavoro operanti fuori linea.
Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il RSP imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare.
Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.
Per semplificare e normalizzare la procedura di apertura del registro di emergenza il RSP ha predisposto il modulo (cartaceo o digitale) riportato di seguito.
L'elenco delle UOP abilitate alla registrazione dei documenti sui registri di emergenza è riportato nell'allegato 15.3.

1.3 Modalità di utilizzo del registro di emergenza

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro il numero totale di

operazioni registrate manualmente.
La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.
Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono quelli stessi previsti dal protocollo generale.
Durante il periodo di interruzione del servizio di protocollo informatico generale, il responsabile del sistema informatico (o persona da lui delegata) provvede a tener informato il RSP sui tempi di ripristino del servizio.

Servizio di gestione informatica del protocollo, dei documenti e degli archivi

Scheda di apertura/chiusura del registro di emergenza
< Identificativo dell'amministrazione >
< Identificativo dell'AOO >
< Identificativo della UOP abilitata >
Causa dell'interruzione: . . . . . .
Data: gg / mm / aaaa di inizio/ fine interruzione
(Depennare la voce incongruente con l'evento annotato)
Ora dell'evento hh /mm
Annotazioni: . . . .
Numero protocollo xxxxxxx iniziale/finale
(Depennare la voce incongruente con l'evento annotato)
Pagina n. . . . . .
Firma del responsabile del servizio di protocollo

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

1.4 Modalità di chiusura e recupero del registro di emergenza

È compito del RSP verificare la chiusura del registro di emergenza.
È compito del RSP, o suo delegato, riportare dal registro di emergenza al sistema di protocollo generale (PdP) le protocollazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.
Una volta ripristinata la piena funzionalità del PdP, il RSP provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.
Per semplificare la procedura di chiusura del registro di emergenza il RSP ha predisposto un modulo (cartaceo o digitale) analogo a quello utilizzato nella fase di apertura del registro di emergenza.

Allegato 15 – Linee guida per la pubblicazione in Albo On Line

Le linee guida per la pubblicazione in Albo on Line adottate da questa amministrazione rispecchiano quelle pubblicate dall'AGID:

http://www.agid.gov.it/sites/default/files/documentazione/ll_gg_gdl_pubblicita_legale.pdf

Allegato 16 - Elenco documenti trasmessi direttamente ai database centrali di altri enti

- DURC
- denunce di infortunio
- contratti
- certificati di malattia
- elenchi alunni
- risultati scrutini alunni
- fatture
- indici di tempestività dei pagamenti
- documenti trattati tramite applicativo Desktop Telematico Agenzia delle Entrate

Allegato 17 - Piano per la continuità operativa

Piano della continuità operativa ICT
Procedure di disaster recovery

Registro delle modifiche		
Versione	**Data**	**Descrizione**
1.0	24/07/2017	Versione iniziale

Piano di continuità operativa ICT

L' art. 15 "Digitalizzazione e riorganizzazione" del CAD sancisce che gli uffici pubblici devono essere organizzati in modo che sia garantita la digitalizzazione dei servizi.
La Pubblica Amministrazione, e quindi il nostro Istituto, ha l'obbligo di assicurare la continuità dei processi che presiedono alla erogazione dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese.
L'utilizzo delle tecnologie ICT nella gestione dei dati e dei procedimenti dei singoli enti, che rende necessario adottare tutte le iniziative tese a salvaguardare l'integrità, la disponibilità, la continuità nella fruibilità dei dati.
Le Pubbliche Amministrazioni devono predisporre appositi piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire i servizi e il ritorno alla normale operatività.

Destinatari

Destinatari del Piano di Continuità Operativa ICT sono:

- il Dirigente Scolastico;
- il DSGA;
- il responsabile della continuità operativa ICT, così come indicato nelle "Linee guida per il DR delle PA" emesso dall'Agenzia per l'Italia Digitale il 26 novembre 2011, individuato nelnresponsabile dei sistemi informativi dell'Istituto;
- il personale amministrativo dell'Istituto (la segreteria);
- la comunità di riferimento territoriale e sociale (famiglie e imprese) dell'Amministrazione;
- le organizzazioni e/o istituzioni che interagiscono con l'Amministrazione in modalità informatiche.

Piano dei Sistemi

Il nostro Istituto deve rispondere in maniera efficiente ad una situazione di emergenza analizzando:

1. i possibili livelli di disastro
2. la criticità dei sistemi/applicazioni.

Per una corretta applicazione del piano, i sistemi devono essere classificati secondo le seguenti definizioni:

- Critici: Le relative funzioni non possono essere eseguite senza essere sostituite da strumenti (mezzi) di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa.
- Vitali: Le relative funzioni possono essere svolte manualmente, ma solo per un breve periodo dintempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici, e queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).
- Delicati: Queste funzioni possono essere svolte manualmente, per un lungo periodo di tempo. Benché queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.
- Non-critici: Le relative funzioni possono rimanere interrotte per un lungo periodo di tempo, e si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.

Punti critici e vitali dell'Istituto

Nel nostro istituto identifichiamo i punti critici e vitali:

- Il server AXIOS che gestisce i dati utilizzati dalla segreteria, composto da un server situato negli uffici di segreteria, protetto in un armadio rack chiuso a chiave.
- Il firewall situato nello stesso armadio rack del server, che permette di proteggere gli accessi indesiderati possibili minacce.
- I dispositivi di backup individuati dall'Istituto in un disco NAS di rete e in un servizio di backup via Cloud.

Un piano d'emergenza deve valutare le strategie di ripristino più opportune su: siti alternativi, metodi di back up, sostituzione dei ruoli e responsabilità dei gruppi degli operatori.

Prevenzione dei danni

Si illustrano alcune precauzioni e indicazioni di massima adottate dal nostro Istituto per prepararci ad un disastro e limitarne o prevenirne i danni:

- Backup dei dati. E' la condizione minima indispensabile: tutti i dati importanti vanno salvati su altri dispositivi. Il mezzo su cui viene mantenuto il backup dovrebbe essere custodito in un luogo ed edificio fisicamente distante. Vengono effettuati test di ripristino e di verifica dell'integrità dei dati a cadenza regolare, insieme ad una attenta analisi di quali dati vengono effettivamente copiati e se questi sono tutti i dati da copiare.
- Protezione dei sistemi da accessi indesiderati o furti. Utilizzo di rack protetti da chiusure e chiavi di sicurezza per rendere inaccessibili il server della segreteria.

- Impianto elettrico a norma, che offra inoltre sufficiente protezione da fulmini, con gruppi di continuità che suppliscano a brevi interruzioni di elettricità ed eventualmente generatori per far fronte a prolungati black-out.
- UPS. Unità di energia supplementare per ovviare a situazioni di mancanza di energia elettrica per permettere di portare in sicurezza i dati dell'Istituto e al limite chiudere il sistema.

Tecniche di Disaster Recovery

Sistemi e dati considerati importanti vengono ridondati in un sito secondario per far sì che, in caso di disastro (terremoto, inondazione, incendio, attacco haker, ecc...) di intensità che sia tale da rendere inutilizzabili i sistemi informativi del sito primario, sia possibile attivare le attività di recupero dati sul sito secondario al più presto e con la minima perdita di dati possibile.

Il nostro Istituto utilizza una tecnica di ridondanza attraverso un sistema via CLOUD i dati che sono il risultato dalla tecnica di backup impostata. Con questa modalità di duplicazione, anche nel caso di disastro, i dati non essendo "in loco" sono sempre disponibili al ripristino.

Sicurezza Informatica

Si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce e della successiva protezione dell'integrità logico-funzionale di un sistema informatico e dei dati in esso contenuti. Tale protezione è ottenuta attraverso misure di carattere organizzativo e tecnologico tese ad assicurarne l'accesso solo ad utenti registrati (autenticazione) la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (permessi), l'oscuramento (cifratura) e la correttezza (integrità) dei dati scambiati in una comunicazione nonché la protezione del sistema da attacchi di software pericolosi.

La sicurezza informatica è un problema sempre più sentito in ambito tecnico-informatico per via della sempre più spinta informatizzazione della società e dei servizi in termini di apparati e sistemi informatici e della parallela diffusione e specializzazione degli attaccanti o hacker. L'interesse per la sicurezza dei sistemi informatici è dunque cresciuto negli ultimi anni proporzionalmente alla loro diffusione ed al loro ruolo occupato nella collettività.

Risulta evidente che per capire le strategie migliori di sicurezza informatica sia necessario entrare nella mentalità dell'attaccante per poterne prevedere ed ostacolarne le mosse.

Perdita dei dati

Le cause di probabile perdita di dati nei sistemi informatici possono essere molteplici, ma in genere le possiamo raggruppare in due eventi:

1. Eventi indesiderati: sono da considerarsi indesiderati gli eventi per lo più inaspettati come:
    a. gli attacchi Hacking che vengono fatti tramite la rete internet, da parte di utenti che si intrufolano abusivamente all'interno del sistema riuscendo ad ottenere piena disponibilità della macchina per gestire risorse e dati senza avere i giusti requisiti richiesti, ma tramite software costruiti da loro stessi.
    b. Gli accessi a sistemi da parte di utenti non autorizzati che, a differenza di un attacco cracker, utilizzano direttamente le macchine locali, forzandone le difese e le protezioni.
2. Eventi accidentali, ovvero danni causati accidentalmente dall'utente stesso, tipo: uso difforme dal consigliato di un qualche sistema, guasti imprevisti, ecc…

Alcune indicazioni attuate dal nostro Istituto per garantire la sicurezza e l'integrità dei dati:

1. Il server di AXIOS è collegato ad un gruppo di continuità che consente di escludere la perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica.

2. L'integrità dei dati sul server amministrativo di AXIOS è garantita da una procedura di backup che avviene giornalmente in orario notturno, attraverso un'unità NAS di backup di rete.
3. Tutti i PC della rete amministrativa vengono protetti da password per impedire al personale non autorizzato l'accesso alla rete. Le password sono gestite centralmente da una struttura Active Directory installata sul server amministrativo AXIOS e rispondono ai requisiti di legge contenuti nell'allegato tecnico del D.lgs 196/2003.
4. Tutti i PC della rete amministrativa sottostanno a alcune policies di rete, controllate centralmente dal server amministrativo AXIOS, che:
    a. Impediscono l'autorun di dispositivi removibili USB al fine di minimizzare i rischi di infezione da virus
    b. Impediscono la modifica di alcune impostazioni di sistema dei client (indirizzo IP, DNS, configurazione di rete, condivisioni, comportamento predefinito di programmi)

Tipi di sicurezza

Tipologie di sicurezza attuabili:

1. Sicurezza passiva: sono le tecniche e gli strumenti di tipo difensivo, ossia quel complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata. Il concetto di sicurezza passiva pertanto è molto generale: ad esempio, per l'accesso a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.
2. Sicurezza attiva: sono tutte quelle tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (riservatezza) sia dalla possibilità che un utente non autorizzato possa modificarli (integrità).

È evidente che la sicurezza passiva e quella attiva siano tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza di un sistema.
Il nostro Istituto utilizza meccanismi di sicurezza passiva (rack chiusi a chiave) e attiva (firewall) atte a incrementare il livello di sicurezza.

Altri strumenti di protezione applicati nel nostro Istituto

- Antivirus: consente di proteggere il proprio computer da software dannosi conosciuti come virus. Un buon antivirus deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente deve avviare con regolarità la scansione dei dispositivi del PC per verificare la presenza di virus e per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'antivirus correttamente configurato a tale scopo. Per maggiori garanzie di funzionamento il nostro Istituto ha optato per un antivirus amministrabile centralmente dall'amministratore di rete, che imposta policies e regole da distribuire poi a tutti i client della rete,
- Antispyware: software facilmente reperibile sul web in versione freeware, shareware o a pagamento. È diventato utilissimo per la rimozione di "file spia", gli spyware appunto, in grado di carpire informazioni riguardanti le attività on line dell'utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.

- Firewall: garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente.
- Firma digitale e crittografia: la firma digitale, e l'utilizzo di certificati digitali e crittografia per identificare l'autorità di certificazione, un sito, un soggetto o un software. Nel nostro Istituto si procede all'archiviazione digitale dei documenti in formato p7m e si indica all'utente la modalità di verifica della firma del dirigente Scolastico tramite l'utilizzo del software infocert. Aprire un file p7m (se pdf) con Adobe reader è possibile ma non offre la garanzia di verifica dell'identità di appartenenza.

Gestione e aggiornamento del piano di continuità operativa

Il piano della continuità operativa ICT non è un documento statico e, pertanto, è necessario pianificare, sia le modalità di verifica dei contenuti (test), sia le modalità di revisione e aggiornamento.

Per quanto attiene ai test, sono possibili varie modalità di test:

- una semplice verifica dell'effettiva disponibilità di tutto quanto si renderebbe necessario in caso di emergenza (nomina responsabile della continuità operativa, nomina Comitato di crisi ICT, gestione delle reperibilità, disponibilità e funzionamento degli impianti del sito secondario, disponibilità delle risorse elaborative e di rete, ecc.).
- un test cosiddetto "walkthrough": questo tipo di test si svolge con una simulazione (cioè, senza attivazione fisica dei sistemi) fatta da tutto il personale da coinvolgere previsto dal piano della continuità operativa ICT.
- test degli impianti e delle risorse: in questo caso non solo le procedure, ma anche l'effettiva attivazione delle risorse fisiche e IT viene verificata, sempre a fronte della simulazione di un'emergenza. Un test di questo tipo richiede una attenta predisposizione e un sensibile impegno per il personale, ma garantisce la reale verifica della soluzione di continuità del piano della continuità operativa ICT.

Allegato 18 – Manuale di conservazione

1.1 Protezione e conservazione degli archivi pubblici

1.1.1 Generalità

Il presente manuale riporta il sistema di classificazione dei documenti, di formazione del fascicolo e di conservazione dell'archivio, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto della documentazione, anche con riferimento all'uso di supporti sostitutivi e di consultazione e movimentazione dei fascicoli.
La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (titolario), cioè di quello che si suole definire "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti".
Il piano di conservazione, collegato con il titolario ed elaborato tenendo conto dei flussi documentali dipendenti dai procedimenti e dalle prassi seguiti dall'AOO nell'espletamento delle funzioni istituzionali, definisce i tempi di conservazione dei documenti e dei fascicoli nella sezione di deposito dell'archivio.
Il titolario e il piano di conservazione sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di protocollazione informatica e di archiviazione, considerato che si tratta degli strumenti che consentono la corretta formazione, gestione e archiviazione della documentazione dell'amministrazione. Spetta ai vertici dell'amministrazione medesima adottare il titolario e il piano di conservazione con atti formali.

1.1.2 Misure di protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti degli enti pubblici non territoriali sono beni culturali inalienabili.
I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'AOO, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.
L'archivio non può essere smembrato, a qualsiasi titolo, e deve essere conservato nella sua organicità.
Il trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della direzione generale per gli archivi.
L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della direzione generale per gli archivi.
Lo scarto dei documenti degli archivi delle amministrazioni/AOO statali è subordinato all'autorizzazione della direzione generale per gli archivi, su proposta delle commissioni di sorveglianza istituite presso ciascun ufficio con competenza corrispondente alla provincia o delle commissioni di scarto istituite presso ogni ufficio con competenza sub provinciale. Per gli enti pubblici non statali la competenza è delegata alla soprintendenza archivistica competente per territorio.
Per l'archiviazione e la custodia nella sezione di deposito o storica dei documenti contenenti dati personali, si applicano in ogni caso le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che convenzionali.

1.2 Titolario o piano di classificazione

1.2.1 Titolario

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.
Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello, etc.
Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.
Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito della funzione di governo dell'amministrazione.
Il titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali e/o regionali.
L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RSP. La revisione anche parziale del titolario viene proposta dal RSP quando è necessario ed opportuno.
Dopo ogni modifica del titolario, il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.
Il titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.
Viene garantita la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.
Per ogni modifica di una voce viene riportata la data di introduzione e la data di variazione.
Di norma le variazioni vengono introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo titolario e valgono almeno per l'intero anno.
Rimane possibile, se il sistema lo consente, registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.
Il titolario è elaborato da un gruppo di lavoro appositamente costituito all'interno dell'amministrazione/AOO e approvato dai competenti organi dell'amministrazione archivistica statale.

1.2.2 Classificazione dei documenti

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.
Essa è eseguita a partire dal titolario di classificazione facente parte del piano di conservazione dell'archivio. Tutti i documenti ricevuti e prodotti dagli UOR dell'AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario.
Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse, etc.), il numero del fascicolo ed eventualmente del sottofascicolo.

1.3 Fascicoli e dossier

1.3.1 Fascicolazione dei documenti

Tutti i documenti registrati nel sistema informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.
Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento.
I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza, sottofascicolo o inserto, secondo l'ordine cronologico di registrazione.

Il software in uso presso questa Amministrazione consente di legare un singolo documento anche a diversi fascicoli, ovviamente in modo logico, senza duplicazione delle informazioni all'interno della base dati.
L'assegnazione ad altri fascicoli, oltre al fascicolo padre, può avvenire anche in momenti diversi.

1.3.2 Apertura del fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'ente, il soggetto preposto (quale, ad esempio, RPA, RSP, responsabile del servizio archivistico addetto alla protocollazione, etc.) provvede all'apertura di un nuovo fascicolo.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

- indice di classificazione, (cioè titolo, classe, sottoclasse, etc.);
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'amministrazione/ AOO;
- data di apertura del fascicolo;
- AOO e UOR;
- collocazione fisica, di eventuali documenti cartacei;
- collocazione logica, dei documenti informatici;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario.
Le informazioni di cui sopra, compaiono sulla camicia del fascicolo.

1.3.3 Chiusura del fascicolo

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto.
Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.
Gli elementi che individuano un fascicolo sono gestiti dal soggetto di cui al paragrafo 1.3.2, primo capoverso, il quale è tenuto anche all'aggiornamento del repertorio dei fascicoli.

1.3.4 Processo di assegnazione dei fascicoli

Quando un nuovo documento viene recapitato all'amministrazione, l'UOR abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso debba essere ricollegato ad un affare o procedimento in corso, e pertanto debba essere inserito in un fascicolo già esistente, oppure se il documento si riferisce a un nuovo affare o procedimento per cui è necessario aprire un nuovo fascicolo.
A seconda delle ipotesi, si procede come segue:

Se il documento si ricollega ad un affare o procedimento in corso, l'addetto:

- seleziona il relativo fascicolo;
- collega la registrazione di protocollo del documento al fascicolo selezionato;
- invia il documento all'UOR cui è assegnata la pratica. (Se si tratta di un documento su supporto cartaceo, assicura l'inserimento fisico dello stesso nel relativo fascicolo).

Se il documento dà avvio ad un nuovo fascicolo, il soggetto preposto:

- esegue l'operazione di apertura del fascicolo;
- collega la registrazione di protocollo del documento al nuovo fascicolo aperto;
- assegna il documento ad un istruttore su indicazione del responsabile del procedimento;
- invia il documento con il relativo fascicolo al dipendente che dovrà istruire la pratica per competenza.

1.3.5 Modifica delle assegnazioni dei fascicoli

Quando si verifica un errore nella assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede (vedi soggetto di cui al paragrafo 1.3.2) a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'UOR di competenza.
Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore di UU che effettua la modifica con la data e l'ora dell'operazione.

1.3.6 Repertorio dei fascicoli

I fascicoli sono annotati nel repertorio dei fascicoli.
Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli.
La struttura del repertorio rispecchia quella del titolario di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo.
Mentre il titolario rappresenta in astratto le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività.
Nel repertorio sono indicati:

- la data di apertura;
- l'indice di classificazione completo (titolo, classe, sottoclasse, etc.);
- il numero di fascicolo (ed altre eventuali partizioni in sottofascicoli e inserti);
- la data di chiusura;
- l'oggetto del fascicolo (ed eventualmente l'oggetto dei sottofascicoli e inserti);
- l'annotazione sullo status relativo al fascicolo, se cioè sia ancora una "pratica" corrente, o se abbia esaurito la valenza amministrativa immediata e sia quindi da mandare in deposito, oppure, infine, se sia da scartare o da passare all'archivio storico;
- l'annotazione sullo stato della pratica a cui il fascicolo si riferisce (pratica in corso da inserire nell'archivio corrente, pratica chiusa da inviare all'archivio di deposito, pratica chiusa da inviare all'archivio storico o da scartare).

Il repertorio dei fascicoli è costantemente aggiornato in automatico del sistema software in uso presso questa Amministrazione.

1.3.7 Apertura del dossier

La formazione di un nuovo dossier avviene attraverso l'operazione di "apertura" che prevede l'inserimento delle seguenti informazioni essenziali:

- il numero del dossier;
- la data di creazione;
- il responsabile del dossier;
- la descrizione o oggetto del dossier;

- la sigla della AOO e dell'UOR;
- l'elenco dei fascicoli contenuti;
- il livello di riservatezza del dossier (viene, di norma, assegnato dal livello di riservatezza del fascicolo a più alto livello di riservatezza).

1.3.8 Repertorio dei dossier

I dossier, di norma, sono annotati nel repertorio dei dossier.
Il repertorio dei dossier è lo strumento di gestione e reperimento dei dossier. Nel repertorio sono indicati:

- il numero del dossier;
- la data di creazione;
- la descrizione o oggetto del dossier;
- il responsabile del dossier.

Il repertorio dei dossier è costantemente aggiornato in automatico del sistema software in uso presso questa Amministrazione.

1.4 Serie archivistiche e repertori

1.4.1 Serie archivistiche

La serie archivistica consiste in un raggruppamento di unità archivistiche (documenti, fascicoli, registri) riunite o per caratteristiche omogenee, quali la natura e la forma dei documenti (es. le determinazioni, i contratti, i registri di protocollo) oppure in base alla materia trattata, all'affare o al procedimento al quale afferiscono (es. i fascicoli personali, le pratiche di finanziamento e in generale le pratiche attivate dall'amministrazione nello svolgimento dell'attività istituzionale).
Le serie documentarie sono formate dai registri e dai relativi fascicoli compresi in un arco d'anni variabile.

I fascicoli subiscono il processo di selezione e scarto dei documenti; le serie così composte, faranno parte, successivamente, della sezione storica dell'archivio. (Riferimento: art. 41 comma 3 D. Lgs. 42/2004; DPR 8 gennaio 2001 n. 37, art.10, regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di vigilanza sugli archivi e per lo scarto dei documenti degli uffici dello Stato (entrambe le disposizioni si riferiscono agli Archivi di Stato e dunque agli archivi statali, ma per prassi si applicano anche agli archivi pubblici non statali, per i quali non esiste una norma analoga; lo scarto dei documenti degli archivi pubblici e degli archivi privati dichiarati di interesse storico particolarmente importante è disciplinato dall'art. 21, comma 1, lett. d) dello stesso decreto legislativo 42/2004).

1.4.2 Repertori e serie archivistiche

I documenti soggetti a registrazione particolare, come i verbali, le delibere degli organi di governo dell'amministrazione, o i contratti, costituiscono una serie archivistica. Tali documenti sono organizzati nel registro di repertorio.
Con riguardo alla gestione dei documenti cartacei, è previsto che per ogni verbale, delibera, determinazione, decreto, ordinanza e contratto siano, di norma, prodotti almeno due originali, di cui:

- uno viene inserito nel registro di repertorio con il numero progressivo di repertorio;
- l'altro, viene conservato nel relativo fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Per quanto concerne la gestione dei documenti informatici, ogni verbale, delibera, determinazione,

decreto, ordinanza e contratto è, di norma, associato:

- al registro di repertorio con il numero progressivo di repertorio;
- al fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Nel repertorio generale sono riportati gli elementi obbligatori del documento (data, classifica e numero di repertorio) che identificano il documento all'interno del repertorio stesso.
Il repertorio è costantemente aggiornato in automatico del sistema software in uso presso questa Amministrazione.

1.4.3 Versamento dei fascicoli nell'archivio di deposito

La formazione dei fascicoli (virtuali o tradizionali), delle serie e dei repertori è una funzione fondamentale della gestione archivistica.
Periodicamente, e comunque almeno una volta all'anno, il RSP provvede a trasferire i fascicoli e le serie documentarie relativi ai procedimenti conclusi in un'apposita sezione di deposito dell'archivio generale costituito presso l'amministrazione/AOO.
Per una regolare e costante "alimentazione" dell'archivio di deposito lo stesso responsabile dell'archivio (che coincide con il RSP) stabilisce tempi e modi di versamento dei documenti, organizzati in fascicoli, serie e repertori, dagli archivi correnti dei diversi UOR/UU dell'amministrazione/AOO all'archivio di deposito.
Con la stessa metodologia vengono riversati nell'archivio di deposito anche gli altri repertori generali.
La regolare periodicità dell'operazione è fondamentale per garantire l'ordinato sviluppo (o il regolare accrescimento) dell'archivio di deposito.
Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.
Prima di effettuare il conferimento di cui sopra, il RPA/UU procede alla verifica:

- dell'effettiva conclusione ordinaria della pratica;
- dell'avvenuta annotazione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;
- della corretta indicazione della data di chiusura sulla camicia del fascicolo;

Il RPA/UU provvede inoltre:

- allo scarto di eventuali copie e fotocopie di documentazione di cui è possibile l'eliminazione al fine di garantire la presenza di tutti e soli i documenti relativi alla pratica trattata senza inutili duplicazioni;
- a verificare che il materiale da riversare sia correttamente organizzato e corredato da strumenti che ne garantiscano l'accesso organico.

Ricevuti i fascicoli e controllato l'aggiornamento del relativo repertorio, il RSP predispone un elenco di "versamento" da inviare al servizio archivistico.
Copia di detto elenco viene conservata dal responsabile che ha versato la documentazione.
I fascicoli che riguardano il personale devono essere trasferiti dall'archivio corrente all'archivio di deposito l'anno successivo a quello di cessazione dal servizio.

1.4.4 Verifica della consistenza del materiale riversato nell'archivio di deposito

L'ufficio ricevente esegue il controllo del materiale riversato.
Il servizio archivistico dell'amministrazione/AOO riceve agli atti soltanto i fascicoli con materiale ordinato e completo.
Il fascicolo che in sede di controllo risulta mancante di uno o più documenti ovvero presenti delle incongruenze deve essere restituito agli UOR/UU tenutari dell'archivio corrente, affinché provvedano alla

integrazione e/o correzioni necessarie.
Nell'eventualità che non sia stato possibile recuperare uno o più documenti mancanti, il responsabile degli UOR deposita il fascicolo dichiarando ufficialmente che è incompleto e si assume la responsabilità della trasmissione agli atti.
Ricevuti i fascicoli e controllato il relativo elenco, il responsabile del servizio archivistico dell'amministrazione firma per ricevuta l'elenco di consistenza.

1.5 Scarto, selezione e riordino dei documenti

1.5.1 Operazione di scarto

Nell'ambito della sezione di deposito dell'archivio viene effettuata la selezione della documentazione da conservare perennemente e lo scarto degli atti che l'amministrazione non ritiene più opportuno conservare ulteriormente, allo scopo di conservare e garantire il corretto mantenimento e la funzionalità dell'archivio, nell'impossibilità pratica di conservare indiscriminatamente ogni documento.
Un documento si definisce scartabile quando ha perso totalmente la sua rilevanza amministrativa e non ha assunto alcuna rilevanza storica.
La legge impone all'amministrazione/AOO l'uso, se già esiste, o la predisposizione di un massimario di selezione e scarto e un piano di conservazione di atti dell'archivio. Questa amministrazione intende predisporre tale massimario entro la prima data di riversamento nell'archivio di deposito (presumibilmente 31/08/2017) e di aggiornarlo costantemente ad ogni ripetersi dell'azione descritta.
Il massimario viene proposto dal RSP, alla direzione generale degli archivi del Ministero per i beni e le attività culturali e viene autorizzato con atto formale dall'organo competente dell'amministrazione.
Le operazioni di selezione e scarto sono effettuate, sotto la vigilanza del RSP (o da persona delegata, ad esempio il responsabile dell'archivio), a cura degli addetti del servizio archivistico.
I documenti e gli atti sottoposti a procedura di scarto sono devoluti gratuitamente secondo quanto stabilito dal decreto del Presidente della Repubblica del' 8 gennaio 2001, n. 47 art. 1. In particolare l'amministrazione/AOO intende procedere come di seguito descritto.
L'Amministrazione, stabilita la scartabilità del documento in base alle regole prima descritte, valuta se tale documento possa avere una valenza storica o altro per quanto a sua conoscenza. In questo caso il documento viene dotato al competente organo, in caso contrario il documento viene semplicemente distrutto avendo cura che nessuno possa più aver accesso a tale documento o a parte del suo contenuto.

1.5.2 Conservazione del materiale presso la sezione di deposito dell'archivio

L'operazione di riordino della sezione di deposito dell'archivio viene effettuata con la periodicità stabilita dall'amministrazione/AOO e consiste nella schedatura dei materiali e nell'organizzazione delle schede, questa Amministrazione ha deciso che tale riordino debba avvenire con cadenza annuale.
L'operazione si conclude con la sistemazione fisica del materiale, mediante l'inserimento in unità di condizionamento (scatole, pallets, etc.) che riportano all'esterno l'indicazione del contenuto, la classificazione e i tempi di conservazione dei documenti.

1.5.3 Versamento dei documenti nell'archivio storico

Gli enti pubblici, territoriali e non, trasferiscono al proprio archivio storico i documenti relativi agli affari esauriti da oltre quarant'anni unitamente agli strumenti che ne garantiscono la consultazione.
I trasferimenti vengono effettuati dopo il completamento delle operazioni di scarto.
Presso l'archivio storico i documenti vengono inventariati al fine della conservazione, consultazione e

valorizzazione.

1.6 Consultazione e movimentazione dell'archivio corrente, di deposito e storico

1.6.1 Principi generali

La richiesta di consultazione, che può comportare la movimentazione dei fascicoli, può pervenire dall'interno dell'amministrazione/AOO oppure da utenti esterni all'amministrazione, per scopi giuridico-amministrativi o per scopi storici.

1.6.2 Consultazione ai fini giuridico-amministrativi (legge 241/90 e successive modifiche)

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15 che qui di seguito si riporta.

"Esclusione dal diritto di accesso".

1. Il diritto di accesso è escluso:
- per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
- nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
- nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
- nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.

2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.

3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.

4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.

5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'àmbito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.

6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi:
- quando, al di fuori delle ipotesi disciplinate dall'articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative

leggi di attuazione;
- quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
- quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;
- quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono;
- quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

7. Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici.
Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale".

1.6.3 Consultazione per scopi storici

La richiesta di consultazione ai fini di ricerca per scopi storici è disciplinata dal regolamento emanato da ciascuna amministrazione/AOO. Per le amministrazioni/AOO non statali il regolamento è emanato sulla base degli indirizzi generali stabiliti dal Ministero per i beni e le attività culturali (a norma dell'art. 124 del decreto legislativo 22 gennaio 2004, n. 42).
La ricerca per scopi storici è:
- gratuita;
- libera riguardo ai documenti non riservati per legge, per declaratoria del Ministero dell'interno (a norma dell'art. 125 del decreto legislativo 22 gennaio 2004, n. 42) o per regolamento emanato dalla stessa amministrazione/AOO. È possibile l'ammissione alla consultazione dei documenti riservati, previa autorizzazione rilasciata dal Ministero dell'interno, su conforme parere dell'autorità archivistica competente (Archivio di Stato o soprintendenza archivistica, a seconda che si tratti di archivi statali o non statali);
- condizionata all'accettazione integrale del "codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" da parte del soggetto consultatore.

1.6.4 Consultazione da parte di personale esterno all'amministrazione

La domanda di accesso ai documenti viene presentata al servizio archivistico o all'Ufficio Relazioni con il Pubblico (URP), che provvede a smistarla al servizio archivistico.
Presso il servizio archivistico e l'URP sono disponibili appositi moduli. Le richieste di accesso ai documenti della sezione storica dell'archivio possono essere inoltrate anche alla soprintendenza per i beni archivistici territorialmente competente, con apposito modulo da questa predisposto.
Le domande vengono evase durante gli orari di apertura al pubblico dell'URP e dell'archivio con la massima tempestività e comunque non oltre 30 giorni lavorativi dalla presentazione.
Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed

archiviate in formato digitale.
In tale caso il responsabile del servizio archivistico provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata. In caso di richieste di consultazione di materiale cartaceo che comportano l'attivazione di ricerche complesse, il termine di evasione della richiesta, di norma, si raddoppia.
L'ingresso all'archivio di deposito e storico è consentito solo agli addetti del servizio archivistico. La consultazione dei documenti è possibile esclusivamente in un locale appositamente predisposto (aula di studio o di consultazione) sotto la diretta sorveglianza del personale addetto.
Il rilascio di copie dei documenti dell'archivio avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'amministrazione.
In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o in rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione entro il termine di 30 giorni.
Le disposizioni dei commi precedenti si applicano anche alla consultazione di archivi storici presso le pubbliche amministrazioni che non si siano ancora dotate di apposito servizio per l'apertura alla pubblica consultazione degli archivi.

1.6.5 Consultazione da parte di personale interno all'amministrazione

Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito o storica.
L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito o storico ad un ufficio del medesimo UOR/UU od altro UOR/UU avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.
Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa redatta in duplice copia su un apposito modello, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, il suo UOR/UU e la sua firma.
Un esemplare della richiesta di consultazione viene conservato all'interno del fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio.
Tale movimentazione viene registrata a cura del responsabile del servizio archivistico in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna/invio e quella di restituzione, nonché eventuali note sullo stato della documentazione in modo da riceverla nello stesso stato in cui è stata consegnata.
Il responsabile del servizio archivistico verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.
L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, rispettandone la sedimentazione archivistica e il vincolo.
Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'amministrazione/AOO.
In ogni caso deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

2. Modalità di produzione e di conservazione delle registrazioni di protocollo informatico

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

2.1 Unicità del protocollo informatico

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica in base al modello organizzativo centralizzato adottato da questa Amministrazione/AOO. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.
Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.
Il numero di protocollo è costituito da almeno sette cifre numeriche.
Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.
Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.
La documentazione che non è stata registrata presso una UOP viene considerata giuridicamente inesistente presso l'amministrazione.
Non è consentita la protocollazione di un documento già protocollato.
Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.
Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

2.2 Registro giornaliero di protocollo

Il RSP provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. La produzione di tale registro viene effettuata in automatico dal sistema informatico di questa Amministrazione.
Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è inviato, al termine della giornata lavorativa, al supporto per la conservazione a norma al fine di garantirne la completa immodificabilità (2C Solution per questa Amministrazione).
Questa operazione è eseguita dall'RSP.

2.3 Registrazione di protocollo

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).
Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.
Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.
Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata

in forma non modificabile;
- il mittente che ha prodotto il documento, registrato in forma non modificabile;
- il destinatario del documento, registrato in forma non modificabile;
- l'oggetto del documento, registrato in forma non modificabile;
- la classificazione.

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.
Tali dati facoltativi sono descritti nei paragrafi seguenti.

2.3.1 Documenti informatici

I documenti informatici sono ricevuti e trasmessi in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'amministrazione.
La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma.
Nel caso di documenti informatici in partenza, l'operatore esegue anche la verifica della validità amministrativa della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto o inviato.
La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati.
I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.
Le UOP ricevono i documenti informatici interni di tipo formale da protocollare all'indirizzo di posta elettronica interno preposto a questa funzione o tramite il sistema di messaggistica interna utilizzato dall'applicazione gestita in questa Amministrazione.

2.3.2 Documenti analogici (cartacei e supporti rimovibili)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza, (il servizio postale pubblico e/o privato o con consegna diretta alla UOP).
La registrazione di protocollo di un documento analogico cartaceo ricevuto, così come illustrato nel seguito, viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.
Nel caso di corrispondenza in uscita o interna formale, l'UOP esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

2.4 Elementi facoltativi delle registrazioni di protocollo

Il RSP, con proprio provvedimento e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può modificare e integrare gli elementi facoltativi del protocollo.
La registrazione degli elementi facoltativi del protocollo, con determinazione del RSP può essere modificata, integrata e cancellata in base alle effettive esigenze delle UOR o degli UOP.
I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.
Di seguito vengono riportati gli elementi facoltativi finalizzati alla conservazione e gestione della

documentazione:

- ora e minuto di registrazione;
- luogo di provenienza o di destinazione del documento;
- tipo di documento;
- mezzo di ricezione/spedizione (ordinaria, espressa, corriere, raccomandata con ricevuta di ritorno, telefax, ecc.);
- collegamento a documenti precedenti e susseguenti;
- numero degli allegati;
- riferimenti agli allegati su supporto informatico;
- nominativo dei destinatari delle copie per conoscenza;
- UOR/UU competente;
- identificativo del RPA;
- termine di conclusione del procedimento amministrativo o di lavorazione del documento;
- indicazione del livello di sicurezza se diverso da quello standard applicato dal sistema di protocollazione;
- stato e tempi parziali delle procedure del procedimento amministrativo;
- classificazione del documento (titolo, categoria e fascicolo; eventuale sottofascicolo e inserto);
- data di istruzione del fascicolo;
- numero del fascicolo;
- numero del sottofascicolo;
- numero dell'inserto;
- data di chiusura del fascicolo;
- repertorio dei fascicoli;
- identificativo del fascicolo e/o del documento;
- numero di repertorio della serie (delibere, determinazioni, verbali, circolari e contratti);
- tipologia del documento con l'indicazione dei termini di conservazione e di scarto;
- scadenzario.

2.5 Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.
La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.
Essa consente di individuare ciascun documento in modo inequivocabile.

2.5.1 Documenti informatici

I dati della segnatura di protocollo di un documento informatico 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) reso disponibile dalla procedura software in dotazione a questa Amministrazione e comunque personalizzabile dall'utenza o direttamente dalla società Axios in base ad eventuali e sopraggiunte necessità anche per migliorare la fruibilità del prodotto.
Le informazioni minime incluse nella segnatura sono quelle di seguito elencate:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- data e numero di protocollo del documento.

È facoltativo riportare anche le seguenti informazioni:

- denominazione dell'amministrazione;
- indice di classificazione;
- il codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo.

Per i documenti informatici in partenza, possono essere specificate, in via facoltativa, anche le seguenti informazioni:

- persona o ufficio destinatario;
- identificazione degli allegati;
- informazioni sul procedimento e sul trattamento.

La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.
Quando il documento è indirizzato ad altre AOO la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.
L'AOO che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.
Qualora l'AOO decida di scambiare con altre AOO informazioni non previste tra quelle definite come facoltative, può estendere il file di cui sopra, nel rispetto delle regole tecniche dettate dal CNIPA, includendo le informazioni specifiche stabilite di comune accordo con l'AOO con cui interagisce.

2.5.2 Documenti cartacei

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un "segno" grafico sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- codice identificativo dell'amministrazione,
- codice identificativo dell'AOO;
- data e numero di protocollo del documento;

Facoltativamente possono essere riportate anche le seguenti informazioni:

- denominazione dell'amministrazione;
- indice di classificazione;
- il codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo;
- ogni altra informazione utile o necessaria, se già disponibile al momento della registrazione di protocollo.

Il "segno" grafico di norma è realizzato con una etichetta autoadesiva corredata di codice a barre o, in alternativa, con un timbro tradizionale.
L'operazione di segnatura dei documenti in partenza viene effettuata dall'UOR/UU/RPA competente che redige il documento se è abilitata, come UOP, alla protocollazione dei documenti in uscita; in alternativa l'operazione viene integralmente eseguita dalla UOP.
L'operazione di acquisizione dell'immagine dei documenti cartacei è eseguibile solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.
Se è prevista l'acquisizione del documento cartaceo in formato immagine, il "segno" della segnatura di protocollo deve essere apposto sulla prima pagina dell'originale; in caso contrario il "segno" viene apposto sul retro della prima pagina dell'originale.

2.6 Annullamento delle registrazioni di protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrati in forma non modificabile - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.
Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RSP.
In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.
Solo il RSP è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.
L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RSP.
A tal fine è istituito un registro (informatico o cartaceo) per le richieste di annullamento delle registrazioni e dei dati obbligatori delle registrazioni.
Il registro riporta i motivi dell'annullamento e, se il documento è stato protocollato nuovamente, il nuovo numero di protocollo assegnato.

2.7 Livello di riservatezza

L'operatore che effettua la registrazione di protocollo di un documento attribuisce allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal sistema.
In modo analogo, il RPA che effettua l'operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza.
Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti che invece hanno un livello di riservatezza superiore lo mantengono.

2.8 Casi particolari di registrazioni di protocollo

2.8.1 Registrazioni di protocollo particolari (riservate)

All'interno dell'AOO è istituito il protocollo riservato - sottratto alla consultazione da parte di chi non sia espressamente abilitato - nel quale sono riportati:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- le tipologie di documenti individuati dalla normativa vigente.

La registrazione nel protocollo particolare, quando non sia palesemente evidente la necessità, può essere disposta dal RSP con l'apposizione, sul documento, della seguente dicitura: "Da registrare sul protocollo particolare".

I documenti (informatici o cartacei) anonimi, come tali individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale, vengono inviati al RSP che ne effettua una valutazione:

- se ritiene che contengano dati o informazioni di interesse dell'amministrazione/AOO, provvede ad inviarli agli uffici competenti per le ulteriori eventuali determinazioni. Questi decidono se registrarli, farli registrare nel protocollo generale;
- se ritiene che non contengano dati rilevanti dal punto di vista amministrativo, il documento viene registrato nel protocollo particolare.

2.8.2 Circolari e disposizioni generali

Le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale.
I destinatari sono indicati in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo secondo le modalità previste dalla gestione anagrafica del sistema.

2.3.3 Documenti cartacei in partenza con più destinatari

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica e viene riportata solo sul documento originale con la dicitura "Questa registrazione di protocollo viene riportata sui documenti degli altri destinatari - Vedi elenco allegato alla minuta/copia presso l'UOR/UU/RPA.
Tale elenco, in formato cartaceo, viene allegato alla minuta dell'originale.

2.8.4 Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma inoltrati al servizio protocollo come documenti senza firma, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

2.8.5 Documenti cartacei ricevuti a mezzo telefax

Il documento ricevuto a mezzo telefax è un documento analogico a tutti gli effetti.
Il documento trasmesso da chiunque ad una pubblica AOO tramite telefax, qualora ne venga accertata la fonte di provenienza, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale.
L'accertamento della fonte di provenienza spetta al RPA e avviene, di norma, per le vie brevi o con l'uso di sistemi informatici.
Qualora non sia possibile accertare la fonte di provenienza, sul telefax viene apposta la dicitura "Documento ricevuto via telefax" e successivamente il RPA provvede ad acquisire l'originale.
Nel caso che al telefax faccia seguito l'originale, poiché ogni documento viene individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione, l'addetto alla registrazione a protocollo, dopo aver registrato il telefax, deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax ed apporre la seguente dicitura: "Già pervenuto via fax il giorno…".
Il RSP accerta comunque che si tratta del medesimo documento ricevuto via fax: qualora dovesse riscontrare una differenza, anche minima, deve procedere alla registrazione con un nuovo numero di protocollo in quanto si tratta di un documento diverso.
Il fax ricevuto con un terminale telefax dedicato (diverso da un PC) è fotocopiato dal ricevente qualora il supporto cartaceo non fornisca garanzie per una corretta e duratura conservazione.
Su di esso o sulla sua foto-riproduzione va apposta, a cura del ricevente, la dicitura "Documento ricevuto via telefax".

Il documento in partenza reca una delle seguenti diciture:

- "Anticipato via telefax" se il documento originale viene successivamente inviato al destinatario;
- "La trasmissione via fax del presente documento non prevede l'invio del documento originale» nel caso in cui l'originale non venga spedito. Il RPA è comunque tenuto a spedire l'originale qualora il destinatario ne faccia motivata richiesta;

La segnatura viene apposta sul documento e non sulla copertina di trasmissione.
La copertina del telefax ed il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.
Il fax ricevuto direttamente su una postazione di lavoro (esempio un PC con l'applicativo per invio e ricezione di fax) è la rappresentazione informatica di un documento che può essere, sia stampato e trattato come un fax convenzionale come è stato descritto nei paragrafi precedenti, sia visualizzato e trattato interamente con tecniche informatiche.
In questo secondo caso il "file" rappresentativo del fax, viene inviato al protocollo generale, per essere sottoposto alle operazioni di protocollazione e segnatura secondo gli standard XML vigenti e poi, trattato secondo le regole precedentemente specificate per la gestione dei documenti informatici.

2.8.6 Protocollazione di un numero consistente di documenti cartacei

Quando si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso (es. scadenza gare o concorsi) che in uscita, deve esserne data comunicazione all'ufficio protocollo con almeno due giorni lavorativi di anticipo, onde concordare tempi e modi di protocollazione e di spedizione.

2.8.7 Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio

La corrispondenza ricevuta con rimessa diretta dall'interessato o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.
Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta. Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, essi saranno accantonati e protocollati successivamente (come di seguito descritto). In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

2.8.8 Fatture, assegni ed altri valori di debito o credito

Le buste contenenti fatture, assegni o altri valori di debito o credito sono immediatamente separate dall'altra posta in arrivo, protocollate su un registro diverso da quello generale e inviate quotidianamente all'UOR competente.

2.8.9 Protocollazione di documenti inerenti a gare di appalto confezionati su supporti cartacei

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo" o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata all'UOR competente.
È compito dello stesso UOR provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi

idonei, sino all'espletamento della gara stessa.
Dopo l'apertura delle buste l'UOR che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.
Per motivi organizzativi tutti gli UOR sono tenuti ad informare preventivamente il RSP dell'amministrazione in merito alle scadenze di concorsi, gare, bandi di ogni genere.

2.8.10 Protocolli urgenti

La richiesta di protocollare urgentemente un documento è collegata ad una necessità indifferibile e di tipo straordinario.
Solo in questo caso il RSP si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale o cartaceo da spedire.
Tale procedura viene osservata sia per i documenti in arrivo che per quelli in partenza, raccomandando, per questi ultimi, che non devono essere protocollati anticipatamente documenti diversi dall'originale (ad esempio bozze del documento), fatti pervenire all'UOP.

2.8.11 Documenti non firmati

L'operatore di protocollo, conformandosi alle regole stabilite dal RSP attesta la data, la forma e la provenienza per ogni documento.
Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "Mittente sconosciuto o anonimo" e "Documento non sottoscritto".
Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.
È poi compito dell'UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

2.8.12 Protocollazione dei messaggi di posta elettronica convenzionale

Considerato che l'attuale sistema di posta elettronica non certificata non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata nei seguenti modi:

- in caso di invio, come allegato, di un documento scansionato e munito di firma autografa, quest'ultimo è trattato come un documento inviato via fax fermo restando che l'RPA deve verificare la provenienza certa dal documento; in caso di mittente non verificabile, l'RPA valuta caso per caso l'opportunità di trattare il documento inviato via e-mail;
- in caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale, il documento e/o il messaggio sono considerati come un documento elettronico inviato con qualunque mezzo di posta;
- in caso di invio di una e-mail contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

2.8.13 Protocollo di documenti digitali pervenuti erroneamente

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all'amministrazione non competente, l'addetto al protocollo provvede o ad annullare il protocollo stesso o provvede a protocollare il documento in uscita indicando nell'oggetto "protocollato per errore" e rispedisce il messaggio al mittente.

2.8.14 Ricezione di documenti cartacei pervenuti erroneamente

Nel caso in cui sia protocollato un documento cartaceo erroneamente inviato all'amministrazione, l'addetto al protocollo provvede o ad annullare il protocollo stesso o provvede a protocollare il documento in uscita indicando nell'oggetto "protocollato per errore"; il documento oggetto della rettifica viene restituito al mittente con la dicitura "protocollato per errore".

2.8.15 Copie per conoscenza

Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nel paragrafo 2.8.3. In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, inserisce nel registro di protocollo i nominativi di coloro ai quali sono state inviate le suddette copie per conoscenza.
Tale informazione è riportata anche sulla segnatura di protocollo.

2.8.16 Differimento delle registrazioni

Le registrazioni di protocollo dei documenti pervenuti presso l'amministrazione destinataria sono effettuate nella giornata di arrivo e comunque non oltre le 48 ore dal ricevimento di detti documenti.
Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del RSP, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.
Il protocollo differito consiste nel differimento dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento sopra citato.

2.8.17 Registrazioni di documenti temporaneamente riservati

Quando si è in presenza di documenti che per la loro natura richiedono una temporanea riservatezza delle informazioni in essi contenute (ad esempio gare e appalti, verbali di concorso, etc.), è prevista una forma di accesso riservato al protocollo generale.
Il responsabile dell'immissione dei dati provvede alla registrazione di protocollo indicando contestualmente l'anno, il mese e il giorno, nel quale le informazioni temporaneamente riservate saranno accessibili nelle forme ordinarie.

2.8.18 Corrispondenza personale o riservata

La corrispondenza personale è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale".
In quest'ultimo caso, la corrispondenza con la dicitura "riservata" o "personale" non è aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli al più vicino ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

2.8.19 Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.

Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.
I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel fascicolo relativo.

2.9 Gestione delle registrazioni di protocollo con il PDP

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono effettuate attraverso il PdP.
Il sistema di sicurezza adottato dall'AOO garantisce la protezione di tali informazioni sulla base dell'architettura del sistema informativo, sui controlli d'accesso e sui livelli di autorizzazione previsti.

2.10 Registrazioni di protocollo

2.10.1 Attribuzione del protocollo

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il servizio di protocollo è realizzato dall'applicativo PdP attraverso l'apposizione di un riferimento temporale come previsto dalla normativa vigente.
Il sistema informativo assicura in tal modo la precisione del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.

- Come previsto dalla normativa in materia di tutela dei dati personali, gli addetti al protocollo adottano tutti gli accorgimenti necessari per la tutela dei dati sensibili. E giudiziari non inserendoli nel campo "oggetto" del registro di protocollo.

2.10.2 Registro informatico di protocollo

Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo generale della AOO si provvede, in fase di chiusura dell'attività di protocollo, ad effettuare le seguenti operazioni:

- estrazione delle registrazioni del giorno corrente (o precedente) dal file del registro generale di protocollo;
- applicazione della firma digitale e di un riferimento temporale al file così realizzato;
- copia del file estratto, del file di firma e del riferimento temporale su supporto rimovibile non riscrivibile;
- salvataggio del file di firma e del riferimento temporale sul sistema di esercizio del PdP.

L'ufficio o l'addetto incaricato di eseguire l'operazione di riversamento dei file in parola su due supporti rimovibili non riscrivibili è stato individuato nel RSP o in chi da lui delegato.
L'uso combinato dei meccanismi permette di conferire validità e integrità ai contenuti del file del registro di protocollo (Le copie giornaliere generali di backup dell'intero sistema informativo dell'amministrazione/AOO esulano dai meccanismi di sicurezza qui richiamati).
È inoltre disponibile, all'occorrenza, per i gestori del PdP una funzione applicativa di "stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.
Al termine delle operazioni giornaliere o, comunque entro il giorno successivo sono effettuate le seguenti operazioni di garanzia:

- Invio in conservazione a norma del registro di protocollo giornaliero

2.10.3 Tenuta delle copie del registro di protocollo

È compito del responsabile della conservazione dei documenti provvedere alla verifica del contenuto dei supporti prodotti dall'ufficio o dall'addetto incaricato.
Una copia dei supporti è conservata nei sistemi di backup della AOO, mentre la seconda copia è custodita nel relativo servizio cloud acquistato appositamente e che consente anche la completa gestione del distaster recovery.
Le modalità di gestione di tali supporti sono definite e regolamentate direttamente dal RSP dell'AOO. I dati contenuti su tali supporti sono conservati con le modalità previste dalla normativa vigente.
Procedendo alle operazioni di riversamento con la periodicità prevista dalla deliberazione CNIPA n. 11/2004.

2.11 Riferimenti

Il riferimento per la stesura di questo documento sono le linee guida pubblicate dall'AGID:
http://www.agid.gov.it/sites/default/files/linee_guida/la_conservazione_dei_documenti_informatici_rev_def_.pdf

Allegato 19/1 - Atto di incarico per la conservazione dei dati a Axios Italia SPA

Questo Istituto ha in essere un contratto di fornitura di servizi con la società Axios Italia SPA.
Il contratto ha durata annuale, viene rinnovato alla fine di ogni anno solare e contiene al suo interno la lettera di incarico con la quale questo Istituto conferisce all'Amministratore Delegato in carica di Axios Italia SPA la nomina a responsabile della conservazione della parte di dati che questo Istituto trasferisce nel Cloud fornito da Axios Italia SPA.

Allegato 19/2 - Atto di incarico per la conservazione dei dati a 2c Solution

Per la parte di dati che concerne la conservazione a norma, Axios Italia SPA si avvale della societa 2c Solution come fornitore di servizi.
Di seguito è riportato il contratto stipulato tra le due società.

SERVIZIO DI FORMAZIONE E CONSERVAZIONE DIGITALE A NORMA

Riferimento Contratto n. 234

Data 05/10/2015

Scheda Servizi Cliente-Specificità del contratto AXIOS ITALIA SERVICE S.R.L.

Soggetto Conservatore
2C Solution S.r.l.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	22/01/2015	Checchin Enrico	Responsabile Trattamento dei dati Responsabile funzione archivistica di Conservazione
Verifica	23/01/2015	Davide Coletto	Responsabile del Servizio di conservazione Responsabile dello sviluppo e della manutenzione del sistema di Conservazione
Approvazione	26/01/2015	Checchin Enrico Davide Coletto	Amministratore Legale rappresentante

Sommario


2C Solution

1 PREMESSA

La presente Scheda Servizio Cliente – Specificità del Contratto (d'ora in avanti Scheda Servizio), parte integrale e sostanziale del contratto e del Manuale di Conservazione, è redatta d'intesa tra Axios e il Conservatore 2C Solution al fine di condividere le modalità di svolgimento della funzione di formazione (servizio opzionale) e conservazione dei documenti informatici.
La Scheda Servizio è aggiornata e condivisa tra il Cliente e il 2C Solution Srl ogniqualvolta intervengano modifiche o integrazioni relative agli oggetti trattati.

2 REVISIONI DEL DOCUMENTO

Versione	Data versione	Descrizione modifiche
1.0	01/10/2015	Prima stesura

3 DOCUMENTI ALLEGATI

Non previsti

4 REFERENTI CONSERVATORE 2C SOLUTION

Nominativo	Ruolo	Contatti	Regole di comunicazione
Servizio di Help Desk	Servizio di Help Desk 2C Solution	supportosdc@2csolution.it	Assistenza di I livello a cui il Cliente è obbligato alla comunicazione
Davide Coletto	Responsabile del Servizio di conservazione Responsabile dello sviluppo e della manutenzione del sistema di Conservazione Legale rappresentante 2C Solution s.r.l.	davide.c@2csolution.it	Da utilizzare solo in reali casi di emergenza ed escalation
Enrico Checchin	Responsabile Trattamento dei dati Responsabile funzione archivistica di Conservazione Amministratore 2CSolution s.r.l.	enrico.c@2csolution.it	Da utilizzare solo in reali casi di emergenza ed escalation
Mario Veltini	Responsabile del rispetto dei requisiti di sicurezza del sistema di conservazione e degli	mario.v@2csolution.it	Da utilizzare solo in reali casi di emergenza ed escalation

	standard stabiliti dalle normative e dalle procedure interne di sicurezza Responsabile del servizio di conservazione e di individuazione di azioni correttive		

5 *DATI DEL PRODUTTORE DEI DOCUMENTI*

Tali dati sono contenuti nella Richiesta di Attivazione.

6 *REFERENTI*

]

	Cognome e nome	Azienda	Ruolo	E-mail
REFERENTE 1	GIANCARLO DELLI COLLI	AXIOS ITALIA SERVICE S.R.L.	**Legale Rappresentante**	giancarlo.dellicolli@axiositalia.com
REFERENTE 2	DANIELE DE VITA	AXIOS ITALIA SERVICE S.R.L.	**Referente per quanto attiene i rapporti generali con il Conservatore 2C Solution**	daniele.devita@3d-solution.it
REFERENTE 3	ALESSANDRA TOSCANO	AXIOS ITALIA SERVICE S.R.L.	**Referente per quanto attiene i rapporti generali con il Conservatore 2C Solution**	alessandra.toscano@axiositalia.com

7 *NORMATIVA E STANDARD DI RIFERIMENTO*

7.1 Normativa di riferimento

Nel presente paragrafo è riportata la principale normativa di riferimento per l'attività di conservazione a livello nazionale, ordinata 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;
- **Legge 24 dicembre 2012, n. 228,** cosiddetta "Legge di stabilità 2013" in merito alla fatturazione elettronica e la conservazione delle fatture (recepimento della direttiva comunitaria 2010/45/UE che modifica gli artt. 21 e 39 del D.P.R. 633/72);
- **Decreto del Presidente della Repubblica 26 ottobre 1972, n. 633** – Istituzione e disciplina dell'imposta sul valore aggiunto;
- **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 19 luglio 2012** – Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al DPCM 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma;
- **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 21 marzo 2013** – Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.
- **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 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;
- **Decreto Ministeriale 9 luglio 2008 -** Modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio;
- **Decreto Ministeriale 3 aprile 2013, n. 55** – Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244;
- **Decreto Ministeriale 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. 82/2005;
- **Circolare del Ministero del Lavoro n. 20 del 21 agosto 2008** – Libro Unico del Lavoro e attività ispettiva – artt. 39 e 40 del DL n. 112 del 2008: prime istruzioni operative al personale ispettivo;
- **Deliberazione CNIPA n. 45 del 21 maggio 2009 e s.m.i.** – Regole per il riconoscimento e la verifica del documento informatico;
- **Circolare Agenzia delle Entrate n. 36/E del 6 dicembre 2006 -** Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto – Decreto ministeriale 23 gennaio 2004;
- **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;
- **Circolare Agenzia delle Entrate n. 18/E del 24 giugno 2014** – IVA. Ulteriori istruzioni in tema di fatturazione;
- **Regolamento ISVAP n. 27 del 14 ottobre 2008** – Regole per la tenuta e conservazione dei registri assicurativi di cui all'art. 101 del D.Lgs. n. 209 del 7 settembre 2005 – Codice delle Assicurazioni Private;

- **Risoluzione Agenzia delle Entrate n. 161/E del 9 luglio 2007 -** Fatturazione elettronica e modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto;
- **Risoluzione Agenzia delle Entrate n. 158/E del 15 giugno 2009** – Consulenza giuridica Associazione e Ordini Professionali – D.M. 23 gennaio 2004 e fatturazione elettronica – risposta a quesiti;
- **Risoluzione Agenzia delle Entrate n. 65/E del 14 giugno 2011** – Modalità di presentazione della dichiarazione di variazione dati relativa al luogo di conservazione delle scritture contabili;
- **Risoluzione Agenzia delle Entrate n. 106/E del 2 dicembre 2014** istituzione del codice tributo "**2501**" da esporre nella sezione erario, denominato "Imposta di bollo su libri, registri ed altri documenti rilevanti ai fini tributari – articolo 6 del decreto 17 giugno 2014".
- **Risoluzione Agenzia delle Entrate n. 4/E del 19 gennaio 2015**: Consulenza giuridica – Conservazione sostitutiva dei documenti informatici rilevanti ai fini tributari – Obbligo di invio dell'impronta dell'archivio informatico di cui all'art. 5 del D.M. 23 gennaio 2004 – Non sussiste
- **Risoluzione Agenzia delle Entrate n. 32/E del 23 marzo 2015 istituzione dei seguenti codici tributo**:
  "2502" denominato "Imposta di bollo su libri, registri ed altri documenti rilevanti ai fini tributari – art. 6, decreto 17 giugno 2014 - SANZIONI".
  "2503" denominato "Imposta di bollo su libri, registri ed altri documenti rilevanti ai fini tributari – art. 6, decreto 17 giugno 2014 – INTERESSI".
- **Linee Guida per la Dematerializzazione della documentazione clinica in laboratorio e in diagnostica per le immagini** – Normativa e prassi – Ministero della Salute.

7.2 Standard

Si riportano di seguito gli standard di riferimento a cui l'attività di conservazione del Conservatore 2C Solution si riferisce, elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° ottobre 2014, come indicato nelle regole tecniche di cui al DPCM 3 Dicembre 2013.

- **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.

8 *RESPONSABILE della CONSERVAZIONE*

La struttura organizzativa di 2C Solution s.r.l., che è descritta più dettagliatamente nel Manuale di conservazione, prevede il ruolo del Responsabile della Conservazione, che è nominato formalmente dal Cliente e al quale sono affidate le seguenti attività:

- 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.

9 *DELEGATO DELLA CONSERVAZIONE*

Il Responsabile della Conservazione, conformemente a quanto previsto dalle Regole tecniche sul sistema di conservazione (art. 6, c. 6 DPCM 3 dicembre 2013) può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate.
Nella seguente tabella sono riportati i dati del soggetto Delegato alla conservazione.

Ragione sociale	**2C Solution s.r.l.**				
con sede operativa in (città)	Gazzo	**CAP**	35010	**(prov.)**	PD
indirizzo	Via Vittorio Alfieri			**(n.)**	34
codice fiscale	04030410288	**partita iva**	04030410288		
telefono	0499426171	**fax**	0492106344		
indirizzo e-mail per Comunicazioni	contratti@2csolution.it supportosdc@2csolution.it				
PEC	2csolution@pec.solutiondoc.eu				

2C SOLUTION SRL, quale Delegato alla conservazione, è tenuto a svolgere i seguenti compiti:

a. definizione delle caratteristiche e dei requisiti del Sistema di conservazione, in funzione della tipologia dei Documenti informatici oggetto della Conservazione, in conformità alla vigente normativa;
b. gestione del processo di conservazione in conformità alla vigente normativa in materia; a riguardo, il Responsabile della conservazione autorizza sin d'ora il Responsabile del servizio di conservazione ad apporre la propria firma digitale sull'indice dei vari pacchetti e sul rapporto di versamento generati nel processo di conservazione;
c. generazione del Rapporto di versamento, secondo le modalità previste dal Manuale di conservazione;
d. generazione e sottoscrizione del pacchetto di distribuzione con firma digitale, nei casi e con le modalità descritte nel Manuale di conservazione;
e. monitoraggio della corretta funzionalità del Sistema di conservazione;

f. verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
g. adozione di misure idonee a verificare e prevenire il degrado dei sistemi di memorizzazione e delle registrazioni, l'obsolescenza dei formati al fine di garantire la conservazione e l'accesso ai Documenti informatici;
h. duplicazione o copia dei Documenti informatici, dovuta all'eventuale evoluzione del contesto tecnologico, secondo quanto previsto dal Manuale di conservazione;
i. adozione di misure idonee per la sicurezza fisica e logica del Sistema di conservazione;
j. richiesta di intervento al pubblico ufficiale, ove previsto, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k. assistenza e impiego delle risorse necessarie per l'espletamento delle attività di verifica e di vigilanza dei diversi organismi competenti previsti dalle norme vigenti in materia;
l. nel caso di amministrazioni statali, versamento dei documenti conservati presso l'archivio centrale dello Stato e gli archivi di Stato secondo quanto previsto dalle norme vigenti;
m. predisposizione del Manuale di conservazione e cura del relativo aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

10 RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE

La struttura organizzativa del Conservatore 2C SOLUTION SRL, che è descritta più dettagliatamente nel Manuale di conservazione, prevede il ruolo del Responsabile del Servizio di Conservazione, che è nominato formalmente e al quale sono affidate le seguenti attività:

- 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.

11 OGGETTI SOTTOPOSTI A CONSERVAZIONE

1	**TIPOLOGIA DOCUMENTALE**	**Documenti fiscali attivi**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**	**Documenti fiscali attivi**
1.2	**Natura di documento informatico amministrativo**	NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.

1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO
1.5	**Metadati**	*1 Anno di riferimento*** *2 Tipo documento (F/NC/ND)*** *3 Numero documento*** *4 Data documento*** *5 Ragione sociale destinatario*** *6 Codice fiscale destinatario*** *7 Partita iva destinatario* *8 Codice CIG* *9 Codice CUP* *10 Numero ordine* *11 Data ordine* *12 Numero protocollo* *13 Data protocollo* *14 Annotazioni* *15 Data scarto (gg/mm/aaaa)*** *16 Scarto in anni (zero=perpetuo)***
1.6	**Presenza di fascicolo informatico o aggregazione documentale**	NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**	
1.8	**Durata di conservazione richiesta**	10 anni
1.9	**Formato del file**	Vedi tabella formati ammessi
1.10	**Frequenza conservazione**	Annuale.

2	**TIPOLOGIA DOCUMENTALE**	**Documenti fiscali passivi**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**	**Documenti fiscali passivi**
1.2	**Natura di documento informatico amministrativo**	NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento (F/NC/ND)*** *3 Numero documento*** *4 Data documento*** *5 Ragione sociale mittente*** *6 Codice fiscale mittente*** *7 Partita iva mittente* *8 Codice CIG*

		9 *Codice CUP* *10* *Numero ordine* *11* *Data ordine* *12* *Numero protocollo* *13* *Data protocollo* *14* *Annotazioni* *15* *Data scarto (gg/mm/aaaa)*** *16* *Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale.

3	**TIPOLOGIA DOCUMENTALE**		**Libro Giornale**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**		**Libro Giornale**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.5	**Metadati****	*1* *Anno di riferimento*** *2* *Produttore*** *3* *Codice fiscale produttore*** *4* *Partita iva produttore* *5* *Data* *6* *Annotazioni* *7* *Data scarto (gg/mm/aaaa)*** *8* *Scarto in anni (zero=perpetuo))***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale.

4	**TIPOLOGIA DOCUMENTALE**		**Registri IVA**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**		**Registri IVA**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo registro (A/V/C)*** *3 Tipo sezionale (IT/CEE/EXTRA)*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore* *7 Mese di riferimento* *8 Annotazioni* *9 Data scarto (gg/mm/aaaa)*** *10 Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale.

5	**TIPOLOGIA DOCUMENTALE**		**DDT Attivi**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**		**DDT Attivi**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento***	

		*3 Numero documento*** *4 Data documento*** *5 Ragione sociale destinatario*** *6 Codice fiscale destinatario*** *7 Partita iva destinatario* *8 Codice CIG* *9 Codice CUP* *10 Numero ordine* *11 Data ordine* *12 Numero protocollo* *13 Data protocollo* *14 Annotazioni* *15 Data scarto (gg/mm/aaaa)*** *16 Scarto in anni (zero=perpetuo)***
1.6	**Presenza di fascicolo informatico o aggregazione documentale**	NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**	
1.8	**Durata di conservazione richiesta**	10 anni
1.9	**Formato del file**	Vedi tabella formati ammessi
1.10	**Frequenza conservazione**	Annuale.

6	**TIPOLOGIA DOCUMENTALE**	**DDT Passivi**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**	**DDT Passivi**
1.2	**Natura di documento informatico amministrativo**	NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Numero documento*** *4 Data documento*** *5 Ragione sociale mittente*** *6 Codice fiscale mittente*** *7 Partita iva mittente* *8 Codice CIG* *9 Codice CUP* *10 Numero ordine* *11 Data ordine* *12 Numero protocollo* *13 Data protocollo*

		14 *Annotazioni* *15* *Data scarto (gg/mm/aaaa)*** *16* *Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

7	**TIPOLOGIA DOCUMENTALE**		**Contratti**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**		Contratti
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1* *Anno di riferimento*** *2* *Numero contratto*** *3* *Data contratto*** *4* *Produttore*** *5* *Codice fiscale produttore*** *6* *Partita iva produttore* *7* *Destinatario*** *8* *Codice fiscale destinatario*** *9* *Partita iva destinatario* *10* *Annotazioni* *11* *Data scarto (gg/mm/aaaa)*** *12* *Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

8	**TIPOLOGIA DOCUMENTALE**	**Registro di protocollo**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**	**Registro di protocollo**
1.2	**Natura di documento informatico amministrativo**	NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Oggetto*** *3 Codice IPA*** *4 Codice AOO*** *5 Codice identificativo registro* *6 Data registro*** *7 Registrazione iniziale*** *8 Registrazione finale*** *9 Cognome responsabile ufficio protocollo*** *10 Nome responsabile ufficio protocollo*** *11 Codice fiscale responsabile ufficio protocollo*** *10 Annotazioni* *11 Data scarto (gg/mm/aaaa)*** *12 Scarto in anni (zero=perpetuo)***
1.6	**Presenza di fascicolo informatico o aggregazione documentale**	NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**	
1.8	**Durata di conservazione richiesta**	10 anni
1.9	**Formato del file**	Vedi tabella formati ammessi
1.10	**Frequenza conservazione**	Mensile

9	**TIPOLOGIA DOCUMENTALE**	**Documenti Contabili**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**	**Documenti Contabili**
1.2	**Natura di documento informatico amministrativo**	NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO. E' onere del produttore provvedere alla firma del documento a meno che non

			richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore* *7 Destinatario* *8 Codice fiscale destinatario* *9 Partita iva destinatario* *10 Annotazioni* *11 Data scarto (gg/mm/aaaa)*** *12 Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

10	**TIPOLOGIA DOCUMENTALE**		**Documenti Amministrativi**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**		**Documenti Amministrativi**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore***	

		6 *Partita iva produttore* *7* *Destinatario* *8* *Codice fiscale destinatario* *9* *Partita iva destinatario* *10* *Annotazioni* *11* *Data scarto (gg/mm/aaaa)*** *12* *Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

11	**TIPOLOGIA DOCUMENTALE**		**Registro di classe**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**		**Registro di classe**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1* *Anno di riferimento*** *2* *Anno scolastico*** *3* *Anno di corso*** *4* *Sezione*** *5* *Produttore*** *6* *Codice fiscale produttore*** *7* *Partita iva produttore* *8* *Annotazioni* *9* *Data scarto (gg/mm/aaaa)*** *10* *Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi

1.10	**Frequenza conservazione**	Annuale.

12	**TIPOLOGIA DOCUMENTALE**		**Registro del docente**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**		**Registro del docente**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.5	**Metadati****	*1 Anno di riferimento*** *2 Anno scolastico*** *3 Anno di corso*** *4 Sezione*** *5 Cognome docente*** *6 Nome docente*** *7 Codice fiscale docente*** *8 Materia*** *9 Produttore*** *10 Codice fiscale produttore*** *11 Partita iva produttore* *12 Annotazioni* *13 Data scarto (gg/mm/aaaa)*** *14 Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

13	**TIPOLOGIA DOCUMENTALE**	**Area personale**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**	**Area personale**
1.2	**Natura di documento informatico amministrativo**	NO

1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore* *7 Destinatario* *8 Codice fiscale destinatario* *9 Partita iva destinatario* *10 Annotazioni* *11 Data scarto (gg/mm/aaaa)*** *12 Scarto in anni (zero=perpetuo)***
1.6	**Presenza di fascicolo informatico o aggregazione documentale**	NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**	
1.8	**Durata di conservazione richiesta**	10 anni
1.9	**Formato del file**	Vedi tabella formati ammessi
1.10	**Frequenza conservazione**	Annuale.

14	**TIPOLOGIA DOCUMENTALE**	**Area docenti**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**	**Area docenti**
1.2	**Natura di documento informatico amministrativo**	NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.

1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore* *7 Destinatario* *8 Codice fiscale destinatario* *9 Partita iva destinatario* *10 Annotazioni* *11 Data scarto (gg/mm/aaaa)*** *12 Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti c cui si avvia la conservazione digitale**		Dal 2015
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

15	**TIPOLOGIA DOCUMENTALE**		**Area genitori**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**		**Area genitori**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore* *7 Destinatario* *8 Codice fiscale destinatario*	

		9 *Partita iva destinatario* *10* *Annotazioni* *11* *Data scarto (gg/mm/aaaa)*** *12* *Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

16	**TIPOLOGIA DOCUMENTALE**		**Area alunni**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**		**Area alunni**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1* *Anno di riferimento*** *2* *Tipo documento*** *3* *Oggetto*** *4* *Produttore*** *5* *Codice fiscale produttore*** *6* *Partita iva produttore* *7* *Destinatario* *8* *Codice fiscale destinatario* *9* *Partita iva destinatario* *10* *Annotazioni* *11* *Data scarto (gg/mm/aaaa)*** *12* *Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi

1.10	**Frequenza conservazione**	Annuale

17	**TIPOLOGIA DOCUMENTALE**		**Area inventario e magazzino**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**		**Area inventario e magazzino**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore* *7 Destinatario* *8 Codice fiscale destinatario* *9 Partita iva destinatario* *10 Annotazioni* *11 Data scarto (gg/mm/aaaa)*** *12 Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

18	**TIPOLOGIA DOCUMENTALE**	**Area fornitori ed acquisti**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**	**Area fornitori ed acquisti**
1.2	**Natura di documento informatico amministrativo**	NO

1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore* *7 Destinatario* *8 Codice fiscale destinatario* *9 Partita iva destinatario* *10 Annotazioni* *11 Data scarto (gg/mm/aaaa)*** *12 Scarto in anni (zero=perpetuo)***
1.6	**Presenza di fascicolo informatico o aggregazione documentale**	NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**	
1.8	**Durata di conservazione richiesta**	10 anni
1.9	**Formato del file**	Vedi tabella formati ammessi
1.10	**Frequenza conservazione**	Annuale

19	**TIPOLOGIA DOCUMENTALE**	**Area consiglio di istituto**
1.1	**Codice della tipologia nel Sistema di conservazione LegalSolutionDOC**	**Area consiglio di istituto**
1.2	**Natura di documento informatico amministrativo**	NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**	NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.

1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore* *7 Destinatario* *8 Codice fiscale destinatario* *9 Partita iva destinatario* *10 Annotazioni* *11 Data scarto (gg/mm/aaaa)*** *12 Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

20	**TIPOLOGIA DOCUMENTALE**		**Area consiglio di classe**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**		**Area consiglio di classe**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore*	

		7 *Destinatario* *8* *Codice fiscale destinatario* *9* *Partita iva destinatario* *10* *Annotazioni* *11* *Data scarto (gg/mm/aaaa)*** *12* *Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

21	**TIPOLOGIA DOCUMENTALE**		**Area giunta esecutiva**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**		**Area giunta esecutiva**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*11* *Anno di riferimento*** *2* *Tipo documento*** *3* *Oggetto*** *4* *Produttore*** *5* *Codice fiscale produttore*** *6* *Partita iva produttore* *7* *Destinatario* *8* *Codice fiscale destinatario* *9* *Partita iva destinatario* *10* *Annotazioni* *11* *Data scarto (gg/mm/aaaa)*** *12* *Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO

1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**	
1.8	**Durata di conservazione richiesta**	10 anni
1.9	**Formato del file**	Vedi tabella formati ammessi
1.10	**Frequenza conservazione**	Annuale

22	**TIPOLOGIA DOCUMENTALE**		**Area ufficio di presidenza**
1.1	**Codice della tipologia nel Sistema di c onservazione LegalSolutionDOC**		**Area ufficio di presidenza**
1.2	**Natura di documento informatico amministrativo**		NO
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO NO. E' onere del produttore provvedere alla firma del documento a meno che non richieda nella Richiesta di Attivazione di usufruire del servizio di formazione.
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da LegalSolutionDOC (nella fase di formazione)**		NO
1.5	**Metadati****	*1 Anno di riferimento*** *2 Tipo documento*** *3 Oggetto*** *4 Produttore*** *5 Codice fiscale produttore*** *6 Partita iva produttore* *7 Destinatario* *8 Codice fiscale destinatario* *9 Partita iva destinatario* *10 Annotazioni* *11 Data scarto (gg/mm/aaaa)*** *12 Scarto in anni (zero=perpetuo)***	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		NO
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		
1.8	**Durata di conservazione richiesta**		10 anni
1.9	**Formato del file**		Vedi tabella formati ammessi
1.10	**Frequenza conservazione**		Annuale

***Il metadato è richiesto dalla normativa di cui al D.P.C.M. 3 dicembre 2013 (allegato 5, cap. 3 Metadati minimi del documento amministrativo informatico) nel caso della conservazione di documenti amministrativi informatici.*

La scelta di valorizzare il predetto campo metadato è di esclusiva responsabilità del titolare dei documenti (pubblica amministrazione). Il Conservatore non esegue alcun controllo di corretta valorizzazione, avviando conseguentemente il processo di conservazione con i dati ricevuti o meno dalla pubblica amministrazione.

Si ricorda che il Servizio prevede esclusivamente l'erogazione della fase di Conservazione dei Documenti Informatici e, se richiesto dal Cliente, l'erogazione della fase di formazione con le modalità specificate al paragrafo 13.4 (apposizione della firma digitale automatica del Cliente ovvero del delegato alla firma digitale che abbia poteri di firma in rappresentanza della società).
È esclusiva responsabilità del Cliente:
- provvedere nei casi previsti e secondo propria valutazione all'apposizione della firma digitale o di altre tipi di firme sul singolo Documento per garantire l'autenticità dell'origine e l'integrità del contenuto ai Documenti Informatici;
- provvedere a garantire il corretto completamento della generazione della copia informatica e/o della copia per immagine ai sensi dell'art. 4 del DM 17 giugno 2014;
- provvedere a garantire le disposizioni dell'art. 2215-bis del Codice Civile.

Il produttore dei documenti deve adeguarsi al seguente elenco dei formati ammessi, che il sistema di conservazione LegalSolutionDOC verifica nella fase di presa in carico per l'accettazione e l'individuazione dello specifico Mimetype.

Formato del file	Proprietario	Estensione	Standard	Tipo Mime	Visualizzatore	Produttore del visualizzatore
PDF	Adobe Systems www.adobe.com	.pdf	ISO32000-1	application/pdf	Adobe Reader	Adobe Systems - www.adobe.com
PDF/A	Adobe Systems www.adobe.com	.pdf	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)	application/pdf	Adobe Reader http://www.pdfa.org/doku.php	Adobe Systems - www.adobe.com
XML	W3C	.xml		application/xml text/xml	Mozilla Chrome Internet Explorer	Firefox Google Microsoft
TXT	Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata	.txt			Mozilla Chrome Internet Explorer	Firefox Google Microsoft

TIFF	Aldus Corporation in seguito acquistata da Adobe	.tif		image/tiff	Vari visualizzatori di immagini	
JPG	Joint Photographic Experts Group	.jpg .jpeg	ISO/IEC 10918:1	image/jpeg	Vari visualizzatori di immagini	Per maggiori informazioni sul formato www.jpeg.org
EML	Vari	.eml	RFC2822		Client di posta elettronica supportano la visualizzazione di file eml	Vari
OOXML	Microsoft	.docx .xlsx .pptx	ISO/IEC DIS 29500:2008			Tale formato deve garantire alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML
ODF	Consorzio OASIS OpenOffice.org	.ods .odp .odg .odb	ISO/IEC 26300:2006	application/vnd.oasis.opendocument.text		www.oasis-open.org

In tutti i casi riportati in tabella, il produttore dei documenti s'impegna a versare al sistema di conservazione LegalSolutionDOC documenti privi di codici eseguibili o macro istruzioni o privi di qualsiasi causa, anche non visibile all'utente, che ne possa alterare il contenuto.
Resta inteso che sui documenti oggetto del servizio di conservazione, i cui possibili formati sono stati specificati nella tabella, il Cliente può apporre una firma digitale nei formati CAdES, PAdES e XAdES

12 STRUTTURA DATI DEL PACCHETTO DI VERSAMENTO

La struttura dei Pacchetti di Versamento trasmessi dal Produttore dei documenti al Sistema di Conservazione è conforme a quanto disposto dalle Regole tecniche sul sistema di conservazione ovvero dallo Standard ISO 14721:2012 OAIS.
Il Pacchetto di Versamento (PdV) del Sistema di conservazione LegalSolutionDOC è costituito da un contenitore (archivio) nel formato non compresso o compresso (zip, rar, ecc.), costituito da:

- i documenti oggetto della conservazione (*Content Information*), il cui formato deve essere coerente con le specifiche contenute nell'allegato 2 delle Regole tecniche sul sistema di conservazione (i formati idonei per la conservazione a lungo termine dei documenti informatici sono specificati nel paragrafo *Controlli di coerenza sui Pacchetti di Versamento*). I documenti sono inseriti all'interno di una cartella (quindi un contenitore, ad esempio in una cartella denominata *Files*);

- l'Indice del Pacchetto di Versamento (IPdV), ovvero le *Preservation Description Information*, finalizzato alla descrizione dell'oggetto della conservazione (l'indice è un file strutturato in formato XML nel quale sono inserite tutte le informazioni riguardanti i metadati dei documenti e i dati del Produttore); le specifiche per la generazione del file Indice sono descritte nel documento *LegalSolutionDOC SDK* (allegato alla presente Scheda Servizio) e sono conformi allo standard UNI SInCRO 11386:2010. Il file IPdV è inserito a livello principale all'interno del pacchetto Archivio. Questo file, prima di essere aggiunto all'interno di un PdV, può essere firmato digitalmente dal produttore dei documenti.

Ogni PdV può contenere quindi i documenti oggetto della conservazione e un Indice del Pacchetto di Versamento riferiti ad una classe documentale e ad un soggetto Produttore dei documenti.

13 TRASMISSIONE E PRESA IN CARICO DEI PACCHETTI DI VERSAMENTO

I Pacchetti di Versamento possono essere trasmessi al Sistema di conservazione tramite dialogo applicativo web service (protocollo SOAP 1.2) oppure mediante il protocollo sFTP collegandosi agli URL di seguito specificati ed accedendo tramite le credenziali rilasciate da 2C Solution tramite PEC ai referenti indicati nella presente Scheda Servizio.

Web Service (test)	https://testsdc2csolution.solutiondocondemand.com/Repositoryservice.svc
Web Service (produzione)	https://sdc2csolution.solutiondocondemand.com/Repositoryservice.svc
sFTP (test)	sftp:// testsdc2csolution.solutiondocondemand.com
sFTP (produzione)	sftp://sdc2csolution.solutiondocondemand.com

13.1 Trasmissione dei Pacchetti di Versamento tramite web service e modalità di presa in carico da parte del Sistema di conservazione

13.1.1 Pacchetti di Versamento trasmessi direttamente tramite chiamate al Web Service del Sistema di conservazione

La trasmissione dei Pacchetti di Versamento attraverso richieste direttamente al Web Service del Sistema di Conservazione avviene secondo il processo descritto nel documento *LegalSolutionDOC SDK* (allegato alla presente Scheda Servizio) e richiede che l'applicazione che effettua la chiamata sia in possesso delle credenziali di accesso comunicate tramite PEC da 2C Solution al referente specificato nella presente Scheda Servizio.

Il Servizio 2C Solution prevede che il referente riceva credenziali diverse per il versamento dei Pacchetti di collaudo e dei Pacchetti di produzione.
Nell'ambito di una singola chiamata al web service del Sistema di Conservazione è possibile trasferire un Pacchetto di Versamento la cui dimensione non superi **20 MB**.
Al termine delle sessioni di versamento effettuate il Sistema risponde comunicando l'ID univoco di presa in carico e l'esito dei controlli effettuati sui Pacchetti di Versamento (che sono specificati nella presente Scheda Servizio).
Gli esiti di presa in carico successivi alla trasmissione dei Pacchetti di Versamento tramite web service sono quindi i seguenti:

- **ID** assegnato al Pacchetto di Versamento dal Sistema di Conservazione (GUID), se il caricamento è stato eseguito correttamente;
- **Eccezione**, se si sono verificati degli errori durante l'invocazione del Web Service.

13.1.2 Pacchetti di Versamento trasmessi dall'area temporanea di archiviazione logicamente separata dal Sistema di conservazione

Il Produttore dei documenti che utilizza l'area temporanea di archiviazione logicamente separata dal Sistema di conservazione LegalSolutionDOC archivia i documenti con le seguenti modalità:

- attraverso **pagina web**, mediante il caricamento dei file (tramite la funzionalità di Sfoglia/drag and drop) ed inserimento manuale dei metadati e successiva archiviazione;
- attraverso **stampante virtuale** integrata con l'area temporanea di archiviazione attraverso protocollo web service; mediante la stampante virtuale è possibile catturare da spool di stampa i documenti stampati da qualsiasi applicativo, convertirli in formato PDF ed archiviarli previo inserimento dei metadati richiesti;
- **Remote Client**, applicazione che attraverso il dialogo su web service consente di navigare sui documenti archiviati nell'area temporanea di archiviazione: integra la possibilità di archiviare documenti con il semplice drag and drop dei file nelle cartelle di archivio previo inserimento dei metadati richiesti;
- **Monitoraggio cartelle**: l'area temporanea di archiviazione integra un motore di acquisizione basato su batch schedulati che, effettuando un *polling* su cartelle predefinite, prendono in carico i documenti e li elaborano anche con tecnologie quali barcode recognition, OCR e OMR con l'ausilio di basi dati a supporto, effettuando l'indicizzazione e la successiva archiviazione.

Presso l'area temporanea di archiviazione sono generati periodicamente – secondo le regole definite dal Produttore dei documenti – i Pacchetti di Versamento contenenti i documenti archiviati ovvero gli Indici dei Pacchetti di Versamento generati secondo le specifiche conformi al DPCM 3 dicembre 2013 e al modello di riferimento OAIS norma ISO 14721:2012. Tali Pacchetti di Versamento sono trasmessi al Sistema di conservazione mediante canale web service: nell'area temporanea di archiviazione è tenuta traccia dello stato di invio dei documenti e dei metadati ad essi associati.

13.2 Controlli di coerenza sui Pacchetti di Versamento

Nel processo di presa in carico dei Pacchetti di Versamento nel Sistema di conservazione, il Servizio LegalSolutionDOC effettua una serie di controlli di coerenza su ciascun PdV e sugli oggetti in esso contenuti e genera un esito di presa in carico.

I controlli eseguiti dal Sistema sui PdV trasmessi sono i seguenti:

- (**Bloccante**) Verifica che il pacchetto di versamento contenga l'IPdV ed i files (non viene effettuato dal metodo web services checkIndicePdV);
- (**Bloccante**) Controllo validità del file IPdV con il file schema XSD;
- (**Bloccante**) Controllo che il soggetto che ha formato ed è titolare dei documenti definito nell'IPdV sia presente e configurato nel Sistema di Conservazione e che per questo soggetto ci sia un soggetto Responsabile della Conservazione configurato nel sistema;
- (**Bloccante**) Controllo che il numero di files presenti nel PdV corrisponda al numero di files dichiarati nell'IPdV (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
- (**Bloccante**) Controllo che i nomi dei files presenti nel PdV corrisponda ai files definiti nell'IPdV (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
- (**Bloccante**) Controllo che il MimeType dei files definito nell'IPdV sia stato specificato;
- (**Bloccante**) Verifica che i formati dei files contenuti nel PdV siano nei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013 e dalla tabella di seguito riportata

Tipo file	Tipo MIME	Codifica	Note
PDF, PDF/A	application/pdf, application/x-pdf, application/x-bzpdf, application/x-gzpdf	Binario	
TIFF	image/tiff, image/tiff-fx	Binario	
JPG-JPEG	image/jpeg	Binario	
TXT	text/plain	8 bit	
EML (Messaggio di Posta elettronica)	RFC 2822/MIME (text/plain, message/rfc822, multipart/alternative, text/html)	8 bit	
XML	application/xml, text/xml	8 bit	
ODT	application/vnd.oasis.opendocument.text	Binario	
FODT	application/vnd.oasis.opendocument.text	Binario	
DOCX	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Binario	
ODS	application/vnd.oasis.opendocument.spreadsheet	Binario	
FODS	application/vnd.oasis.opendocument.spreadsheet	Binario	
XLSX	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Binario	
ODP	application/vnd.oasis.opendocument.presentation	Binario	
FODP	application/vnd.oasis.opendocument.presentation	Binario	
PPTX	application/vnd.openxmlformats-officedocument.presentationml.presentation	Binario	
ODG	application/vnd.oasis.opendocument.graphics	Binario	
FODG	application/vnd.oasis.opendocument.graphics	Binario	

- (**Bloccante**) Verifica della presenza di files nell'IPdV con Id documento NON specificato;
- (**Bloccante**) Verifica della presenza di files nell'IPdV con lo stesso Id documento;
- (**Bloccante**) Se l'IPdV è firmato il sistema verifica che la firma sia valida, se non è firmato NON lo verifica (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV).

Per ogni documento definito nell'IPdV si effettuano i seguenti controlli:

- (**Bloccante**) Verifica che la tipologia definita per il documento corrisponda a quella definita per l'IPdV (campo: SourceVdA);
- (**Bloccante**) Verifica che il numero di metadati definiti per il documento corrisponda a quelli definiti all'interno della tipologia configurata nel sistema di conservazione (definita nell'IPdV nella sezione SourceVdA);
- (**Bloccante**) Verifica che il nome e l'ordine dei metadati definiti per il documento corrisponda a quanto definito all'interno della tipologia configurata nel sistema di conservazione (definita nell'IPdV nella sezione SourceVdA);
- (**Bloccante**) Verifica della presenza del valore per i metadati obbligatori, seguendo lo schema dei metadati (inserito nel PdV nella sezione SourceVdA);
- (**Bloccante**) Validazione del valore per i metadati in base all'eventuale espressione regolare definita, seguendo lo schema dei metadati (inserito nel PdV nella sezione SourceVdA);
- (**Bloccante**) Verifica che non ci siano documenti con lo stesso Id documento, all'interno del Sistema di Conservazione, per la tipologia associata all'azienda;
- (**Bloccante**) Verifica degli Hash dei file con il valore inserito nel PdV (Il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
- (**Bloccante**) Verifica della validità della firma sul file (opzionale); il predetto controllo non viene effettuato dal metodo web services checkIndicePdV.

Se le verifiche di coerenza eseguite nella fase di presa in carico sono positive il PdV viene preso in carico dal Sistema di conservazione, altrimenti l'esito di presa in carico ne evidenzia il rifiuto definitivo.

In caso di presa in carico, il sistema di conservazione LegalSolutionDOC esegue, con una schedulazione periodica il cui timing è configurabile per ciascun produttore dei documenti, eventuali ulteriori controlli di continuità (se previsti nella presente Scheda Servizio) e genera un rapporto, il **Rapporto di Versamento** (RdV), quale esito di tutte le verifiche effettuate sul PdV a partire dalla sua ricezione.

Nella fase di verifica di coerenza del PdV, i risultati dei controlli vengono tutti registrati all'interno della funzionalità di LOG Management System del Sistema.

13.3 Apposizione della firma digitale sui documenti presi in carico con esito positivo dal Sistema di conservazione

Nel caso delle tipologie documentali, specificate nella Richiesta di attivazione, per le quali è prevista l'apposizione della firma digitale, nella fase di formazione, su ciascun singolo documento, il Cliente soggetto produttore dei documenti versa al Conservatore 2C Solution S.r.l. un pre-Pacchetto di Versamento (pPdV) contenente l'IPdV e i documenti oggetto della conservazione non firmati.
In caso di esito positivo dei predetti controlli di coerenza effettuati dal Sistema di conservazione, 2C Solution S.r.l. appone sui documenti la firma del titolare dei documenti specificato nella Richiesta di attivazione e genera un diverso PdV contenente i documenti firmati ed un nuovo IPdV, nel quale è riportato l'hash del documento non firmato (dichiarato dal Cliente nell'IPdV contenuto nel pPdV) ed il nuovo hash del documento firmato.

Il nuovo PdV generato da 2C Solution S.r.l., contenente i documenti versati dal Cliente mediante il versamento del pPdV e firmati dal titolare dei documenti attraverso la procedura descritta, è quindi versato al Sistema di conservazione.
In caso di esito positivo dei controlli di coerenza effettuati dal Sistema di conservazione sul PdV versato da 2C Solution S.r.l., sia l'hash del documento non firmato (*Previoushash*), sia l'hash del documento firmato, sono riportati nell'IPdA generato dal Conservatore 2C Solution S.r.l. al termine del processo di conservazione.

14 RAPPORTO DI VERSAMENTO

Il **Rapporto di Versamento** previsto dalle Regole tecniche in materia di sistema di conservazione è generato dal Sistema di conservazione esclusivamente in caso di esito positivo della presa in carico e ha lo scopo di formalizzare l'acquisizione degli oggetti da conservare inviati dal Produttore tramite un Pacchetto di Versamento. Tale rapporto può riferirsi ad uno o più Pacchetti di Versamento.

Nel Sistema di conservazione LegalSolutionDOC, la generazione del RdV, avviene tramite la schedulazione di un job all'interno dello schedulatore dei processi integrato nel Sistema di conservazione.

Per ogni Azienda Produttore dei documenti possono essere generati 1 o più RdV per ogni schedulazione, in quanto:

- ogni RdV si riferisce ad una sola tipologia documentale;
- per ogni Produttore è possibile definire il numero massimo di PdV ai quali un Rapporto di Versamento può riferirsi, per evitare la generazione di Rapporti di Versamento relativo ad un numero troppo alto di documenti e quindi con una size notevole.

Il RdV, la cui naming è univoca all'interno del Sistema di conservazione, è costituito da un file XML dove all'interno vengono riportate le seguenti informazioni:

- Versione del Sistema di Conservazione;
- Produttore dei documenti riferimento della Conservazione;
- Riferimenti dell'utente che ha trasmesso il PdV;
- Data di Generazione del RdV;
- Riferimenti del Responsabile della Conservazione associato al Produttore dei documenti;
- Numero di PdV inclusi nel RdV;
- Numero totale dei files contenuti nei PdV inclusi all'interno del RdV;
- La funzione di Hash con cui è stato generato l'hash dell'IPdV;
- Hash del/i IPdV a cui si riferiscono i RdV;
- L'indirizzo IP della macchina dove è stato generato il PdV;
- La lista dei messaggi del Responsabile della conservazione contenuti nel Pacchetto di versamento collegati al file;
- L'esito dei check una volta ricevuto il PdV da parte del Sistema di conservazione.

Di seguito è riportata la struttura del Rapporto di Versamento:

DescGenerale

- **IdSetup**, il codice cliente produttore.
- **IdAzienda**, L'identificativo univoco all'interno del sistema documentale.
- **RagSociale**, La ragione sociale/denominazione del produttore.
- **CodFiscale**, Il codice fiscale del produttore.
- **PartitaIVA**, La partita iva del produttore rappresentata con il Codice Paese e il numero di partita iva separato da ":" es. IT:04030410288.
- **IdTipologia**, Il codice della tipologia/classe documentale riferita al PdV considerato.
- **Tipologia**, Descrizione della tipologia documentale riferita al PdV considerato.
- **DataGenerazione**, La data di generazione del RdV in formato UTC.
- **RdC**, Dati del Responsabile della conservazione.
  - **Nome e Cognome/Ragione sociale,** la denominazione del Responsabile della conservazione.
  - **CodFiscale**, Codice Fiscale del Responsabile della conservazione.
  - **PartIVA**, Partita Iva del Responsabile della conservazione.
- **Delegato**, Dati del Delegato alla conservazione.
  - **Nome e Cognome/Ragione sociale,** la denominazione del Delegato alla conservazione.
  - **CodFiscale**, Codice Fiscale del Delegato alla conservazione.
  - **PartIVA**, Partita Iva del Delegato alla conservazione.
- **RespSdC**, Dati del Responsabile del Servizio di conservazione.
  - **Nome e Cognome/Ragione sociale,** la denominazione del Responsabile del Servizio di conservazione.
  - **CodFiscale**, Codice Fiscale del Responsabile del Servizio di conservazione.
  - **PartIVA**, Partita Iva del Responsabile del Servizio di conservazione.
- **SdC**, Indicazioni del sistema di conservazione che ha creato il RdV
  - **Nome**, Nome commerciale del sistema di conservazione.
  - **Versione**, Versione del sistema di conservazione.

PdVGruppo (1-n), Costituisce il gruppo di PdV considerati dal RdV.

- **PdV**
  - **Id**, Id del Pdv incluso nel Rapporto.
  - **Utente**, Dati dell'utente produttore che versato il PdV.
    - **Nome**, Nome del produttore.
    - **Cognome**, Cognome del produttore.
    - **CodFiscale**, Codice Fiscale del produttore.
    - **PartIVA**, Partita Iva del produttore.
  - **NumFiles**, Numero di File inclusi nel pacchetto di versamento.
  - **IpProduttore**, Ip del server/pc dove è stato formato il PdV.
  - **Hash** Descrizione della funzione di hash adottata per la generazione dell'impronta informatica.
    - **Tipo**, Tipo di algoritmo (ad es. SHA256).
    - **Valore**, Il valore di HASH del IPdV ottenuto in fase di presa in carico.
  - **FormatoData**, Descrizione del formato della data es. yyyy-MM-ddTHH:mm:ssK

- **Annullato**, Indica se il pacchetto di versamento è stato annullato.
- **RdCMessageGroup**, In questa sezione vengono raccolti tutti i messaggi del Responsabile della conservazione inseriti sui PdV, oppure derivati dal registro anomalie.
- **FileGroup** (1-n), Il gruppo dei file inclusi nel PdV.
  - **IdDoc**, Id Documento nel sistema documentale.
  - **PathFile**, Nome file oggetto da conservare.
  - **AnnoRiferimentoDoc**, L'anno a cui si riferisce l'oggetto da conservare.
  - **RdCMessageGroup**, Messaggi del responsabile della conservazione riferiti al file considerato.
- **CheckGroup** (1-n)
  - **Descrizione**, Descrizione del tipo di Check effettuato e la descrizione dell'esito.
  - **Esito**, può essere OK o KO.
  - **Data**, La data di esecuzione del check.

Il rapporto generato viene firmato dal responsabile della conservazione e archiviato nel sistema di conservazione.

Il Conservatore consente al cliente di ricevere/effettuare il download del Rapporto di Versamento con le seguenti modalità:

- attraverso **e-mail** configurata nel Sistema di conservazione LegalSolutionDOC , la e-mail viene formattata in modo automatico dal Sistema e in allegato viene inserito il RdV firmato dal Responsabile della conservazione e il file non firmato (per una più agevole elaborazione del file da parte di un eventuale sistema di terze parti). Viene inoltre fornito un file XSLT per la visualizzazione agevole tramite browser;
- tramite **chiamata** (da parte del Cliente) **al web service del Sistema di conservazione**, secondo le modalità specificate nel documento LegalSolutionDOC SDK (allegato alla presente Scheda Servizio);
- direttamente **dalla piattaforma web del Sistema di conservazione**, secondo le modalità specificate nel documento LegalSolutionDOC – Manuale User (allegato alla presente Scheda Servizio).

Nel caso del Cliente:

- il Rapporto di Versamento è generato dal Responsabile della Conservazione entro 24 ore dopo la presa in carico del Pacchetto di Versamento cui si riferisce;
- il Rapporto di Versamento può riferirsi ad un massimo di 100 Pacchetti di Versamento;

SE REGISTRO DI PROTOCOLLO

- il Rapporto di Versamento è generato dal Responsabile della Conservazione con uno SLA di X + 1 ora rispetto alla ricezione del PdV. Si ricorda che il Cliente è tenuto a trasmettere al Sistema di conservazione il registro giornaliero di protocollo entro la giornata lavorativa

successiva alla sua formazione (si rimanda a quanto disposto dal D.P.C.M. 3 dicembre 2013, Regole tecniche per il protocollo informatico, art. 7 c. 5). Al fine di garantire la generazione dei RdV della tipologia documentale *Registro di protocollo* entro la medesima giornata di versamento dei PdV al Sistema di conservazione, il Cliente è tenuto ad effettuare il versamento entro e non oltre le ore 12.

- il Rapporto di Versamento può riferirsi ad un massimo di 10 Pacchetti di Versamento

15 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

I documenti contenuti nei PdV presi in carico dal Sistema di conservazione sono archiviati all'interno del Sistema; la loro conservazione a norma avviene contestualmente alla generazione e alla sottoscrizione, da parte del Responsabile della Conservazione, dei Pacchetti di Archiviazione (PdA). Un PdA contiene documenti trasmessi dal Produttore all'interno di uno o più PdV e il file IPdA.

L'IPdA, conformemente a quanto disposto dall'allegato 4 del DPCM 3 dicembre 2013, è un file in formato XML associato ad ogni PdA ed è generato secondo lo standard UNI SInCRO 11386:2010. L'Indice, che è marcato temporalmente e sottoscritto dal Responsabile della Conservazione, ovvero dal Responsabile del Servizio di conservazione, attesta il corretto svolgimento del processo di conservazione e contiene in particolare:

- informazioni relative all'IPdA: identificatore univoco dell'IPdA e informazioni sull'applicazione che lo ha generato (nome e versione dell'applicazione e nome del produttore dell'applicazione);
- informazioni relative al PdA cui l'IPdA si riferisce: identificatore univoco del PdA; eventuali riferimenti ad altri PdA da cui deriva il Pacchetto; informazioni relative ai PdV contenuti nel PdA (identificatore univoco, impronta);
- informazioni relative ai file contenuti nel PdA: metadati associati ai documenti delle diverse tipologie documentarie conservate;
- informazioni relative al processo di produzione del PdA: indicazione del nome e del ruolo dei soggetti che intervengono nel processo di produzione del PdA; riferimento temporale adottato; normativa applicata per l'implementazione del processo di produzione del PdA.

16 MODALITÀ DI ACCESSO, CONSULTAZIONE ED ESIBIZIONE

L'utente può consultare le unità documentarie versate nel Sistema di conservazione mediante interfaccia web collegandosi all'indirizzo https://legal.solutiondocondemand.com e autenticandosi tramite le credenziali di accesso (username e password) fornite da 2C Solution s.r.l.
Gli utenti da abilitare per l'accesso tramite interfaccia web al Sistema di conservazione sono indicati nella Richiesta di Attivazione.

L'accesso web consente all'utente di poter eseguire tutte le funzionalità di ricerca, consultazione ed esibizione descritte nel manuale di conservazione ed in particolare nel documento **LegalSolutionDOC – Manuale User**.

Le funzionalità di ricerca permettono all'utente di richiedere l'estrazione di un PdD.

Un PdD consiste in un file in formato ZIP che contiene:

- I **documenti** (oggetti digitali conservati nel sistema) richiesti dall'Utente.
- **Uno o più files IPdA** associati ai predetti documenti richiesti dall'Utente; tali file, che garantiscono l'interoperabilità, sono firmati digitalmente dal Responsabile della Conservazione e marcati temporalmente.
- **File indice del PdD (IPdD)**: file XML conforme allo standard UNI SINCRO 11386:2010 e firmato digitalmente dal Responsabile della Conservazione, che contiene l'hash dell'IPdA, l'hash di ogni singolo file (documento richiesto o presente all'interno di un PdV richiesto) e della Super Impronta (se presente).
- La **Super Impronta** (opzionale, se presente) generata per il produttore (Azienda) a cui si riferiscono i documenti (ad esempio presente per tutti i documenti con rilevanza tributaria oggetto di conservazione, propedeutica alla comunicazione dell'impronta dell'Archivio secondo il Provvedimento Attuativo Agenzia delle Entrate n. 2010/143663 del 25 ottobre 2010, abrogato con l'entrata in vigore del DM 17 Giugno 2014).

Per ogni PdD generato viene archiviato il file indice (IPdD) all'interno del Sistema di conservazione, per la tracciatura formale delle richieste di documenti da LegalSolutionDOC. Questo file indice contiene al suo interno:

- **Id del PdD**, generato in seguito al salvataggio su Data Base;
- **Data** della **generazione** del **PdD** (in formato UTC);
- **Produttore** (Azienda) a cui si riferisce il PdD (Rag. Sociale, Id setup, Id azienda, Cod. Fiscale, Partita IVA);
- L'**utente che ha richiesto il PdD** (Nome, Cognome, Codice Fiscale e/o Partita IVA);
- **Responsabile della Conservazione** (Nome, cognome, Cod. Fiscale e/o Partita IVA);
- L'indirizzo **IP da cui è arrivata la richiesta di generazione**;
- **PdA consegnati** (Id PdA, Hash, Funzione di hash utilizzata, Uri file nel Sistema di conservazione e nel PdD);
- La **lista dei file richiesti** (Id documento, Id tipologia, Nome tipologia, Nome file, Hash file, Funzione di hash utilizzata, Uri file nel Sistema di conservazione e nel PdD).

17 PROCEDURA DI SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

Scaduto il periodo di conservazione di pacchetti e documenti concordato tra Produttore dei documenti e Conservatore nella presente Scheda Servizio, il sistema LegalSolutionDOC deve implementare la procedura di scarto dei pacchetti di archiviazione, al fine di rispettare il principio di necessità.
Il sistema notifica al produttore (via mail/pec), con 30 gg di anticipo rispetto alla predetta scadenza, l'avvio della funzionalità di scarto per determinati PdA dandone quindi informativa secondo la normativa vigente e fornendo le informazioni necessarie al produttore per valutare l'eventuale richiesta di estensione del periodo di conservazione.
In caso di superamento della scadenza prefissata ed in assenza di richiesta di estensione, il job della procedura di scarto si attiva e produce dei Pacchetti di Scarto (PdS) in relazione ai PdA oggetto della procedura. L'operazione è tracciata nel sistema e viene prodotto un file Indice del Pacchetto di Scarto (IPdS) nel formato UNI SInCRO 11386:2010 firmato digitalmente dal Responsabile della

Conservazione che grazie al file XSLT può essere visualizzato dal Produttore dei documenti o altri soggetti interessati per la verifica della corretta procedura eseguita.
Nel sistema LegalSolutionDOC, inoltre, viene registrato se la gestione della procedura di scarto è relativa ad archivi pubblici o privati che rivestono interesse storico particolarmente importante; in questo caso si attiva un alert e la procedura di scarto del pacchetto di archiviazione avviene solo previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia e secondo gli accordi definiti nella "Scheda Servizio Cliente – Specificità del Contratto".

18 CESSAZIONE DEL SERVIZIO

In caso di cessazione del servizio le caratteristiche dei pacchetti informative e le procedure del sistema di conservazione LegalSolutionDOC permettono al Produttore di garantire l'interoperabilità in caso di migrazione (way out) ad altro sistema di conservazione.
Il Produttore ha la possibilità di recuperare tutti i pacchetti di distribuzione tramite chiamate web service o tramite richiesta dei propri utenti autorizzati dall'interfaccia web.

19 SERVICE LEVEL AGREEMENT (SLA)

2C Solution conserverà i documenti ricevuti con uno SLA pari a X + 30 giorni dove X è la data ed ora di versamento dal Cliente al conservatore.
In caso di presenza di anomalie del PdV e quindi di scarto dell'intero pacchetto, il cliente procede ad un nuovo invio e quindi sarà rispettato un nuovo SLA di erogazione del servizio.
Nel calcolo dei predetti SLA vengono considerati esclusivamente i giorni lavorativi. In caso di esito negativo verrà data comunicazione al Cliente, tramite email o PEC indicata nel contratto, che avrà X giorni lavorativi per intervenire e rimuovere l'anomalia segnalata e comunque entro il giorno prima del termine di scadenza del processo di Conservazione previsto per legge per quella tipologia documentale (La gestione degli errori potrà avvenire manualmente oppure tramite procedura informatica Workflow indicata da 2C SOLUTION). Qualora il Cliente non abbia rimosso lo stato di anomalia segnalato e l'anomalia stessa non precluda il buon esito del processo di Conservazione digitale, il Conservatore è autorizzato ad avviare e completare ugualmente il processo suddetto. Il Fornitore e i soggetti da esso delegati alla conservazione non potranno essere ritenuti responsabili della mancata rimozione da parte del Cliente della situazione di anomalia segnalata.

20 OBBLIGHI

20.1 Definizione degli aspetti contrattuali e delle responsabilità

- Finalizzazione del contratto di servizio e relativi allegati, inclusa la presente Scheda Servizio Cliente – Specificità del Contratto. La sottoscrizione del contratto deve essere conclusa tra le parti prima dell'avvio in produzione.
- Il Cliente si impegna a nominare il Responsabile della Conservazione il quale nomina 2C Solution s.r.l., quale delegato alla Conservazione nonché a nominare 2C Solution Srl Responsabile esterno del Trattamento dei dati, acquisite le informazioni ai sensi dell'art. 13 D.Lgs. 196/2003
- In caso di conservazione del Libro Unico del Lavoro (LUL) deve essere tenuto fisicamente il pacchetto di distribuzione presso il Produttore mediante download dal portale LegalSolutionDOC.

- Il cliente si obbliga a versare nel perimetro di 2C Solution pacchetti di documenti e dati privi di dati personali sensibili (ad esempio dati che possono rilevare lo stato di salute e le convinzioni religiose delle persone) e di dati giudiziari (ovvero dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale). In caso di presenza di documenti e dati che per legge necessitano di un trattamento riservato il Cliente deve dichiararlo a 2C Solution all'inizio del progetto (nella fase preliminare) ed il requisito va riportato nella presente Scheda Servizio con la condivisone degli eventuali impatti sul servizio.

20.2 Adempimenti prescritti dalla Legge in carico all'azienda Produttore (ambito tributario)

- Assolvimento dell'imposta di bollo sul documento informatico come ad esempio nel caso di conservazione del libro giornale e/o del libro inventario (art. 6 DMEF 17 giugno 2014) tramite pagamento con F24 da effettuarsi in un'unica soluzione entro 120 giorni dalla chiusura dell'esercizio. È il Cliente a dover gestire in autonomia l'assolvimento e nel caso di libri e registri l'imposta è dovuta ogni 2.500 registrazioni o frazioni di esse, dove per registrazione s'intende il singolo accadimento contabile (ad esempio nel libro giornale il singolo accadimento contabile è l'operazione contabile registrata senza considerare le righe di dettaglio). Le fatture elettroniche relative ad operazioni non assoggettate ad IVA e di importo superiore a € 77,47 sono soggette all'imposta di bollo di cui sopra. È il Cliente a dover gestire in autonomia l'assolvimento dell'imposta di bollo riportando nella fattura specifica annotazione dell'assolvimento del DM 17 giugno 2014. Il pagamento dell'imposta, tramite modello F24 e codice tributo "2501", deve essere effettuato in un'unica soluzione entro 120 giorni dalla chiusura dell'esercizio.
- Comunicazione (nella dichiarazione dei redditi relativa al periodo di imposta di riferimento) della conservazione in modalità elettronica dei documenti rilevanti ai fini tributari (art. 5, comma 1, DMEF 17 giugno 2014), come previsto nel modello dichiarativo di riferimento (ad esempio UNICO SC-Società di Capitale).
- Comunicazione all'IVASS almeno 60 gg prima dall'avvio del processo di trasferimento e conservazione dei registri presso un soggetto terzo. La comunicazione dovrà contenere l'elenco dei documenti che l'impresa intende trasferire con l'indicazione del periodo a cui si riferiscono, il nuovo indirizzo di tenuta e luogo di conservazione dei documenti e le motivazioni del trasferimento. La comunicazione all'ISVAP è dovuta, anche per i libri e registri prescritti dal codice civile, da leggi tributarie o da altre leggi speciali, diversi dai registri assicurativi (Regolamento ISVAP n. 27 del 4 ottobre 2008 e s.m.i.).

Data

Per accettazione e presa visione

AXIOS ITALIA SERVICE S.R.L.

PER LE SUCCESSIVE MODIFICHE E NUOVE VERSIONI

*****Si richiede al Cliente di inviare il seguente testo:

Il sottoscritto …, a nome del Cliente …, con riferimento al Servizio di conservazione erogato da 2C Solution S.r.l. e conformemente a quanto richiesto dalla Scheda Servizio Cliente – Specificità del contratto, comunica l'accettazione della Scheda Servizio-Specificità del contratto (versione … emessa in data gg/mm/aaaa).

Allegato 20 – Manuale di conservazione del Conservatore

Il manuale della conservazione del Conservatore 2c Solution è riportato di seguito.
Il manuale è anche pubblicato nell'elenco dei Conservatori Accreditati sul sito istituzionale dell'Agenzia per l'Italia Digitale (AgID) www.agid.gov.it

Manuale della Conservazione

DI

Indice del documento

Lista di revisione		
Rev.	Data	Descrizione della modifica
1.0	30/01/2015	Prima emissione secondo lo schema del manuale AgID per l'accreditamento ai sensi dell'art.44 bis del CAD
1.1	11/04/2015	Correzione dei numeri di pagina da pagina 46, correzioni di forma su organigramma, aggiunta specifica sul trattamento in Conservazione a norma del RdV. Aggiunti i riferimenti normativi per lo scarto dei documenti per gli enti di notevole interesse storico, aggiunti i riferimenti alla gestione dei log nel paragrafo 10 e tutte lo sottosezioni. Modificata la nomenclatura del file IPdA per la compliance allo standard UNI SInCRO 11386:2010. Verifica sulla nomenclatura e definizione del Responsabile del Servizio di Conservazione.
1.2	24/11/2015	Modifica e aggiornamento nella struttura dati dei pacchetti PdA. Eliminata la necessità di inserire una distinta di versamento per il trasferimento de PdV tramite FTP, modifiche varie nel testo.
1.3	22/01/2016	Riorganizzata la numerazione dei capitoli secondo quanto previsto dallo schema di manuale di conservazione v.2 AgID. Aggiunto il link "torna al sommario" su tutti i paragrafi. Inserimento di descrizione definita come "didascalia" per ogni figura. Verificata la compliance per l'accessibilità

	Data	Nominativo	Funzione
Redazione	16/11/2015	Davide Coletto	Responsabile del servizio di conservazione – Responsabile dello sviluppo e della manutenzione del sistema di conservazione – Legale Rappresentante
Verifica	17/11/2015	Enrico Checchin	Responsabile della funzione archivistica di conservazione - Responsabile del trattamento dei dati personali
Verifica	20/11/2015	Mario Veltini	Responsabile della sicurezza dei sistemi per la conservazione - Responsabile dei sistemi informativi per la conservazione
Approvazione	22/01/2016	Davide Coletto	Responsabile del servizio di conservazione – Responsabile dello sviluppo e della manutenzione del sistema di conservazione – Legale Rappresentante

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente Manuale della Conservazione del sistema *LegalSolutionDOC*, erogato e gestito da 2C Solution SRL, è adottato secondo le disposizioni dell'art. 8 del DPCM 3 dicembre 2013.

Il documento illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, le procedure, 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.

Il predetto documento e gli eventuali ulteriori documenti rilasciati quali "specifiche forniture del servizio di conservazione" sono custoditi presso la sede del Conservatore 2C Solution SRL. Il documento è identificato attraverso il livello di revisione e la data di emissione. Il Conservatore esegue periodicamente un controllo di conformità del processo di erogazione del servizio di conservazione e, ove necessario, aggiorna il documento in oggetto anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

Il Manuale della Conservazione, depositato e pubblico presso l'Agenzia per l'Italia Digitale, è un documento informatico prodotto nel formato PDF/A, su cui è apposta la firma digitale del Responsabile del Servizio di Conservazione e Rappresentante Legale ed è conservato secondo le disposizioni della normativa vigente, al fine di assicurarne l'origine, la data certa e l'integrità del contenuto dalla sua emissione e per tutto il periodo di conservazione.

Il presente Manuale della Conservazione è collegato ai documenti riportati nella successiva tabella, che entrano più nel dettaglio in diversi aspetti del sistema e del servizio di conservazione e costituiscono parti integranti e sostanziali del Manuale della Conservazione.

Documenti collegati	
Specificità del Contratto	Rappresenta il documento che contiene le specifiche condizioni del servizio di conservazione (SPECIFICITÀ DEL CONTRATTO) ed è parte integrante e sostanziale del contratto di servizi sottoscritto tra le parti e del Manuale di conservazione. In genere denominato "Richiesta di attivazione" o "Scheda Servizio". Redatto dal Conservatore sulla base delle informazioni condivise con il Produttore dei documenti, contenente i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fasi del sevizio (attivazione, versamento, conservazione, post-produzione, distribuzione) oltre ai livelli di Servizio (SLA); tale documento è redatto in fase di analisi, prima del collaudo e della produzione del primo processo di conservazione.
Piano per la Sicurezza	Rappresenta il documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici LegalSolutionDOC da possibili rischi nell'ambito dell'organizzazione di 2C Solution.

Torna al sommario

2 TERMINOLOGIA

2.1 Glossario

Glossario dei termini	
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 dichiarazione
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento
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 che permette una loro classificazione (indicizzazione) ai fini della ricerca e consultazione
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
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticazione del documento informatico	La validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione
Autenticità	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 di dati	Collezione di dati correlati e registrati tra loro
Certificato qualificato	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva
Certification authority (CA)	Il soggetto che secondo quanto disposto dall'art. 27 del CAD presta servizi di certificazione delle firme elettroniche qualificate o che fornisce altri servizi connessi con queste ultime, quali ad esempio quello delle marche temporali

Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico
Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche
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
Comunità di riferimento	Un gruppo ben individuato di potenziali utenti che dovrebbero essere in grado di comprendere l'informazione conservata. Una comunità di riferimento può essere composta anche da più comunità di utenti
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 e descritto nel manuale di conservazione
Copia analogica del 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'art. 12 del DPCM 3 dicembre 2013
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Dispositivo sicuro per la creazione della firma:	I dispositivi sicuri per la generazione della firma qualificata che devono essere dotati di certificazione di sicurezza secondo l'art. 35 del CAD
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica

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'art. 41 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica
Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
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
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
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Formazione	l processo atto ad assicurare l'autenticità dell'origine e l'integrità del contenuto dei documenti informatici, con apposizione della firma digitale su ciascun singolo documento e/o della marca temporale ai fini di associare una data certa elettronica ove richiesto
FTP Server	Programma che permette di accettare connessioni in entrata e di comunicare in maniera sicura con un Client attraverso il protocollo FTP
Funzioni archivistiche	Funzioni per la conservazione delle informazioni (acquisizione, archiviazione, gestione dei dati, accesso, distribuzione)
Funzione di 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
Identificativo univoco	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
Identificazione informatica	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata

	attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso
IDM	Strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
Immodificabilità	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	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
Indice del Pacchetto di Archiviazione	Struttura dell'insieme dei dati a supporto del processo di conservazione, riferita allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010)
Indice del Pacchetto di Versamento	Struttura dell'insieme dei dati a supporto del processo di versamento del pacchetto di versamento (PdV), ispirata allo standard internazionale OAIS ISO 14721:2012 e definita nello specifico dal Conservatore in accordo con il produttore dei documenti
Indice del Pacchetto di Distribuzione	Struttura dell'insieme dei dati a supporto del processo di distribuzione del pacchetto di distribuzione (PdD), ispirata allo standard internazione OAIS ISO 14721:2012 e definita nello specifico dal Conservatore in accordo con il produttore dei documenti
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Log di sistema	Registrazione cronologica delle operazioni eseguite sul sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'art. 8 del DPCM 3 dicembre 2013, regole tecniche in materia di sistema di conservazione.
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
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 3 dicembre 2013

Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013 e secondo le modalità riportate nel manuale di conservazione
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Pacchetto di scarto	Pacchetto contenente i documenti da scartare dal Sistema di conservazione perché hanno raggiunto il loro termine temporale di conservazione
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
Piano per la sicurezza	È il documento aziendale che analizza il contesto in cui l'azienda opera riportando i fattori interni ed esterni che lo influenzano ed evidenzia le principali criticità legate alla gestione della sicurezza delle informazioni gestite
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
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 9 delle regole tecniche sul sistema di conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'art. 7, c. 1, del DPCM 3 dicembre 2013 e che opera presso il Produttore
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile del servizio di conservazione	Soggetto persona fisica nominato responsabile del servizio di conservazione *LegalSolutionDOC* di 2C Solution con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Responsabile della funzione archivistica di conservazione	Soggetto persona fisica nominato responsabile della funzione archivistica di conservazione *LegalSolutionDOC* di 2C Solution con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)

Responsabile del trattamento dei dati personali	Soggetto persona fisica nominato responsabile del trattamento dei dati personali del servizio di conservazione *LegalSolutionDOC* di 2C Solution con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Responsabile della sicurezza dei sistemi per la conservazione	Soggetto persona fisica nominato responsabile della sicurezza dei sistemi per la conservazione *LegalSolutionDOC* di 2C Solution con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Service Level Agreement	È l'accordo tra produttore e responsabile del servizio di conservazione sui livelli di servizio da garantire ed indica i giorni entro cui devono essere conservati i documenti nel Sistema di conservazione
Sessione di distribuzione	Sessione telematica per la consegna (distribuzione) di uno o più Pacchetti di Distribuzione dall'Ente Conservatore all'Ente Produttore, sulla base di un modello-dati per i formati ed i contenuti definito e concordato tra le parti.
Sessione di ricerca	Una sessione telematica avviata da un Utente di un sistema di conservazione, durante la quale l'Utente usa gli Strumenti di Ricerca del sistema per individuare e consultare gli oggetti digitali in esso presenti.
Sessione di versamento	Sessione telematica per la consegna (versamento) di uno o più pacchetti di Versamento dall'Ente Produttore all'Ente Conservatore, sulla base di un modello-dati per i formati ed i contenuti definito e concordato tra le parti.
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'art. 44 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
Titolare	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi
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

Torna al sommario

2.2 Acronimi

Acronimi	
AE	Agenzia delle Entrate
AgID	Agenzia per l'Italia Digitale (già DigitPA e CNIPA)
CAD	Codice dell'Amministrazione Digitale
CNIPA	Centro Nazionale per l'Informatica della Pubblica Amministrazione, ora AgID
FTP	File Transfer Protocol
SFTP	SSH File Transfer Protocol o SFTP è un protocollo di rete che prevede il trasferimento dei dati e funzionalità di manipolazione. Usato con protocollo SSH-2 per il trasferimento dei file sicuro.
IDM	Identity Management
IPA	Indice delle Pubbliche Amministrazioni
IPdA	Indice del Pacchetto di Archiviazione
IPdD	Indice del Pacchetto di Distribuzione (o Rapporto di distribuzione)
IPdV	Indice del Pacchetto di Versamento
ISO	International Organization for Standardization
OAIS	Open Archival Information System, ISO 14721:2012
PdD	Pacchetto di Distribuzione
PdS	Pacchetto di Scarto
PdV	Pacchetto di Versamento
RdV	Rapporto di Versamento
SdI	Sistema d'Interscambio per la fatturazione elettronica PA per lo scambio delle fatture e delle relative notifiche/ricevute ai sensi del DM 3 aprile 2013, n. 55
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SLA	Service Level Agreement
TSA	Time Stamping Authority
SdC	Sistema di Conservazione

Torna al sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Nel presente paragrafo è riportata la principale normativa di riferimento per l'attività di conservazione a livello nazionale, ordinata 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;

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.

Regolamento europeo eIDAS 910/2014/EC del 24 luglio 2014 – regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

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.

La normativa specifica relativa alle diverse tipologie di documenti riguardanti il contratto di erogazione del servizio di conservazione è riportata nel documento "Specificità del Contratto".

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento a cui l'attività di conservazione del Conservatore 2C Solution si riferisce, elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° ottobre 2014, come indicato nelle regole tecniche di cui al DPCM 3 Dicembre 2013.

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.

Torna al sommario

4 RUOLI E RESPONSABILITÀ

Il sistema di conservazione descritto nel presente manuale, come prescritto dall'art. 5 del DPCM 3 dicembre 2013, descrive l'adozione del modello organizzativo governato dal conservatore 2C Solution, che coinvolge soggetti, strutture e/o funzioni deputate al versamento, all'implementazione, all'erogazione del processo, alla gestione e al controllo del sistema di conservazione di documenti informatici.

Il sistema di conservazione *LegalSolutionDOC*, gestito dal Conservatore **2C Solution SRL** e dal suo Responsabile del Servizio di Conservazione, è basato su un modello organizzativo di riferimento definito formalmente nei ruoli e nelle responsabilità dei vari attori coinvolti nel processo di conservazione dei documenti informatici, come riportato nella tabella successiva, in conformità ai ruoli e alle attività ad essi associati indicati nel documento "Profili professionali" pubblicato da AgID sul proprio sito istituzionale.

Si precisa che il nominativo ed i riferimenti del Responsabile della conservazione del cliente sono indicati nell'allegato "Specificità del contratto" nel quale sono anche riportate le attività affidate al Responsabile del servizio di conservazione.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile del servizio di conservazione	Davide Coletto	Definizione ed 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.	28/01/2015
Responsabile della sicurezza dei sistemi per la conservazione	Mario Veltini	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.	28/01/2015
Responsabile della funzione archivistica di conservazione	Enrico Checchin	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni	28/01/2015

		documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove 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 del trattamento dei dati personali	Enrico Checchin	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	28/01/2015
Responsabile dei sistemi informativi per la conservazione	Mario Veltini	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; 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.	28/01/2015
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Davide Coletto	Coordinamento dello sviluppo e manutenzione delle componenti hardware e 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;	28/01/2015

	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; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Di seguito l'organigramma adottato dalla organizzazione 2C Solution per la gestione del servizio e sistema di conservazione di documenti informatici:

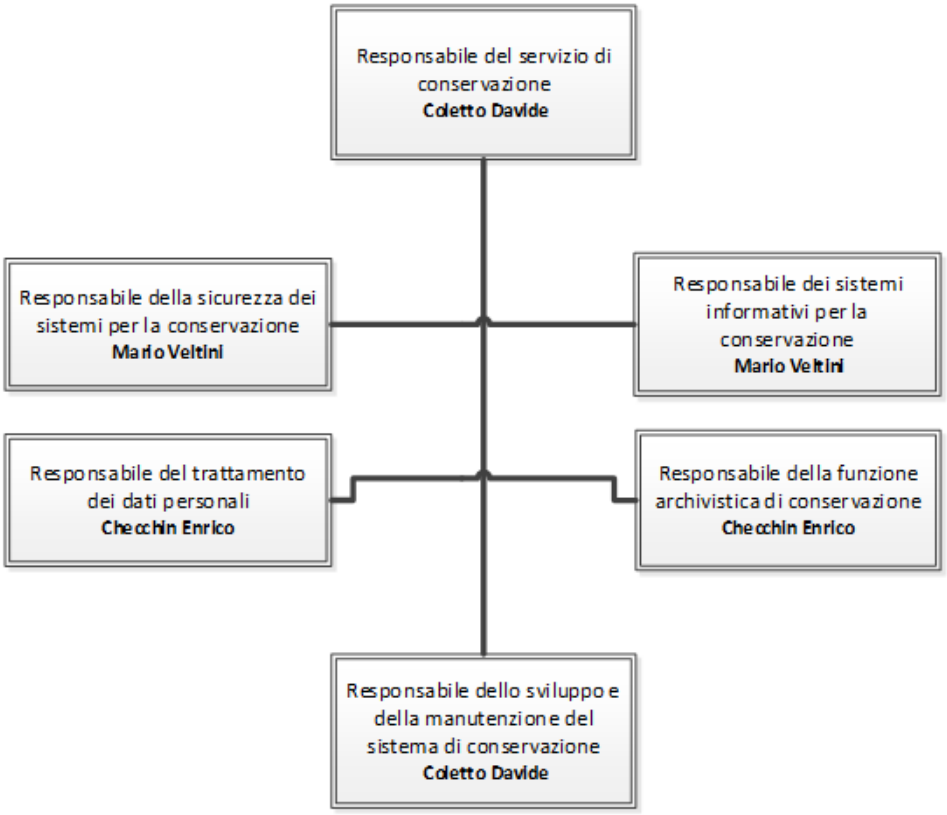

Figura 1 Organigramma del servizio e sistema di conservazione

Torna al sommario

5.2 Strutture organizzative

2C Solution considera il miglioramento continuo delle performance dei propri processi e servizi, nonché del Sistema della Sicurezza delle informazioni, uno degli strumenti strategici attraverso il quale conseguire gli obiettivi del proprio business, costituito dalla fornitura di risorse e professionalità e quindi di una struttura organizzativa a supporto per la progettazione, sviluppo, gestione, erogazione e commercializzazione dei propri servizi.

In particolare, per il servizio *LegalSolutionDOC* di conservazione di documenti informatici, 2C Solution ha certificato il proprio sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione (certificazione ISO/IEC 27001:2013), in particolare nel perimetro "Progettazione ed erogazione di servizi gestiti in modalità Saas, Paas e on premise in ambito Enterprise Content Management e paperless business (Business Process Management, acquisizione e trasmissione dei documenti, fatturazione elettronica, formazione documenti, gestione archiviazione e conservazione a Norma di documenti informatici)";

Il servizio di conservazione *LegalSolutionDOC* di 2C Solution presenta un ciclo di vita caratterizzato da tre fasi principali: *Attivazione, Esercizio e Post-Produzione*.

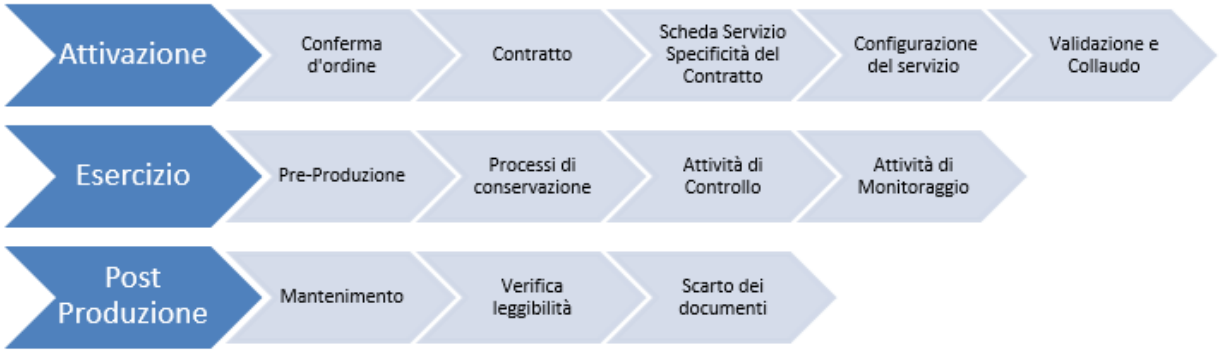

Figura 2 Ciclo di vita del Servizio di Conservazione

In ciascuna fase del servizio sono presenti sotto fasi.

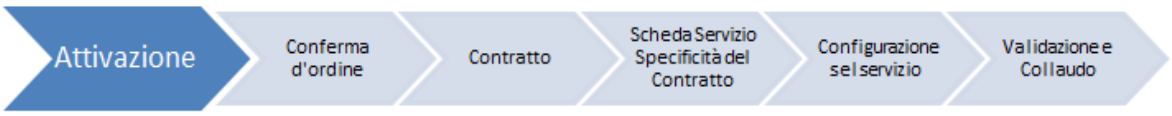

Figura 2 Fase attivazione

La fase di **Attivazione** del servizio avviene in caso di formale accettazione dell'offerta commerciale e delle condizioni contrattuali da parte del Cliente/Produttore dei documenti, inclusi gli atti di nomina sottoscritti tra le parti per svolgere il ruolo di Conservatore, Responsabile del servizio di Conservazione e Responsabile del trattamento dei dati.

L'**Area Commerciale** di 2C Solution una volta ricevuta l'offerta commerciale, provvede a comunicare l'attivazione all'ufficio amministrativo, il quale provvede alla gestione di inserimento nei sistemi informativi dell'anagrafica del cliente e la compilazione della **conferma d'ordine** da mandare al cliente.

Successivamente all'invio della conferma d'ordine al cliente, vengono attivati tramite il sistema informativo interno le attività per l'Area di Supporto che prende in carico l'attività, contatta il cliente ed avvia la predisposizione del "***Contratto***" e del documento "***Specificità del Contratto***". Quest'ultimo documento è fondamentale per l'erogazione del servizio ad un determinato Cliente/Produttore dei documenti ed è parte integrante del contratto di servizio e del manuale, redatto dal Conservatore sulla base delle informazioni condivise con il produttore dei documenti (Cliente) e contenente i requisiti essenziali del Servizio.

Successivamente alla fase di avvio formale dell'acquisizione dell'ordine, L'area supporto di 2C Solution, prende contatto con il cliente per definire eventuali pre-processi o integrazioni necessarie per il versamento dei PdV fornendo supporto al cliente.

La predisposizione della corretta definizione iniziale dei requisiti e quindi la conformità alla normativa vigente in materia di sistemi di conservazione, con anche l'individuazione degli adempimenti correlati, è assicurata in fase di analisi dalla predisposizione del **documento "Specificità del contratto",** con il controllo e la supervisione da parte del **Responsabile della funzione archivistica di conservazione**, del **Responsabile del trattamento dei dati personali** (in caso di necessità) e del **Responsabile del servizio di conservazione**, che ha in carico l'approvazione finale.

Successivamente, il processo prevede che ad ogni variazione del Servizio (Change Process), il documento Specificità del contratto debba essere aggiornato e nuovamente condiviso tra le parti.

Predisposto e condiviso il documento "Specificità del contratto", validato dal **Responsabile del servizio di conservazione di 2C Solution** e dal **Cliente**, l'area di Supporto ingaggia l'**Area di Produzione** che avvia le attività di configurazione del servizio nella piattaforma *LegalSolutionDOC.*
Prima viene eseguito un collaudo interno (verifica interna dell'**Area di Produzione delle configurazioni eseguite** in coerenza con quanto concordato nel **Documento "Specificità del Contratto"**). È poi se richiesto, si esegue il collaudo con il cliente.

Le modalità dell'eventuale collaudo sono indicatenel documento "Specificità del contratto"; a seguito dell'eventuale collaudo e della sua validazione formale da parte del cliente si procede con la successiva fase di messa in produzione (*LegalSolutionDOC Produzione*).

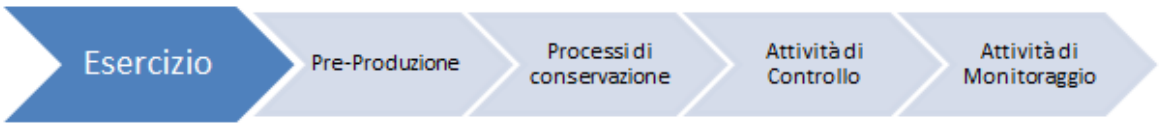

Figura 3 Fase esercizio

L'area organizzativa di **Produzione** si occupa di gestire le componenti hardware e software del servizio e di presidiare, controllare e monitorare il corretto funzionamento dei sistemi per la sua erogazione tramite l'ausilio del sistema di monitoraggio **SysAid**, report ed altri strumenti di controllo.

Inoltre, l'**Area di Produzione** presidia e gestisce gli asset di infrastruttura e la corretta esecuzione del processo, dalla fase di presa in carico, al controllo di coerenza, dalla generazione del rapporto di versamento, alla preparazione e gestione dei pacchetti di archiviazione, fino alla preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta dell'utente.

In particolare, il **Responsabile dei sistemi informativi** per la conservazione ha l'ownership delle attività di controllo degli asset e di monitorare il corretto svolgimento del servizio. In caso di riscontro di incident viene attivato il processo di gestione e risoluzione dell'incident attraverso la creazione di un ticket automatico al fine di tracciare l'accaduto e risolvere l'anomalia. Eventuali incident di rilievo e difformità sono segnalate al **Responsabile del servizio di conservazione** attraverso la procedura prevista dallo standard ISO/IEC 27001:2013.

Completato con esito positivo il processo produttivo della conservazione dei documenti, il servizio per un determinato Cliente deve essere mantenuto nel tempo anche nella fase di post-produzione, per tutta la durata contrattuale concordata, garantendo ai documenti ed ai pacchetti informativi integrità, autenticità dell'origine, leggibilità, disponibilità e reperibilità, sicurezza e riservatezza.

Figura 4 Fase Post-Produzione

Il mantenimento dei documenti e dei pacchetti generati nel processo di conservazione è garantito dalle attività dell'Area di Produzione (owner Responsabile dei sistemi informativi per la conservazione) e dall'Area di Ricerca e Sviluppo (owner Responsabile dello sviluppo e della manutenzione del sistema di conservazione) che garantiscono sia dal punto di vista infrastrutturale che applicativo il presidio e il controllo degli asset del servizio e quindi il corretto mantenimento dei documenti e dei pacchetti per tutto il periodo di conservazione concordato con il produttore dei documenti.

Durante la fase di post-produzione la struttura organizzativa del Conservatore 2C Solution, in particolare con le attività dell'Area di Assistenza e di Produzione, supporta gli adempimenti previsti dalla normativa.

Infine, scaduto il periodo di conservazione, concordato contrattualmente tra produttore, Responsabile della conservazione dei documenti e Responsabile del servizio di conservazione, viene avviata la procedura di Scarto concordata, con la produzione del Pacchetti di Scarto e la verbalizzazione dello scarto e della chiusura del servizio. Owner di queste attività sono l'**Area di Supporto e Produzione**.

Prima dell'avvio dello scarto e della procedura di chiusura del Servizio, che si conclude con un verbalizzazione dell'attività, viene comunicato al produttore l'avvio dello scarto entro 30 gg al fine di fornirgli un periodo transitorio per richiedere formalmente l'estensione (prolungamento) del periodo di conservazione. Inoltre come da disposizioni del codice dei beni culturali (D. Lgs. 22 gennaio 2004, n.42) nel caso di enti pubblici o privati dichiarati di notevole interesse storico, per effettuare lo scarto verrà richiesta l'autorizzazione preventiva alla Soprintendenza Archivistica da parte del Produttore.

Infine, in tutte le predette fasi del servizio di conservazione *LegalSolutionDOC* ed in generale in tutte le attività in carico ad un Conservatore è necessario garantire la Gestione dei sistemi informativi e della sicurezza a supporto del servizio.

Torna al sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il funzionamento del sistema di conservazione *LegalSolutionDOC* è basato sulla compliance alle regole tecniche di cui al DPCM 3 dicembre 2013 ed allo standard ISO 14721:2012 OAIS (Open Archival Information System), modello di riferimento di sistema informativo per l'archiviazione e la conservazione degli oggetti digitali.
Alla base del funzionamento del predetto modello OAIS e quindi delle regole tecniche vigenti vi è il concetto di informazione da conservare e quindi di pacchetto informativo.
Il versamento dei pacchetti (contenenti documenti e dati) al Sistema *LegalSolutionDOC* da parte di un Ente Produttore e ogni distribuzione di documenti dal Sistema ad un Utente autorizzato avvengono infatti nella forma di una o più trasmissioni distinte (sessioni) ovvero tramite lo scambio (versamento o distribuzione) di pacchetti informativi.

Il Responsabile del Servizio di Conservazione e Conservatore 2C Solution, ispirandosi ai principi dello standard OAIS, ha quindi implementato nel Sistema di Conservazione e nella fasi fondamentali del processo i pacchetti informativi intesi come contenitori astratti contenente due tipologie di informazioni:

- contenuto informativo;
- informazioni sulla Conservazione (PDI).

Contenuto informativo

L'insieme delle informazioni che costituisce l'obiettivo originario della conservazione; è un *Oggetto informativo* composto dal suo *Oggetto dati* e dalle sue *Informazioni di rappresentazione*:

- Oggetto dati: oggetto digitale composto da un insieme di sequenze di bit;
- Informazioni sulla rappresentazione: informazioni che rappresentano un Oggetto dati ovvero lo associano a concetti più significativi (es: formato). Include le Information properties, ovvero le informazioni significative che devono essere mantenute nel tempo (es.: alcuni elementi della formattazione, ecc.)

Informazioni sulla Conservazione (PDI Preservation Description Info):
Informazioni necessarie per un'adeguata conservazione del Contenuto informativo: sono fornite dai metadati e possono essere classificate in:

- *Informazioni sulla provenienza* (documentano la storia del Contenuto informativo: ad esempio forniscono informazioni sull'origine/sulla fonte del Contenuto informativo e su chi ne ha curato la custodia sin dalla sua origine).
- *Informazioni sull'identificazione* (identificano e se necessario descrivono uno o più meccanismi di attribuzione di identificatori al Contenuto informativo).
- *Informazioni sull'integrità* (informazioni che garantiscono che il Contenuto informativo non sia stato alterato senza una documentazione dell'evento).
- *Informazioni sul contesto* (informazioni che documentano le relazioni del Contenuto informativo con il suo ambiente, inclusi i motivi della creazione del Contenuto informativo e il modo in cui è in relazione con altri Contenuti informativi).
- *Informazioni sui diritti di accesso* (informazioni che possono identificare i limiti di accesso al contenuto informativo, inclusi i termini di licenza, le restrizioni legali e i sistemi di controllo).

Il Contenuto informativo e le Informazioni sulla conservazione sono incapsulati ed identificabili mediante le Informazioni sull'Impacchettamento, ovvero informazioni usate per collegare ed identificare le componenti di un pacchetto informativo (Contenuto informativo e Informazioni sulla conservazione).

Il pacchetto informativo, infine, può essere trovato nel sistema di conservazione tramite le informazioni descrittive ovvero l'insieme delle informazioni – composto essenzialmente dalla Descrizione del pacchetto – necessarie all'utente per ricercare, richiedere e recuperare le informazioni conservate dal Sistema.

Affinché la conservazione dell'oggetto informativo avvenga correttamente il Sistema *LegalSolutionDOC* è basato, quindi, su un modello che permette di identificare e comprendere l'oggetto-dati e le relative informazioni sulla rappresentazione, che contengono informazioni sia di natura sintattica che semantica.

Torna al sommario

6.1 Oggetti conservati

Nel documento "Specificità del Contratto" concordato tra Ente Conservatore 2C Solution e Ente Produttore sono elencate e descritte le tipologie di documenti sottoposte a conservazione per un determinato Produttore e le relative politiche di conservazione.
In particolare, le predette politiche di conservazione relative agli oggetti conservati riguardano per ciascuna tipologia documentale:

- la natura e l'oggetto della tipologia documentale;
- l'elenco e la descrizione dei formati (comprensivi della relativa versione) dei file utilizzati;

- l'indicazione dei visualizzatori relativi ai formati gestiti, necessari per garantire la leggibilità nel tempo dei documenti conservati;

- l'elenco e la descrizione dei metadati associati ai documenti;
- il periodo di conservazione;
- i livelli di servizio (SLA) concordati con l'ente produttore;
- altre politiche (regole) che caratterizzano il processo di conservazione.

Le tipologie di documenti che caratterizzano gli oggetti digitali da versare nel sistema di conservazione *LegalSolutionDOC* sono definite attraverso le attività di analisi e di classificazione documentale nella fase di prevendita ed attivazione del servizio.
La descrizione delle tipologie documentali, con l'indicazione della loro natura, dei formati, dei metadati obbligatori e dei metadati opzionali, delle regole e della durata di conservazione (piano di conservazione e successivo scarto) sono riportate nel dettaglio in una tabella per ciascuna tipologia nel documento allegato "–Documento - Specificità del Contratto" e sono peculiari di ciascun produttore dei documenti e di ciascuna tipologia documentale.

Di seguito si riporta un esempio di draft della tabella da compilare nella "Documento Specificità del Contratto" del Servizio *LegalSolutionDOC*

1	**TIPOLOGIA DOCUMENTALE**		**……**
1.1	**Codice della tipologia nel Sistema di conservazione *LegalSolutionDOC***		……..
1.2	**Natura di documento informatico ammini strativo**		Sì o No
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da *LegalSolutionDOC* (nella fase di formazione)**		Sì o No
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da *LegalSolutionDOC* (nella fase di formazione)**		Sì o No
1.5	**Metadati**	*In questa sezione della tabella sono inseriti tutti i metadati associati alla specifica tipologia documentale, indicandone la loro descrizione ed il loro valore (stringa, numero, data).* *Per ciascun metadato si dichiara se è un metadato "obbligatorio" in quanto richiesto dalla normativa vigente a seconda della natura della tipologia documentale ovvero in quanto richiesto dall'accordo tra ente produttore ed ente conservatore.*	
1.6	**Presenza di fascicolo informatico o aggreg azione documentale**		Sì o No
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		…..
1.8	**Durata di conservazione richiesta**		Esempio: 10 anni
1.9	**Formato del file**		…

I formati dei files contenuti nel Pacchetti di Versamento devono essere conformi all'elenco dei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013.
I formati associati alla tipologia documentale sottoposta a conservazione sono dichiarati nella tabella precedente nella fase di analisi antecedente l'attivazione del servizio *LegalSolutionDOC*.

Il produttore dei documenti deve adeguarsi al seguente elenco dei formati ammessi, che il sistema di conservazione *LegalSolutionDOC* verifica nella fase di presa in carico per l'accettazione e l'individuazione dello specifico Mimetype.

Formato del file	Proprietario	Estensione	Standard	Tipo Mime	Visualizzatore	Produttore del visualizzatore
PDF	Adobe Systems - www.adobe.com	.pdf	ISO32000-1	application/ pdf	Adobe Reader	Adobe Systems - www.adobe.com
PDF/A	Adobe Systems - www.adobe.com	.pdf	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)	application/ pdf	Adobe Reader http://www.pdfa.org/doku.php	Adobe Systems - www.adobe.com
XML	W3C	.xml		application/ xml text/xml	Mozilla - Chrome - Internet Explorer	Firefox - Google - Microsoft -
TXT	Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata	.txt			Mozilla - Chrome - Internet Explorer	Firefox - Google - Microsoft -
TIFF	Aldus Corporation in seguito acquistata da Adobe	.tif	-	image/tiff	Vari visualizzatori di immagini	
JPG	Joint Photographic Experts Group	.jpg, .jpeg	ISO/IEC 10918:1	image/jpeg	Vari visualizzatori di immagini	Per maggiori informazioni sul formato www.jpeg.org
EML	Vari	.eml	RFC2822		Client di posta elettronica supportano la visualizzazione di file eml	Vari

Formato del file	Proprietario	Estensione	Standard	Tipo Mime	Visualizzatore	Produttore del visualizzatore
OOXML	Microsoft	.docx, .xlsx, .pptx	ISO/IEC DIS 29500:2008	-		Tale formato deve garantire alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML
ODF	Consorzio OASIS OpenOffice.org	.ods, .odp, .odg, .odb	ISO/IEC 26300:2006	application/ vnd.oasis.opendocument.text		www.oasis-open.org

In tutti i casi riportati in tabella, il produttore dei documenti s'impegna a versare al sistema di conservazione *LegalSolutionDOC* documenti privi di codici eseguibili o macro istruzioni o privi di qualsiasi causa, anche non visibile all'utente, che ne possa alterare il contenuto.

Infine, gli oggetti da conservare sono versati al sistema di conservazione dall'Ente Produttore all'interno di Pacchetti Informativi denominati Pacchetti di Versamento e descritti nel paragrafo successivo.

Torna al sommario

6.2 Pacchetto di Versamento

Il Pacchetto di Versamento (PdV) del Sistema di conservazione *LegalSolutionDOC* è costituito da un contenitore (archivio) nel formato zip compresso, contenente:

- i documenti oggetti da conservare (*Content Information*), eventualmente firmati digitalmente (nello standard di firma CAdES ".p7m" ovvero nello standard PAdES ovvero XAdES) o eventualmente marcati temporalmente (nello standard di validazione temporale CAdES-T ovvero nello standard PAdES-T ovvero XAdES-T);

- un file Indice IPdV (Indice del Pacchetto di Versamento) ovvero le *Preservation Description Information* , finalizzato alla descrizione dell'oggetto della conservazione e che secondo lo standard ISO 14721:2012 OAIS permette di identificare il produttore, di contenere i dati descrittivi ed

informativi sull'impacchettamento ed i dati descrittivi e di rappresentazione di ciascun documento contenuto nel pacchetto.

Il file Indice del Pacchetto di Versamento (IPdV) è un file nel formato XML, che in conformità allo standard UNI SINCRO 11386:2010 assicura:

- l'identificazione del soggetto che ha prodotto il Pacchetto di Versamento (produttore dei documenti);
- l'identificazione dell'applicativo che lo ha prodotto;
- la definizione della tipologia documentale (a cui appartengono i documenti inclusi nel pacchetto) ed eventuali messaggi del Responsabile del Servizio di Conservazione;
- la definizione dei documenti inclusi nel pacchetto, con le relative informazioni quali: nome file, hash calcolato, indici e relativi valori, messaggi del Responsabile del Servizio di Conservazione, ecc.

Il file Indice del Pacchetto di Versamento (IPdV) può essere eventualmente firmato digitalmente dal Produttore dei documenti.

Di seguito la rappresentazione grafica del file XSD dell'Indice del Pacchetto di Versamento del sistema *LegalSolutionDOC*:

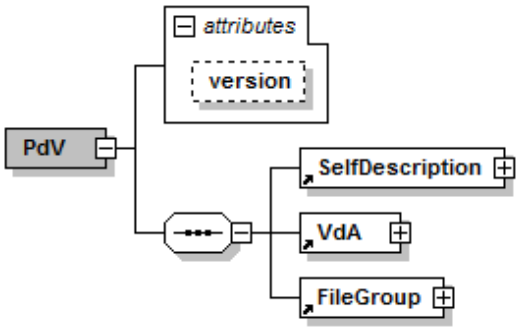

Figura 6 Struttura del Indice IPdV suddiviso nelle componenti principali

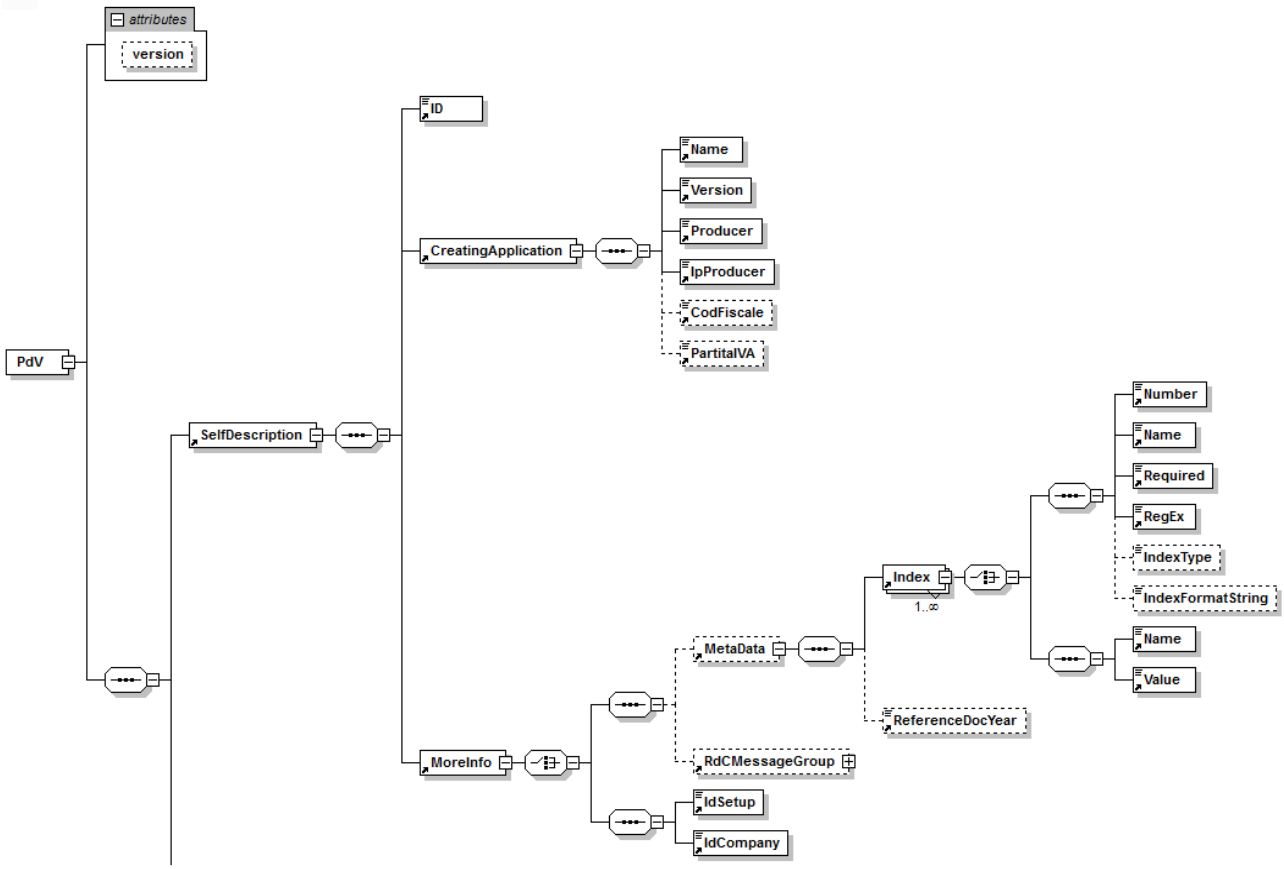

Figura 7 Struttura Indice PdV sezione (SelfDescription)

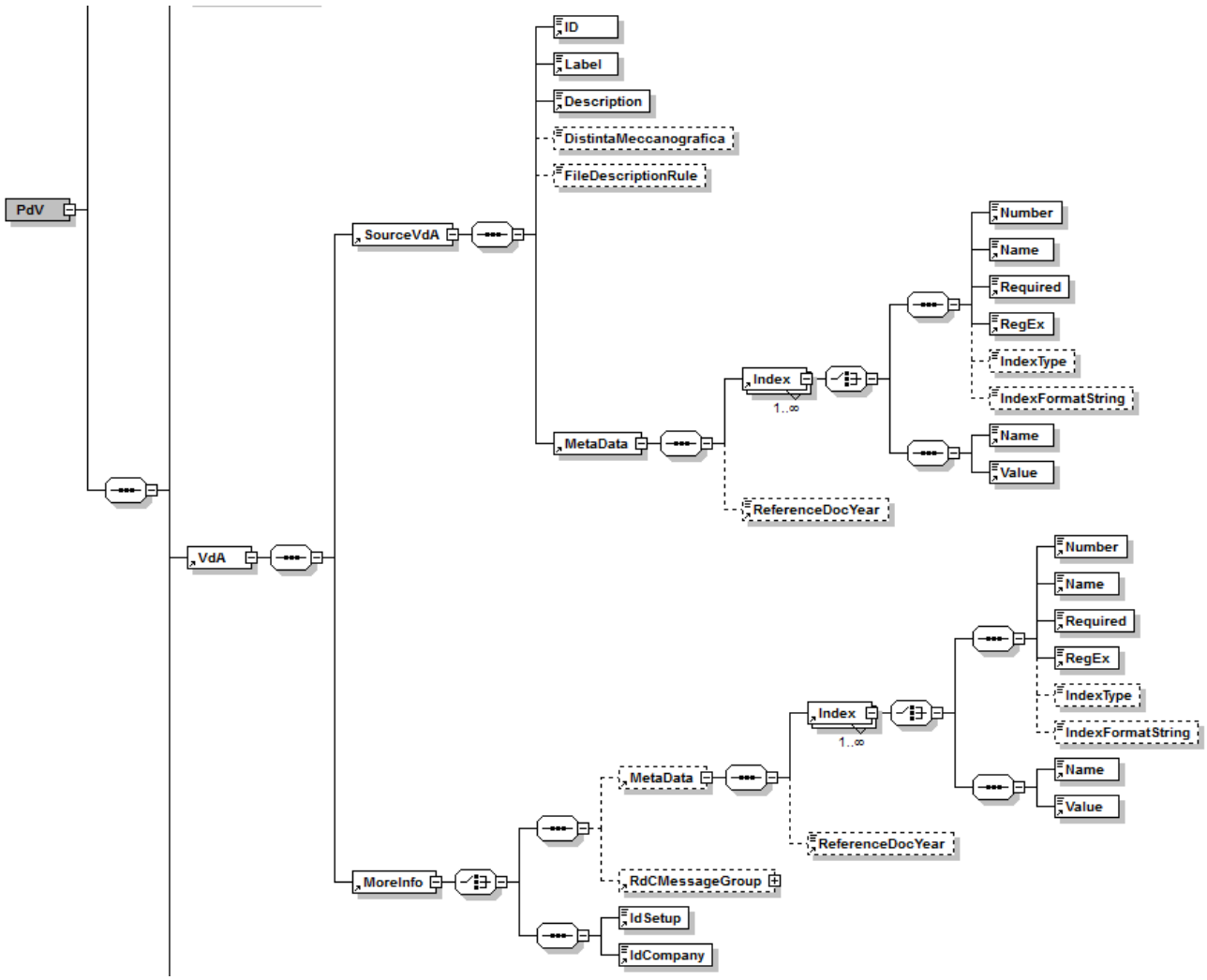

Figura 8 Struttura Indice PdV (Sezione VdA)

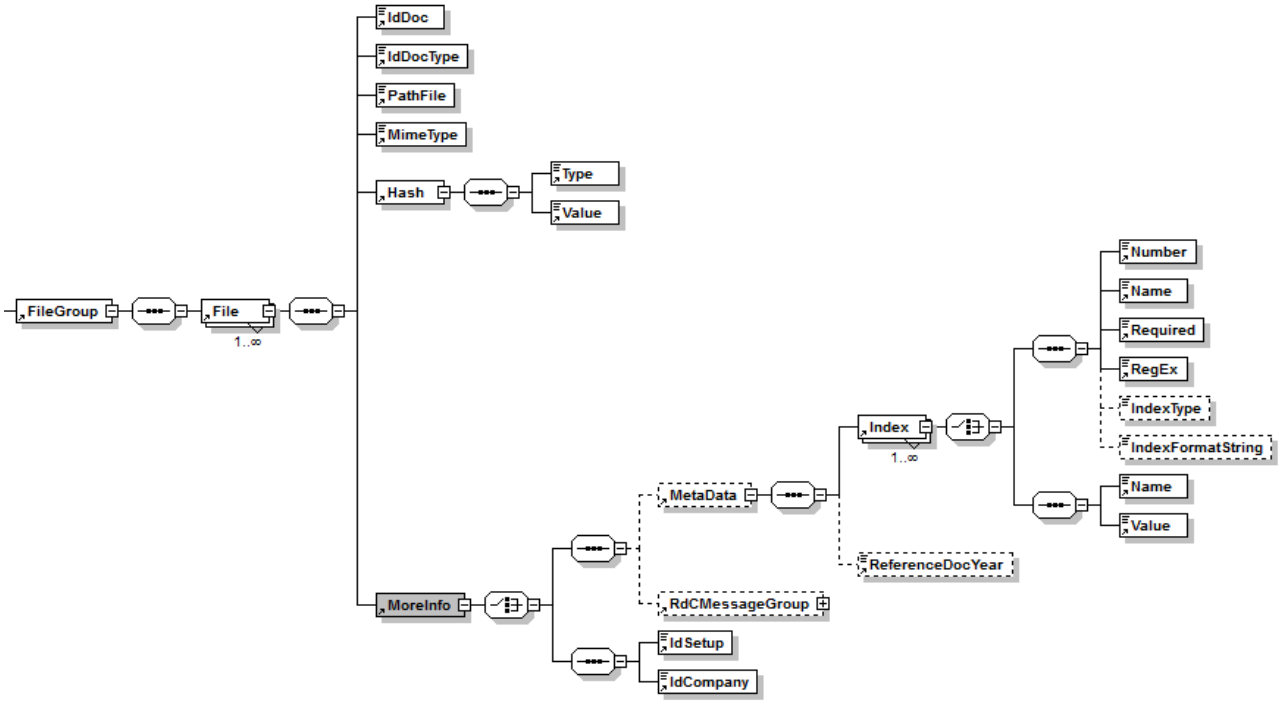

Figura 9 Struttura Indice PdV (Sezione FileGroup)

Il modello-dati del Pacchetto di Versamento e le informazioni di dettaglio sono riportate nella Documento– "Specificità del Contratto".
Le eventuali personalizzazioni sul Pacchetto di Versamento e sulla sessione di versamento sono descritte e concordate tra le parti nell'allegato Documento "Specificità del contratto".

Torna al sommario

6.3 Pacchetto di Archiviazione

Il Pacchetto di Archiviazione (PdA) generato nel processo di conservazione del sistema *LegalSolutionDOC* è una specializzazione del Pacchetto Informativo ed è composto dalla trasformazione di uno o più Pacchetti di Versamento secondo le modalità riportate nel presente manuale di conservazione.

Un Pacchetto di Archiviazione (PdA) è un contenitore informativo che contiene:

- gli oggetti informativi individuati per la conservazione (quindi i documenti, i fascicoli elettronici o le aggregazioni documentali sottoposti al processo di conservazione a lungo termine);
- un Indice del Pacchetto di Archiviazione (IPdA) che rappresenta le Informazioni sulla Conservazione.

In particolare, la struttura dati dell'IPdA del sistema *LegalSolutionDOC* fa riferimento allo standard nazionale SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

L'IPdA è l'evidenza informatica nel formato XML associata ad ogni PdA, contenente un insieme di informazioni descritte nelle regole tecniche in materia, in cui è riportata nel dettaglio la struttura dati prevista. Su ciascun IPdA viene apposta una marca temporale e la firma digitale del Responsabile del Servizio di Conservazione.

La struttura dati del PdA del sistema *LegalSolutionDOC* completa delle ulteriori strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO.

- **SelfDescription (1)*:** Descrizione generale del pacchetto
  - **Id:** Identificativo univoco del PdA generato dal Sistema di conservazione (Id PdA generato dal data base)
  - *CreatingApplication (1):*
    - **Name**: Sistema di conservazione LegalSolutionDOC
    - **Version**: Versione ricavata dal Web Service
    - **Producer**: Produttore del Sistema di Conservazione: 2C SOLUTION SRL
  - **SourceIdC(0**-n)
    - **ID**: Id del pacchetto archiviazione (PdA) precedente
    - **Path**: Percorso relativo del IPdA (SInCRO) del pacchetto precedente
    - Hash: Valore restituito dalla funzione applicandola al file IPdA del pacchetto precedente, contiene l'attributo "function" che identifica la funzione di Hash utilizzata per il calcolo.
  - *Moreinfo (1)*
    - **EmbeddedMetadata**: Riferimenti dell'azienda a cui si riferisce il processo di Conservazione
      - *SoggettoProduttore*
        - **IdSetup**: Id Cliente (Es.: Codice Cliente)
        - **IdAzienda**: Id azienda all'interno di LegalSolutionDOC
        - **Denominazione:** Ragione Sociale dell'azienda
        - **CodFiscale:** Codice Fiscale dell'azienda
        - **PartitaIVA:** Partita IVA dell'azienda
        - **VersionIPdA:** La versione dell'IPdA
- *VdC (1):*
  - **ID**: Identificativo univoco del PdA generato dal Sistema di conservazione (Id PdA generato da Data Base)
  - *MoreInfo (1)*
    - **EmbeddedMetadata**: Elenco dei PdV inclusi all'interno del PdA
      - *VdCGroup*
        - **PdV**
          - **IdPdV:** Id del PdV restituito dal Sistema di conservazione al termine della presa in carico
          - **FunzioneHash**: Funzione di hash utilizzata per calcolare hash dell'IPdV

- **Hash:** Valore restituito dalla funzione di hash applicata al file IPdV**RdCMessageGroup**: Eventuali comunicazioni tra il produttore, il Responsabile della Conservazione o il Responsabile del Servizio di Conservazione relative al PdV.

- *FileGroup (1-n):*
  - **Label:** Nome della tipologia documentale
    - **File:** Definizione del file comprensiva di codifica, estensione e formato (MimeType)
      - **ID:** Id del documento (univoco all'interno del Sistema di Conservazione))
      - **Path:** Indirizzo logico del file rappresentato da un URI (individua il file all'interno dello storage)
      - **Hash:** Funzione di hash utilizzata e valore restituito dalla funzione applicandola al file oggetto della Conservazione
      - *MoreInfo:*
        - **EmbeddedMetadata**
          - **File (1)**
            - **IdDoc, Id** del documento assegnato dal Produttore ed è univoco all'interno di una tipologia documentale per l'azienda.
            - *Indici (1)*
              - **Indice (1-n)**
                - **Nome:** Nome del campo indice (metadato)
                - **Valore:** Valore del campo indice (metadato)
            - **AnnoRiferimentoDoc:** Anno di riferimento per il documento
            - **Oggetto:** Il campo oggetto del documento viene calcolato in automatico dal sistema, in funzione alle regole definite in fase di versamento. Metadato funzionale a riassumere brevemente il documento e comunque a chiarirne la natura.
            - **RdCMessageGroup**: Eventuali comunicazioni tra il produttore ed il Responsabile del Servizio di Conservazione relative al file.
    - *MoreInfo*
      - **EmbeddedMetadata**
        - **Tipologia (1)**
          - **IdTipologia:** Id della Tipologia documentale a cui appartiene il documento
          - *Indici (1)*
            - **Indice (1-n)**
              - **Numero:** Numero indice. Posizione del campo indice (metadato) all'interno della definizione della Tipologia
              - **Nome:** Nome del campo indice (metadato)

- **Richiesto:** Indica se il valore dell'indice (metadato) è obbligatorio (Possibili valori: True, False)
- **RegEx:** Eventuale espressione di validazione per il valore dell'indice (metadato)
- **IndexType:** Tipo di dati del metadato (Possibili valori: stringa, intero, data)
- **IndexFormatString:** Formato del tipo di dato

- *Process (1)*
  - **Agent (1-n):** Definizione dei soggetti che fanno parte del processo di Conservazione (vedere l'Allegato 4 delle Regole tecniche in materia di sistema di conservazione: Specifiche tecniche del Pacchetto di Archiviazione)
    - *AgentName*
      - **NameAndSurname** oppureFormalName.
        - **FirstName,** Nome soggetto
        - **LastName,** Cognome soggetto
        - **FormalName,** Denominazione o ragione sociale
      - **Agent_ID (1-n):** Id univoco del soggetto che interviene nel processo di produzione del pacchetto di Archiviazione (Cod. Fiscale o Partita IVA). Se il soggetto appone la firma, allora uno di questi campi riporta l'Id del certificato digitale del soggetto.
    - *MoreInfo (0-n)*
      - **EmbeddedMetadata**
        - **Soggetto (1-n)**
          - **Mansione:** La descrizione della mansione riferita al soggetto
  - *TimeReference (1)*
    - **TimeInfo:** Data in cui è stata prodotto il file indice. Corrisponde entro certi limiti temporali (richiesti dal processo di firma e marca del file) alla data di rilascio della marca temporale.
  - **LawAndRegulations**: Riferimento alla norma di riferimento: *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.*

* Il numero indicato tra parentesi precisa il numero di ricorrenze che l'elemento può assumere all'interno dell'IPdA: ad es. "(1)" specifica che l'elemento può ricorrere una sola vola; "(1-n)" specifica che può ricorrere 1 o più volte.

Torna al sommario

6.4 Pacchetto di Distribuzione

Un Pacchetto di Distribuzione (PdD) del sistema *LegalSolutionDOC* può essere delle seguenti tipologie:

- **PdD distribuito a seguito di ricerca di un singolo documento**, in risposta alla richiesta dell'Utente;

- **PdD distribuito a seguito di ricerca di più documenti, anche appartenenti a più PdA**, in risposta alla richiesta dell'Utente.

In entrambe le tipologie, il PdD è costituito da un contenitore compresso (ad esempio zip) che contiene i seguenti elementi:

- ✓ I **documenti** (oggetti digitali conservati nel sistema) richiesti dall'Utente.
- ✓ **Uno o più files IPdA** firmati digitalmente dal Responsabile del Servizio di Conservazione e marcati temporalmente associati ai predetti documenti richiesti dall'Utente.
- ✓ **File indice del PdD (IPdD)**: file XML ispirato allo standard UNI SINCRO 11386:2010 e firmato digitalmente dal Responsabile del Servizio di Conservazione, che contiene l'hash dell'IPdA, l'hash di ogni singolo file (documento richiesto o presente all'interno di un PdV richiesto), Super Impronta (se presente).
- ✓ La **Super Impronta** (opzionale, se presente) generata per il produttore (Azienda) a cui si riferiscono i documenti. [ad esempio presente per tutti i documenti con rilevanza tributaria oggetto di conservazione, propedeutica alla comunicazione dell'impronta dell'Archivio secondo il Provvedimento Attuativo Agenzia delle Entrate n. 2010/143663 del 25 ottobre 2010, abrogato con l'entrata in vigore del DM 17 Giugno 2014].

Per ogni PdD generato viene archiviato il file indice (IPdD) all'interno del Sistema di conservazione, per la tracciatura formale delle richieste di documenti da *LegalSolutionDOC*. Questo file indice contiene al suo interno:

- ✓ Id del PdD, generato in seguito al salvataggio su Data Base
- ✓ Data della generazione del PdD (in formato UTC)
- ✓ Azienda a cui si riferisce il PdD (Rag. Sociale, Id setup, Id azienda, Cod. Fiscale, Partita IVA)
- ✓ L'utente che ha richiesto il PdD (Nome, Cognome, Codice Fiscale e/o Partita IVA)
- ✓ Responsabile del Servizio di Conservazione (Nome, cognome, Cod. Fiscale e/o Partita IVA)
- ✓ Operatore conservazione delegato della conservazione.
- ✓ Responsabile del servizio di conservazione.
- ✓ L'indirizzo IP da cui è arrivata la richiesta di generazione
- ✓ PdA consegnati (Id PdA, Hash, Funzione di hash utilizzata, Uri file nel Sistema di conservazione e nel PdD)
- ✓ La lista dei file richiesti (Id documento, Id tipologia, Nome tipologia, Nome file, Hash file, Funzione di hash utilizzata, Uri file nel Sistema di conservazione e nel PdD).

Di seguito viene riportata la struttura dati del pacchetto di distribuzione, secondo lo standard SInCRO.

- **DescGenerale,** Informazioni del richiedente, del Responsabile del Servizio di Conservazione e del sistema di conservazione
  - **ID**, Id del documento estratto dal Sistema di conservazione

- **IdSetup,** Il codice Cliente associato al produttore
- **IdAzienda**, L'id dell'azienda di riferimento nel sistema documentale
- **RagSociale**, La ragione sociale del produttore dei documenti
- **CodFiscale**, Il codice fiscale del produttore dei documenti
- **PartitaIVA,** La partita Iva del produttore dei documenti
- **DataGenerazione**, La data in formato UTC riferita alla produzione del PdD
- **Richiedente,** Dati anagrafici del richiedente
  - **Nome**, Il nome del richiedente
  - **Cognome**, Il cognome del richiedente
  - **CodiceFiscale**, Il codice fiscale del richiedente
  - **PartIVA,** La partita IVA del richiedente
- **Soggetti** La lista dei soggetti coinvolti nel processo di conservazione
- **Soggetto,** Dati anagrafici e ruolo del soggetto.
  - **Nome**, Nome del Soggetto
  - **Cognome**, Cognome del Soggetto
  - **RagSociale,** Denominazione del soggetti in caso di soggetto giuridico
  - **Ruolo,** Il ruolo svolto nel processo
  - **CodFiscale**, Codice Fiscale del Responsabile del Servizio di Conservazione
  - **PartIVA**, Partita IVA del Responsabile del Servizio di Conservazione
- **SdC,** Indicazioni anagrafiche del sistema di conservazione
  - **Nome**, Denominazione del sistema di conservazione
  - **Versione**, Versione del sistema di conservazione

- **PdAGruppo,** Descrizione del PdA estratto
  - **PdA,** descrizione del pacchetto di archiviazione
    - **Id**, Id del pacchetto di archiviazione (identificativo univoco del data base)
    - **FunzioneHash**, il tipo di algoritmo usato per calcolare l'hash
    - **Hash**, Il valore di hash ottenuto dal PdA
    - **UrlFile,** Percorso relativo dell'IPdA all'interno del pacchetto di distribuzione
    - **FileGruppo**, descrizione dei file estratti
      - File
        - **IdDoc,** id del documento nel sistema documentale o altro sistema
        - **PathFile,** Il nome file
        - **AnnoRiferimentoDoc**, anno di riferimento dell'oggetto conservato
        - **FunzioneHash**, il tipo di funzione di hash usata per calcolare il valore
        - **Hash**, Il valore hash del file considerato.
        - **UrlFile,** Percorso relativo del file all'interno del pacchetto di distribuzione

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nell'allegato "*Documento - Specificità del contratto*".

Torna al sommario

7 *IL PROCESSO DI CONSERVAZIONE*

Il processo di conservazione implementato dal sistema *LegalSolutionDOC* è governato in tutte le sue fasi dall'**entità di Amministrazione del sistema,** che interagisce con le altre entità del Sistema, con il Produttore dei documenti e con gli Utenti e le eventuali Comunità di riferimento (Gruppi di Utenti) ed è governata dal **Responsabile del servizio di Conservazione** (ruolo ricoperto dal Conervatore 2C Solution S.R.L. ed espletato attraverso la struttura organizzativa descritta nel presente manuale).

Il Responsabile del servizio di Conservazione, in conformità ai compiti previsti dall'art. 7 del DPCM 3 Dicembre 2013, gestisce i servizi e le funzioni per l'operatività complessiva del sistema *LegalSolutionDOC.*

Nel seguito viene rappresentato il processo di conservazione implementato nel sistema di conservazione *LegalSolutionDOC* in conformità all'art. 8 del DPCM 3 Dicembre 2013.

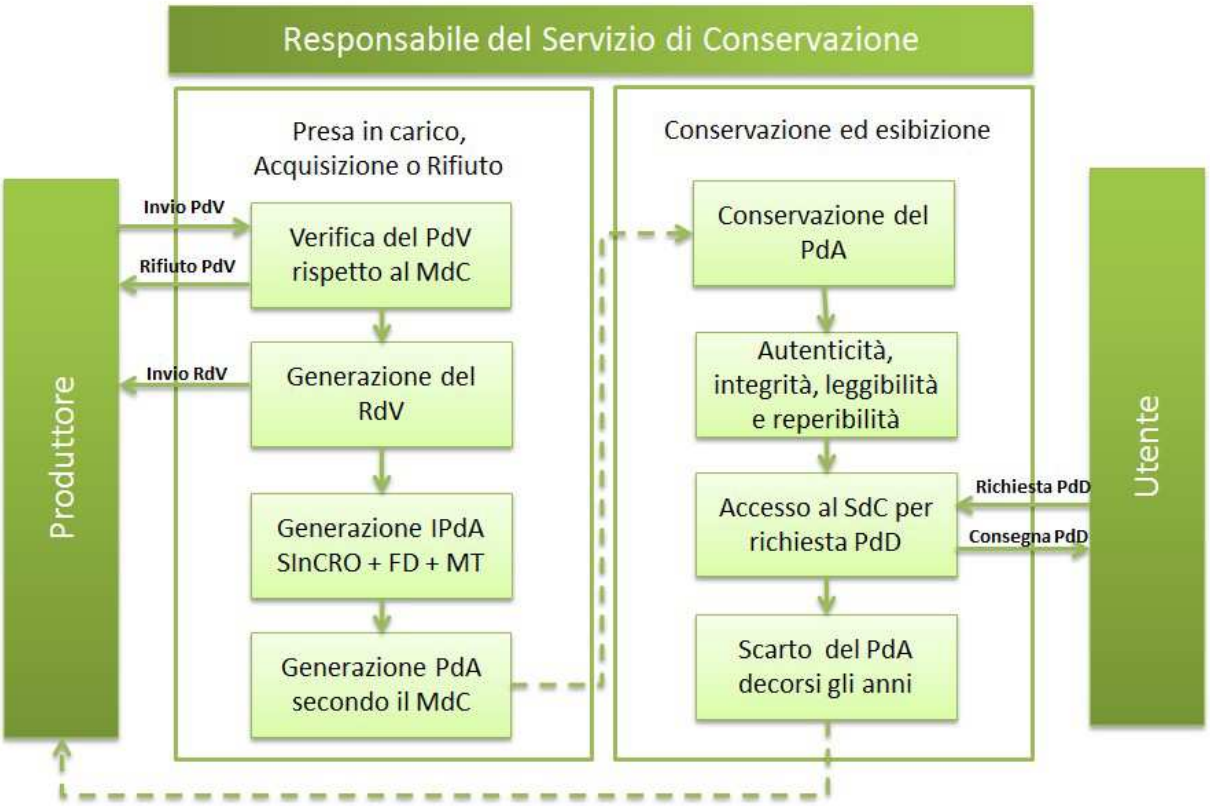

Figura 10 Processo di conservazione in LegalSolutionDOC

Per ciascuna delle seguenti fasi del processo viene riportata nel seguito una descrizione esaustiva

Torna al sommario

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

Il sistema *LegalSolutionDOC* prevede le seguenti modalità di trasmissione dei PdV da parte dell'Ente Produttore verso l'Ente Conservatore:

Tramite Web Services (processo sincrono)
Tramite sFTP e successivo caricamento all'interno di *LegalSolutionDOC* (processo asincrono)

La presa in carico del PdV può avvenire in due modalità:

Sincrona
Trasferimento via web services
Check effettuati per il PdV in fase di presa in carico Risposta web services (esito presa in carico).

Asincrona
Trasferimento PdV nella cartella dedicata SFTP
Presa in carico da Job Schedulato
Inserimento nel Sistema di conservazione
Check effettuati per il PdV in fase di presa in carico Creazione del file "Esito di presa in carico".

Crittografica delle Informazioni trasmesse
Entrambe le modalità di versamento garantiscono la sicurezza e riservatezza dei dati trasmessi grazie alla crittografia del canale adottato (HTTPS o sFTP). Il canale HTTPS integra sul protocollo base HTTP la crittografia di tipo Transport Layer Security (SSL/TLS), questa tecnica aumenta il livello di protezione contro gli attacchi, ll certificato digitale utilizzato per la connessione HTTPS è fornito e garantito da GlobalSign, Il protocollo sFTP prevede il trasferimento dei dati usando il protocollo SSH-2, che garantisce la cifratura delle informazioni trasmesse

Le specifiche ed il modello-dati adottati per il PdV sono i medesimi e la presa in carico per entrambe le modalità si conclude con il rilascio da parte del sistema *LegalSolutionDOC* di un file "Esito di presa in carico" contenente:

- un identificativo Id (GUID) assegnato al PdV in caso di caricamento con esito positivo in modo da identificarlo in maniera univoca nel sistema di conservazione in tutto il ciclo di vita del servizio;
- una Eccezione, se si sono verificati degli errori durante il caricamento.

In particolare, nella modalità sFTP l'esito restituito dalla presa in carico è un file testuale che viene depositato in una cartella di output definita e concordata tra Produttore e Conservatore.

I sistemi di 2C Solution per la presa in carico dei pacchetti di versamento sono tutti in alta disponibilità e garantiscono la ridondanza dei dati.

Inoltre, nel servizio *LegalSolutionDOC* sono attive procedure per la generazione di backup dei PdV versati dal produttore. Le politiche di salvataggio e backup possono essere definite a livello di classe documentale, tale impostazione consente di specificare quanto tempo la copia di sicurezza del PdV debba essere mantenuta nello storage dedicato ai PdV.

Lo storage che mantiene le copie di backup è costituito da 3 repliche, due sul sito primario e una sul sito DR, questa architettura garantisce l'alta affidabilità e il recupero a seguito di un disastro.
Pertanto in caso di necessità di un recupero dei dati dei PdV ancora non trasformati in PdA dal sistema, avviene in accordo con l'Ente Produttore, il quale può richiederlo attraverso un ticket di richiesta all'area di Assistenza. La richiesta smistata all'area tecnico-operativa di 2C Solution permette di attivare il "restore" delle copie dei PdV mantenute nell'area di storage dedicata, al fine di ricreare il processo di acquisizione dei PdV e quindi dare il via ad un nuovo processo di presa in carico.

Le specifiche sulla sessione di versamento e presa in carico del PdV, il modello-dati del PdV sono dettagliate nella "Scheda Servizio Cliente - Specificità del Contratto."

Tutti le attività di presa in carico dei singoli PdV vengono tracciate tramite il sistema di Log Management integrato nel sistema di conservazione. I log vengono mantenuti per tutto il periodo di conservazione degli oggetti versati.
Periodicamente vengono effettuati i controlli di coerenza sui PdV, che compredono controlli di numerosità e altri controllo eventualmente necessari, tutte le attività di controllo vengono tracciate e mantenute sul SdC consentendo di generare dei report a cadenza impostabile per poi essere conservati a sistema.

Ulteriori specifiche concordate tra Produttore e Conservatore 2C Solution e suo Responsabile del Servizio di Conservazione in merito alla sessione di versamento, alla generazione e trasformazione dei PdV, al modello- dati del PdV e alla presa in carico del PdV, sono dettagliate nel documento di "Specificità del Contratto".

Torna al sommario

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

Nel processo di presa in carico dei PdV nel sistema di conservazione, il servizio *LegalSolutionDOC* effettua una serie di controlli di coerenza su ciascun PdV e sugli oggetti in esso contenuti e genera un **esito di presa in carico**.

I controlli eseguiti dal Sistema sui PdV trasmessi sono i seguenti:
(**Bloccante**) Verifica che il pacchetto di versamento contenga l'IPdV ed i files (non viene effettuato dal metodo web services checkIndicePdV);

(**Bloccante**) Controllo validità del file IPdV con il file schema XSD;

(**Bloccante**) Controllo che il soggetto che ha formato ed è titolare dei documenti definito nell'IPdV sia presente e configurato nel Sistema di Conservazione e che per questo soggetto ci sia un soggetto Responsabile del Servizio di Conservazione configurato nel sistema;
(**Bloccante**) Controllo che il numero di files presenti nel PdV corrisponda al numero di files dichiarati nell'IPdV (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
Nel caso specifico della tipologia documentale distinta meccanografica il numero di files presenti nel indice del pacchetto di versamento deve coincidere con il numero di documenti presenti nella singolo documento distinta contenuto nel PdV. Il sistema controlla che tutti i files indicizzati all'interno dell'IPdV, abbiano una corrispondenza con i documenti contenuti nella distinta;
(**Bloccante**) Controllo che i nomi dei files presenti nel PdV corrisponda ai files definiti nell'IPdV (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
(**Bloccante**) Controllo che il MimeType dei files definito nell'IPdV sia stato specificato;
(**Bloccante**) Verifica che i formati dei files contenuti nel PdV siano nei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013 e dalla tabella di seguito riportata

Tipo file	Tipo MIME	Codifica	Note
PDF, PDF/A	application/pdf, application/x-pdf, application/x-bzpdf, application/x-gzpdf	Binario	
TIFF	image/tiff, image/tiff-fx	Binario	
JPG-JPEG	image/jpeg	Binario	
TXT	text/plain	8 bit	
EML (Messaggio di Posta elettronica)	RFC 2822/MIME (text/plain, message/rfc822, multipart/alternative, text/html)	8 bit	
XML	application/xml, text/xml	8 bit	
ODT	application/vnd.oasis.opendocument.text	Binario	
FODT	application/vnd.oasis.opendocument.text	Binario	
DOCX	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Binario	
ODS	application/vnd.oasis.opendocument.spreadsheet	Binario	
FODS	application/vnd.oasis.opendocument.spreadsheet	Binario	
XLSX	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Binario	
ODP	application/vnd.oasis.opendocument.presentation	Binario	
FODP	application/vnd.oasis.opendocument.presentation	Binario	
PPTX	application/vnd.openxmlformats-officedocument.presentationml.presentation	Binario	
ODG	application/vnd.oasis.opendocument.graphics	Binario	
FODG	application/vnd.oasis.opendocument.graphics	Binario	

(**Bloccante**) Verifica della presenza di files nell'IPdV con Id documento NON specificato;
(**Bloccante**) Verifica della presenza di files nell'IPdV con lo stesso Id documento;
(**Bloccante**) Se l'IPdV è firmato il sistema verifica che la firma sia valida, se non è firmato NON lo verifica (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV).

Per ogni documento definito nell'IPdV si effettuano i seguenti controlli:

(**Bloccante**) Verifica che la tipologia definita per il documento corrisponda a quella definita per l'IPdV (campo: SourceVdA);
(**Bloccante**) Verifica che il numero di metadati definiti per il documento corrisponda a quelli definiti all'interno della tipologia configurata nel sistema di conservazione (definita nell'IPdV nella sezione SourceVdA);
(**Bloccante**) Verifica che il nome e l'ordine dei metadati definiti per il documento corrisponda a quanto definito all'interno della tipologia configurata nel sistema di conservazione (definita nell'IPdV nella sezione SourceVdA);
(**Bloccante**) Verifica della presenza del valore per i metadati obbligatori, seguendo lo schema dei metadati (inserito nel PdV nella sezione SourceVdA);
(**Bloccante**) Validazione del valore per i metadati in base all'eventuale espressione regolare definita, seguendo lo schema dei metadati (inserito nel PdV nella sezione SourceVdA);
(**Bloccante**) Verifica che non ci siano documenti con lo stesso Id documento, all'interno del Sistema di Conservazione, per la tipologia associata all'azienda;
(**Bloccante**) Verifica degli Hash dei file con il valore inserito nel PdV (Il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
(**Bloccante**) Verifica della validità della firma sul file (opzionale); il predetto controllo non viene effettuato dal metodo web services checkIndicePdV.
(**Bloccante**) Verifica dell'anno di riferimento documento: deve essere lo stesso per tutti i documenti (definito dell'IPdV nella sezione FileGroup/File/MoreInfo/MetaData/ReferenceDocYear)

Ulteriori personalizzazioni sui controlli eseguiti sono riportati nella "Specificità del Contratto".

Se le verifiche di coerenza eseguite nella fase di presa in carico sono positive il PdV viene preso in carico dal Sistema di Conservazione, altrimenti l'esito di presa in carico ne evidenzia il rifiuto definitivo.

Nella fase di verifica di coerenza del PdV, i risultati dei predetti controlli vengono tutti registrati all'interno della funzionalità di LOG Management System del Sistema con la registrazione di un time stamp (riferimento temporale). Periodicamente effettuate delle verifiche sui log dei controlli effettuati, tali verifiche vengono annotate all'interno del SdC, dove periodicamente è possibile ricavare un report dei controlli effettuati.

Inoltre, l'esito di presa in carico generato dal sistema di conservazione *LegalSolutionDOC* contiene un riferimento temporale e, come meglio specificato nel paragrafo successivo, il Rapporto di Versamento (RdV) generato dal sistema contiene il Tag "<DataGenerazione>" ed è firmato digitalmente dal Responsabile del Servizio di Conservazione. Il riferimento temporale associato al Rapporto di Versamento, rappresenta quindi un'informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC) che identifica la data di formazione del RdV.

Per quanto riguarda i riferimenti temporali si evidenzia che l'orologio di sistema di tutti gli elaboratori impiegati nel servizio di conservazione di documenti informatici sono sincronizzati con i segnali di tempo campione generati dall'Istituto Nazionale di Ricerca Metrologica (INRIM) in Torino

(www.inrim.it). Questo permette al server di firma massiva di mantenere un tempo di sistema che si discosta dal tempo campione dell'istituto metrologico primario INRIM con un errore sicuramente inferiore al minuto.

Torna al sommario

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

In caso di presa in carico, il sistema di conservazione *LegalSolutionDOC* esegue, con una schedulazione periodica il cui timing è configurabile per ciascun produttore dei documenti, eventuali ulteriori controlli di continuità (se previsti nella Specificità del Contratto) e genera un rapporto, il **Rapporto di Versamento (RdV)**, quale esito di tutte le verifiche effettuate sul PdV dalla sua ricezione.

Il Rapporto di Versamento previsto dalle regole tecniche (DPCM 3 Dicembre 2013) ha lo scopo di formalizzare l'acquisizione degli oggetti da conservare inviati tramite un PdV dal Produttore dei documenti. Tale rapporto, come previsto dalla normativa, viene generato anche automaticamente dal sistema *LegalSolutionDOC* e può contenere uno o più pacchetti di versamento.

Il Rapporto di Versamento generato da *LegalSolutionDOC* , viene firmato digitalmente dal Responsabile del Servizio di Conservazione. Alla firma inoltre è associato un riferimento temporale che identifica la data di formazione del documento informatico RdV. Il riferimento temporale e riferito al Tempo Universale Coordinato (UTC).

Per ogni Ente Produttore possono essere generati uno o più RdV per ogni schedulazione, in quanto:

- ogni RdV si riferisce ad una sola tipologia documentale;
- per ogni Ente Produttore è possibile definire il numero massimo di PdV da includere all'interno di un rapporto RdV per evitare di includere un numero elevato di PdV per RdV.
- Il RdV è costituito da un file XML dove all'interno vengono riportate le seguenti informazioni:
- Indicazioni della versione del Sistema di Conservazione
- Indicazioni ed autenticazione del Produttore dei documenti in riferimento al sistema di Conservazione
- Riferimenti dell'utente che ha trasmesso il PdV
- Data di Generazione del RdV
- Riferimenti del Responsabile del Servizio di Conservazione associato al produttore dei documentiRiferimenti del Responsabile della conservazione
- Riferimento del delegato conservatore
- Numero di PdV inclusi nel RdV
- Numero totale dei files contenuti nei PdV inclusi all'interno del RdV
- La funzione di Hash con cui è stato generato l'hash del IPdV
- Hash del/i IPdV considerato/i nel RdV
- L'indirizzo IP della macchina dove è stato generato il PdV
- La lista dei messaggi del RdC contenuti nel/nei pacchetto/i di versamento collegato/i al file

L'esito dei check una volta ricevuto il PdV da parte del Sistema di conservazione
Il rapporto di versamento, generato nel formato XML, viene firmato dal Responsabile del Servizio di Conservazione e conservato periodicamente nel sistema di conservazione *LegalSolutionDOC.*

Ulteriori specifiche sulla generazione del RdV ed il modello dati dello stesso sono dettagliate nella "Specificità del Contratto."

Il Rapporto di Versamento (RdV) generato secondo lo standard UNI SInCRO 11386:2010, che formalizza il buon esito del versamento dei pacchetti da parte del produttore dei documenti, una volta l'anno viene posto in conservazione a norma.

Periodicamente vengono effettuati dei controlli sui RdV generati e inviati, tali verifiche vengono annotate all'interno del SdC. Tali annotazioni vengono inoltre riportate sui report periodici prodotti ai fini dell'archiviazione.

Torna al sommario

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

Durante le verifiche di coerenza possono essere riscontrate le seguenti anomalie che generano il rifiuto dei pacchetti di versamento:

- PdV non contiene l'IPdV ed i documenti;
- File IPdV non valido rispetto allo schema XSD;
- Identificazione del Produttore dei documenti e non corrispondenza nel sistema di conservazione;
- Assenza di un Responsabile del Servizio di Conservazione nel Sistema di conservazione per il produttore dei documenti a cui il PdV si riferisce;
- Numero di files presenti nel PdV non corrispondente al numero di files dichiarati nell'IPdV;
- Nomi dei files presenti nel PdV non corrispondenti ai nomi files definiti nell'IPdV;
- Verifica tipo MIME dichiarato nell'IPdV (MimeType tra quelli ammessi per la conservazione dei files);
- Verifica formati dichiarati nell'IPdV (formati tra quelli ammessi per la conservazione dei files);
- Presenza di files nell'IPdV con Id documento non specificato;
- Presenza di files nell'IPdV con lo stesso Id documento;
- Verifica della validità della firma digitale solo se il IPdV è firmato;
- Verifica che la tipologia documento nel sistema di conservazione corrisponda a quella definita per l'IPdV (campo: SourceVdA);
- Verifica che la tipologia documentale configurata nel Sistema di conservazione corrisponda a quella dichiarata nel'IPdV (campo: SourceVdA);
- Verifica che i metadati configurati per quella tipologia documentale nel sistema di conservazione corrispondano a quelli dichiarati nel'IPdV (campo: SourceVdA);
- Verifica che il nome e l'ordine dei metadati configurati per quella tipologia documentale nel sistema di conservazione corrispondano a quelli dichiarati nell'IPdV (campo: SourceVdA);
- Verifica della presenza dei metadati settati come obbligatori nell'IPdV (campo: SourceVdA);
- Verifica dell'eventuale espressione regolare dei metadati dichiarati nell'IPdV (campo: SourceVdA);
- Verifica che non ci siano documenti con lo stesso Id documento, all'interno del Sistema di Conservazione, per la medesima tipologia documentale associata ad un determinato produttore dei documenti;
- Verifica corrispondenza degli hash (impronte) dei documenti calcolati dall'ente conservatore con l'hash dichiarato nell'IPdV dall'ente produttore;
- Verifica della validità della firma sul singolo documento. Il controllo della verifica sui documenti firmati può essere opzionale ed attivabile solo sui documenti firmati.

Ulteriori controlli possono essere eseguiti in merito al rispetto della continuità della numerazione o all'ordinamento cronologico, eventualmente generando ulteriori anomalie riportate nel Rapporto di Versamento, ma ciò è concordato tra produttore e Responsabile del Servizio di Conservazione nel documento "Specificità del Contratto".

Il sistema di conservazione, successivamente alla sua generazione, prevede la possibilità di inoltro al produttore dei documenti del RdV tramite e-mail o messa a disposizione via sFTP o tramite chiamata web service.
La modalità di consegna del RdV dal sistema di conservazione al produttore prevede la creazione di un pacchetto contenitore, contenente il file RdV firmato dal Responsabile del Servizio di Conservazione, il file RdV non firmato per una più agevole elaborazione del file da un eventuale sistema informativo ed un file XSLT per la semplice visualizzazione tramite browser.

É inoltre possibile richiedere il RdV direttamente accedendo dall'interfaccia web di consultazione in *LegalSolutionDOC* da parte di un utente autorizzato dal produttore dei documenti.
Periodicamente il Responsabile del Servizio di Conservazione conserva in conformità alla normativa vigente tutti i RdV generati, che rimangono sempre a disposizione per la consultazione ed esibizione. Si evidenzia che nel sistema di conservazione *LegalSolutionDOC* è prevista una procedura per permettere al Responsabile del Servizio di Conservazione, su esplicita richiesta del produttore, di annullare dei PdV già acquisiti solo se non fanno parte di un processo di conservazione già completato (Pacchetto di Versamento già incluso in un PdA firmato e marcato).
L'annullamento dei PdV avviene tramite interfaccia Web attraverso una specifica funzionalità accessibile solo tramite il sistema di ticketing di 2C Solution.
Tali pacchetti se annullati attraverso l'interfaccia web resteranno comunque salvati e disponibili nel Sistema di conservazione ma nello stato annullato e quindi non potranno più essere selezionati per la successiva fase di generazione dell'IPdA.
L'operazione di annullamento dal processo di conservazione di un PdV viene comunicata al produttore dei documenti all'interno del successivo RdV per esso generato.
In conclusione, nel presente paragrafo e nel paragrafo 7.2 sono stati descritti i controlli eseguiti dal servizio *LegalSolutionDOC* sui PdV ricevuti in cui si è descritto che le anomalie rilevate sui PdV vengono tracciate negli esiti di presa in carico e nel rapporto di versamento (RdV).
La comunicazione al Produttore delle anomalie riscontrate dai predetti controlli avviene, pertanto, attraverso la consegna o messa a disposizione degli esiti di presa in carico e dei rapporti di versamento.
Il Conservatore 2C Solution consente all'Ente Produttore di avere a disposizione gli esiti di presa in carico tramite dialogo applicativo web services o tramite sFTP nella cartella di destinazione "RX" definita tra le parti neldocumento "Specificità del Contratto".

Si riporta un esempio di generazione del file *Esito di presa in carico (estensione .esito)* messo a disposizione del Produttore:

```
<?xml version="1.0" encoding="utf-8"?>
<EsitoPresaInCarico>
<NomeFile><![CDATA[Files.zip]]></NomeFile>
<DataVersamento>2014-09-11T07:58:01Z</DataVersamento>
<Id>000000001_2014</Id>
```

<IdPdV>54115609b84ac914886a905b</IdPdV>
<HashIPdV>B6D3163419584386155E39810111ED69BF8D7166FF38502A451371DB42DA0186</HashIPdV>
<FunzioneHashIPdV>SHA-256</FunzioneHashIPdV>
<CodFiscale>COD_FISCALE</CodFiscale>
<PartitaIVA>IT:PARTITA_IVA</PartitaIVA>
<Errori />
</EsitoPresaInCarico>

Gli elementi presenti nel file di esito hanno il seguente significato:

NomeFile: Nome file del pacchetto di versamento (Archivio Zip o Non Zip).
DataRicezione: Data e ora in cui è stato ricevuto il PdV.
Id: Progressivo (es.: Guid) generato dal Sistema Documentale, oppure dal sistema che ha prodotto il PdV. Viene inserito all'interno dell'IPdV da parte del produttore.
IdPdV: Id univoco del PdV assegnato dal Sistema di conservazione.
HashIPdV: Hash del file IPdV.
FunzioneHashIPdV: Funzione di hash con cui è stata calcolato l'hash dell'IPdV.
CodFiscale: Codice Fiscale del produttore ricavato dal PdV.
PartitaIVA: Partita Iva del produttore ricavata dal PdV.

Si riporta un esempio di possibili errori che possono essere riscontrati dai controlli del sistema di conservazione *LegalSolutionDOC*:
<Errori>
<Errore><![CDATA[Il file indice PdV contiene 1 files, mentre nel pacchetto sono presenti 2 files.]]></Errore>
<Errore><![CDATA[Il file NON è presente nel file indice PdV, ma è presente nel pacchetto. Nome file: 1.pdf]]></Errore>
</Errori>

La generazione e la consegna degli esiti di presa in carico sono tutte azioni registrate nel Log management System del sistema di conservazione *LegalSolutionDOC* con un riferimento temporale.

Il Conservatore 2C Solution consente all'Ente Produttore di avere a disposizione i Rapporti di Versamento con le seguenti modalità:

attraverso **comunicazione via PEC o mail ordinaria**, secondo l'indirizzo di posta elettronica configurato nel Sistema di conservazione *LegalSolutionDOC* nella anagrafica del Produttore (servizio configurato su richiesta del Cliente e concordato nel documento di Specificità del Contratto); la e-mail viene formattata in modo automatico dal Sistema e in allegato viene inserito il RdV firmato dal Responsabile del Servizio di Conservazione e il file non firmato (per una più agevole elaborazione del file da parte di un eventuale sistema di terze parti). Viene inoltre fornito un file XSLT per la visualizzazione agevole tramite browser;

- tramite **chiamata al webservice del sistema di conservazione**, secondo le modalità specificate nel documento LegalSolutionDOC SDK allegato alla Specificità del Contratto;

- tramite **accesso alla piattaforma web del Sistema di conservazione LegalSolutionDOC** da parte di un utente autorizzato per quel determinato Produttore.

Anche in questo caso tutte le azioni sono tracciate nel Log management System del sistema di conservazione *LegalSolutionDOC* con un riferimento temporale.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

La generazione dell'IPdA avviene secondo le specifiche dell'Allegato 4 del DPCM 3 Dicembre 2013 e secondo il modello dati definito dallo standard SInCRO – Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.
La generazione dell'IPdA corrisponde alla chiusura definitiva del processo di conservazione a norma. Questa procedura viene avviata nel sistema *LegalSolutionDOC* tramite un job configurato all'interno dell'entità funzionale schedulatore del processi presente nel sistema, sulla base delle regole di conservazione configurate nel sistema per il produttore dei documenti.
Una volta generato l'IPdA viene apposto su di esso la firma digitale del Responsabile del Servizio di Conservazione ed una marca temporale, quindi i Pacchetti di Versamento inclusi nel PdA non potranno più essere modificati.
La firma digitale e la marca temporale sono emesse, in conformità alla normativa vigente, da 2C Solution, rispettivamente in qualità di Certification Authority (CA) e di Time Stamping Authority, in conformità alla normativa vigente.
Il sistema, anche nel caso della generazione dei PdA, registra i log per la tracciatura delle azioni effettuate sui pacchetti di archiviazione.
La procedura di ripristino in caso di corruzione o perdita dei dati dei PdA prevede la gestione dell'incident con livello di priorità massima ed il ripristino attraverso l'utilizzo del PdA copia di backup da parte del team preposto, secondo il piano operativo esposto nella documentazione sulla continuità operativa gestita per la certificazione ISO 27001:2013.
Specifici casi in cui è necessario adottare metodi di crittografia per proteggere i dati conservati nei PdA sono descritti nell'allegato – Documento "Specificità del contratto", che rappresenta l'accordo sulle condizioni di servizio specifiche tra Ente Conservatore ed Ente Produttore.

Periodicamente vengono effettuati dei controlli sui PdA prodotti; tali verifiche vengono inserite come annotazione sul sistema di conservazione e riportati sui report che vengono mantenuti in archiviazione.

Torna al sommario

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

In risposta ad un ordinativo (richiesta dell'Utente) tramite l'interfaccia di ricerca documenti di *LegalSolutionDOC*, il sistema di conservazione fornisce all'Utente richiedente tutto o parte o una raccolta di Pacchetti di Archiviazione, sotto forma di Pacchetto di Distribuzione (PdD).

L'Utente può ricercare da interfaccia web, attraverso l'inserimento di apposite chiavi di ricerca, i documenti come output della ricerca, su cui poi richiedere la distribuzione del relativo PdD

attraverso un pulsante "Genera Pacchetto di Distribuzione"; in alternativa un'utenza applicativa autorizzata può richiedere un PdD

tramite chiamata web service. Il PdD distribuito dal sistema *LegalSolutionDOC* contiene tutte le evidenze di un singolo documento o quelle di un sottoinsieme di documenti conservati, a seconda della tipologia di PdD richiesta.

Una volta che l'utente richiede un PdD il sistema restituisce tramite canale crittografato (protocollo HTTPS) il pacchetto PdD in formato di cartella compressa .zip dove all'interno l'utente ha a disposizione tutti i file necessari. Le tipologie di Pacchetti di Distribuzione ed i modelli-dati sono descritti nel paragrafo 6.4 del presente manuale.
L'utente può richiedere la generazione di più PdD e ogni azione di richiesta e messa a disposizione del PdD viene tracciata con un identificativo univoco all'interno del sistema di Log Management System di *LegalSolutionDOC* e con la registrazione di un riferimento temporale.
Lo storage che mantiene i Pacchetti di Archiviazione e dei Pacchetti di Distribuzione è costituito da 3 repliche, due sul sito primario e una sul sito DR, questa architettura garantisce l'alta affidabilità e il recupero dei dati a seguito di corruzione o perdita dei dati.

Ulteriori informazioni di dettaglio, concordate con il soggetto Produttore, sono descritte nell'allegato Documento "Specificità del Contratto".

Torna al sommario

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

L'utente autorizzato ad accedere al sistema di conservazione *LegalSolutionDOC* tramite le sue credenziali può eseguire le ricerche attraverso una interfaccia web e tramite l'ausilio di una serie di chiavi di ricerca (metadati) predefinite.
Una volta ottenuto l'output della ricerca l'utente ha la possibilità di richiedere la distribuzione di un PdD o più semplicemente può eseguire la richiesta di download dei duplicati dei documenti informatici conservati, per singolo documento o per range di documenti.

La richiesta e l'ottenimento di un duplicato di un documento informatico conservato può essere avanzata anche attraverso chiamate web service da un utente autorizzato.
Inoltre, attraverso il sistema di ticketing aziendale e secondo quanto concordato nel documento "Specificità del Contratto", l'utente può inoltrare richiesta in merito alla necessità di ricevere duplicati. Il Conservatore 2C Solution potrà in tal caso mettere a disposizione secondo la modalità concordata (ad esempio sFTP) in un pacchetto contenitore tutti i duplicati richiesti dall'utente.

Vi sono casi in cui è necessaria la produzione di una copia informatica con attestazione di conformità da parte di un pubblico ufficiale:

- per adeguare il formato del documento all'evoluzione tecnologica attivando un processo di riversamento sostitutivo a seguito dei controlli da parte del Responsabile del Servizio di Conservazione;
- su esplicita richiesta dell'utente in quanto concordato nel documento Specificità del Contratto.

Nel primo caso l'ownership dell'attività è in carico al Responsabile del Servizio di Conservazione che secondo un piano preventivo di controlli esegue le verifiche di integrità, di leggibilità e di adeguatezza della rappresentazione informatica dei documenti all'evoluzione tecnologica.
Il processo, completamente tracciato nei Log Management System e presidiato operativamente dall'Area di Assistenza Dematerializzazione e Sicurezza Digitale di 2C Solution, richiede la gestione di un riversamento sostitutivo, ovvero il processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, modificando la loro rappresentazione informatica, garantendo il mantenimento dell'integrità del contenuto.
Proprio per la garanzia della conformità del contenuto nel passaggio da una rappresentazione informatica ad un'altra rappresentazione, più aggiornata tecnologicamente, è necessario nel processo l'intervento del pubblico ufficiale. La procedura prevede la messa a disposizione dei documenti originali e dei documenti copia al pubblico ufficiale, che una volta verificata l'immodificabilità del contenuto, appone la firma digitale su un file denominato "attestazione di conformità".
Questo documento viene posto in conservazione nel sistema *LegalSolutionDOC* come allegato integrativo (collegamento tramite hash tra i PdA) assieme al documento copia conforme e poi entrambi conservati. Tutte le evidenze dell'operazione eseguita vengono mantenute nel tempo dal Responsabile del Servizio di Conservazione.
Si evidenzia che la scelta di formati idonei, previsti e consigliati dalla normativa vigente (ad esempio il formato PDF/A) da parte del Responsabile del Servizio di Conservazione 2C Solution e del Produttore dei documenti è la scelta perseguita come prevenzione e minimizzazione dei rischi legati all'obsolescenza tecnologica.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Superato il periodo di conservazione di pacchetti e documenti concordato tra Ente Conservatore e Ente Produttore, il sistema *LegalSolutionDOC* deve implementare la procedura di scarto dei pacchetti di archiviazione.
Il sistema notifica (via mail/pec) al produttore con 30 gg di anticipo l'avvio della funzione di scarto per determinati PdA dandone quindi informativa secondo la normativa vigente e fornendo le informazioni necessarie al produttore per valutare l'eventuale richiesta di estensione del periodo di conservazione.
In caso di superamento della scadenza prefissata ed in assenza di richiesta di estensione, il job della procedura di scarto si attiva e produce dei Pacchetti di Scarto (PdS) in relazione ai PdA oggetto della procedura. L'operazione è tracciata nel sistema e viene prodotto un file Indice del Pacchetto di Scarto (IPdS) nel formato UNI SInCRO 11386:2010 firmato digitalmente dal Responsabile del Servizio di Conservazione che grazie al file XSLT può essere visualizzato dal Produttore dei documenti o altri soggetti interessati per la verifica della corretta procedura eseguita.
In ultimo, nel sistema *LegalSolutionDOC* viene registrato se la gestione della procedura di scarto è relativa ad archivi pubblici o privati che rivestono interesse storico particolarmente importante secondo (D.Lgs. 22 gennaio 2004, n.42); in questo caso si attiva un alert e la procedura di scarto del pacchetto di archiviazione avviene solo previa autorizzazione della Soprintendenza Archivistica del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia e secondo gli accordi definiti nella "Specificità del Contratto".

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

La principale struttura-dati a garanzia dell'interoperabilità per 2C Solution è il Pacchetto di Archiviazione generato secondo le regole tecniche in materia di sistema di conservazione e secondo lo standard nazionale UNI SINCRO 11386:2010.
La sua distribuzione attraverso la richiesta di uno o più Pacchetti di Distribuzione (PdD) tramite diverse funzionalità e modalità (interfaccia web, web service, sFTP, ecc.) messe a disposizione dal servizio *LegalSolutionDOC* garantisce la corretta trasferibilità da parte del produttore ad altro conservatore.
Nel caso di riconsegna di tutti i PdA conservati (ad esempio per la chiusura del servizio o per la cessazione anticipata del servizio secondo quanto concordato contrattualmente) il produttore dei documenti (utente) potrà richiedere la loro distribuzione al sistema *LegalSolutionDOC*, selezionando la richiesta tramite dei filtri da interfaccia web e l'apposita funzionalità.
Ogni PdD contiene un Indice del PdD, generato secondo lo standard UNI SInCRO 11386:2010 e firmato dal Responsabile del Servizio di Conservazione, che rappresenta un rapporto (verbale) della distribuzione eseguita. Il PdD contiene anche il file XSLT per la corretta visualizzazione dell'IPdD.
Se il Produttore dei documenti volesse richiedere una personalizzazione del servizio di distribuzione con l'esecuzione di attività aggiuntive per la migrazione o per l'interfacciamento diretto di 2C Solution con altri Conservatori ai fini della trasferibilità, le attività saranno eseguite da 2C Solution sulla base di quanto concordato nella "Specificità del Contratto" con il produttore stesso.

Il sistema *LegalSolutionDOC* di 2C Solution è in grado di acquisire pacchetti di versamento/pacchetti di archiviazione conformi con la struttura UNI SINCRO 11386:2010 nel caso di subentro su archivi gestiti da altro conservatore che abbia adottato tale standard per la generazione dell'IPdA.

Torna al sommario

8 Il sistema di conservazione LegalSolutionDOC

Il sistema di conservazione *LegalSolutionDOC* e una soluzione informatica sviluppata e mantenuta da 2C Solution per la conservazione a norma dei documenti informatici. Conforme con la disposizioni tecniche del DPCM Dicembre 2013.

L'infrastruttura di erogazione del servizio di conservazione dei documenti informatici *LegalSolutionDOC* è stata concepita, organizzata e sviluppata in modo che le varie fasi di lavoro risultino atomiche e che il flusso di lavoro sia modulare e scalabile. Sfruttando tecnologie oggi conosciute come BigData, quindi utilizzando database NoSQL e Object Storage.

8.1 Componenti Logiche

Le principali componenti della soluzione di conservazione di documenti informatici *LegalSolutionDOC*
possono essere schematizzate dalla seguente rappresentazione grafica.

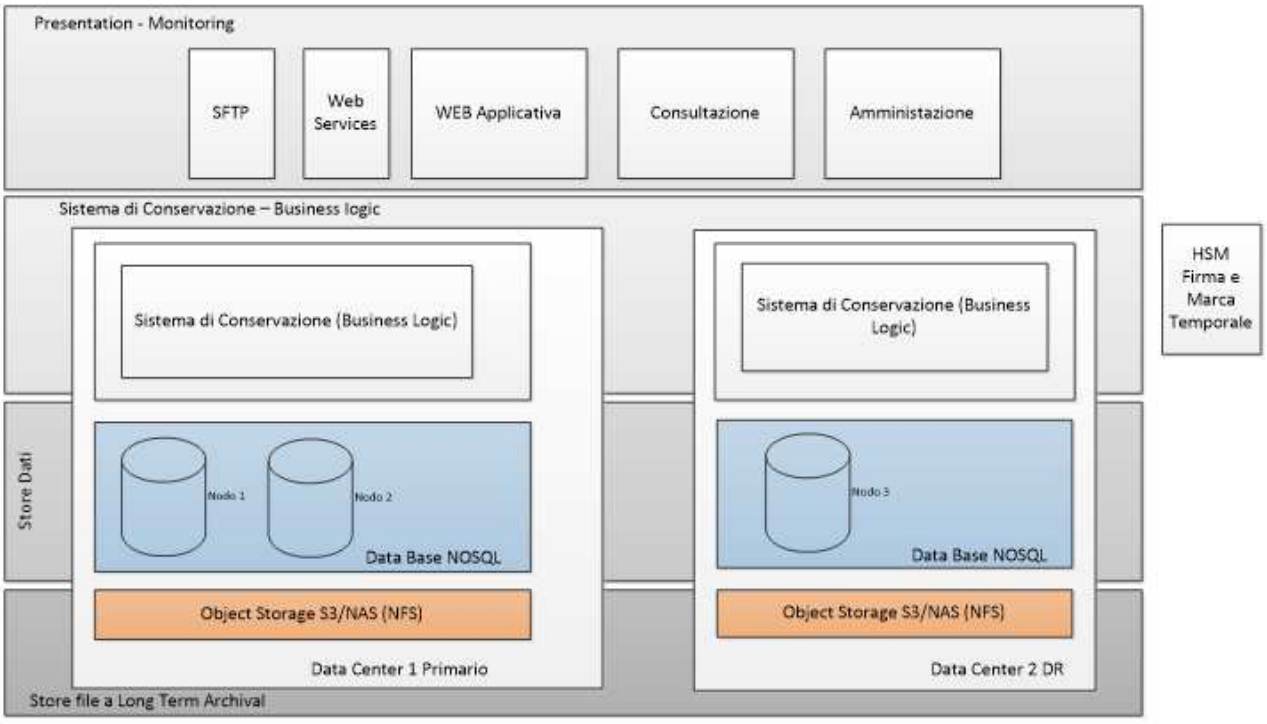

Figura 11 Architettura del Sistema di Conservazione

Come rappresentato in figura la soluzione è basata su una struttura multi-tier e più livelli:

Presentation - Monitoring: La soluzione è stata progettata per garantire una veloce scalabilità, il livello presentation costituisce l'interfaccia dove i produttori e gli amministratori di sistema possono operare e gestire il sistema di conservazione, vediamo in dettaglio le singole componenti:

- ***SFTP***, Il servizio di FTP che ha il compito di ricevere i PdV da parte dei produttori, processo asincrono.
- ***Web Sevirvices***, l'interfaccia web esposta su protocollo SOAP che consente ai produttori tramite l'integrazione con i loro sistemi di trasferire direttamente i PdV con processi sincroni. Il Web Services inoltre espone le funzionalità di ricerca dei documenti e le funzionalità di generazione dei PdD.
- ***Web Applicativa/Consultazione/Amministrazione,*** Costituisce il client di gestione web del sistema di conservazione, in questa web application e possibile gestire la configurazione del sistema di conservazione, definizione dei soggetti produttori, configurazione dei soggetti per i processi di conservazione, definire le classi documentali e i rispettivi metadati, definire le policy di accesso o gli utenti che dovranno consultare i documenti.

Torna al sommario

8.2 Componenti Tecnologiche

Sistema di Conservazione - Business Logic: Lo strato di Business Logic integrata nel servizio di Conservazione, implementa tutti i processi del sistema di conservazione, dalla gestione di ogni singolo pacchetto (PdV, PdA, PdD) rapporti di versamento, i log del processo di conservazione, e l'interfaccia con il database e lo storage dei dati.

Store Dati: *LegalSolutionDOC* utilizza un data base NoSQL per lo storage dei dati, con una struttura a tre nodi replicati, due nodi sul sito primario e un terzo nodo sul sito DR. Tale struttura ci consente oltre a gestire una scalabilità orizzontale del sistema, una grande affidabilità e SLA di servizio molto alti. Ognuno dei 3 nodi dati quindi è replicato a livello applicativo e tale replica garantisce sia la salvaguardia delle informazioni trattate sia la continuità operativa del servizio e la disponibilità dei documenti e dati, qualora uno tre nodi non dovesse essere operativo.

Store file e Long Term Archival: Per Lo storage dei file *LegalSolutionDOC* utilizza un sistema di storage basato su tecnologia Object Storage su tre nodi. Anche per la gestione dello storage dei file utilizziamo un'architettura a 3 nodi, 2 nodi dati sul primario e 1 nodo dati sul DR, al fine di garantire l'alta affidabilità e SLA nell'ordine del 99,99 sulla perdita delle informazioni. Il gruppo di server distribuiti, interconnessi tra loro, dove sono conservati gli oggetti digitali della conservazione è ubicato nel territorio nazionale.

Dalla struttura di erogazione del servizio (struttura primaria), è previsto un collegamento diretto, cifrato e privato, verso la struttura di Disaster Recovery. Tale struttura è logicamente suddivisa, come la struttura primaria.

Maggiori dettagli sulle componenti tecnologiche sono riportati nella documentazione del Sistema di Gestione della Sicurezza certificato ISO/IEC 27001:2013.

Torna al sommario

8.3 Componenti Fisiche

Il sistema di conservazione *LegalSolutionDOC* è installato ed eroga i servizi su data center Televideocom.

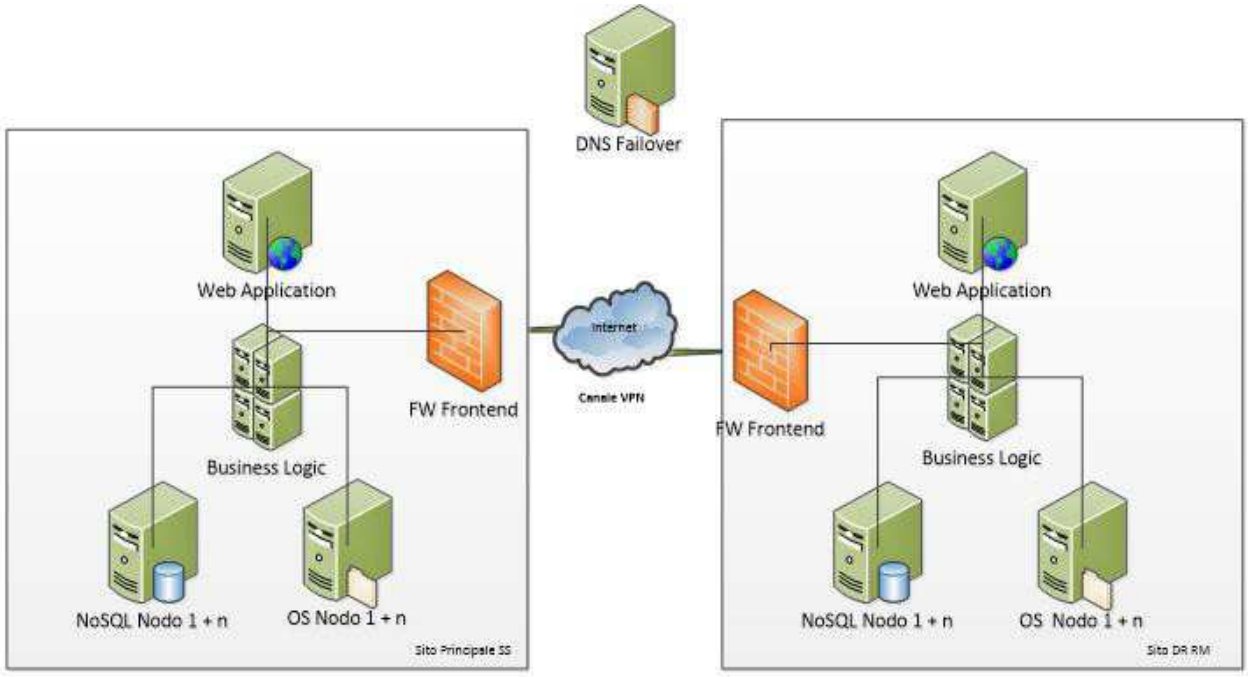

Figura 5 Struttura Indice PdV (Sezione VdA)

- **Sito Primario**, situato su datacenter di Sassari con tutte le componenti necessarie in HA e collegato tramite connettività descritta sotto.
- **Sito Secondario DR,** su datacenter di Pomezia (RM), gestito ed amministrato da Televideocom, con le componenti necessarie per la ripartenza dei servizi in maniera completamente automatica.

L'architettura di rete che compone il sistema informativo di Televideocom è strutturata secondo lo schema "Network Fully Connected / Any to Any" completamente ridondato.

La distanza dei siti elaborativi Sassari (SS) e Pomezia (RM), i quali erogano i servizi informatici di produzione per il business di 2C Solution, evidenzia quanto segue:

Distanza in linea d'aria

- Sassari (Produzione) – Pomezia (Disaster Recovery) → 400 km
- 2C Solution (Esercizio) – Sassari (Produzione) → 750 km

Per gli approfondimenti ed il dettaglio in relazione alle componenti fisiche ed alla continuità operativa si rimanda alla documentazione relativa al sistema di gestione della sicurezza informatica, certificato ISO/IEC 27001:2013.

Torna al sommario

8.4 Procedure di gestione e di evoluzione

2C Solution, con il supporto di tutte le strutture aziendali, ciascuna per la parte di propria competenza, ha provveduto ad istituire un sistema di governo e presidio del servizio con lo scopo di:

- garantire la riservatezza, l'integrità, la leggibilità, la reperibilità e la disponibilità dei documenti e dati nel sistema;
- formalizzare e garantire i requisiti del sistema in conformità alla normativa vigente;
- manutenzione del servizio:
- ottimizzare la gestione dell'incident management;
- valutare i livelli di rischio e di continuità operativa;
- monitorare i livelli di sicurezza;
- gestire operativamente le attività di sicurezza (incidenti, prevenzione frodi, gestione della comunicazione in emergenza, ecc.).

Conduzione e manutenzione del sistema di conservazione

I requisiti di sicurezza (sicurezza fisica, sicurezza logica e sicurezza organizzativa) adottati nella conduzione e manutenzione del sistema di conservazione, nelle politiche di gestione dell'incident management e della continuità operativa del servizio di conservazione sono specificati e riportati nel piano della sicurezza e nella documentazione del sistema di gestione della sicurezza.

Il conservatore 2C Solution mantiene un registro cronologico delle componenti della piattaforma software *LegalSolutionDOC*, comprensivo di tutte le release, inoltre registra le diverse release di sistema operativo e di applicativi utilizzati nell'intero processo di conservazione nell'arco degli anni al fine di rendere comunque disponibili e fruibili nel tempo i documenti ed i dati relativi al servizio.
La procedura dei rilasci del software è una procedura che segue i requisiti imposti dalla certificazione ISO/IEC 27001:2013.

2C Solution mette a disposizione sia internamente che per i soggetti esterni (clienti, fornitori, ecc.) un servizio di assistenza specifico e di competenza, istanziato da parte dell'utente autorizzato attraverso il sistema di ticketing e strutturato nel seguente modo:

- **Help Desk 1° Livello**, sono gli operatori che ricevono il primo contatto da parte dell'Utente in caso di necessità, riescono a dare supporto su tematiche relative all'utilizzo della piattaforma, al processo, al servizio, ecc. Se il supporto non riesce a soddisfare la richiesta viene ingaggiato l'Help Desk di 2° Livello, che a seconda della catalogazione del ticket è rappresentato dall'Area di Assistenza Dematerializzazione e Sicurezza Digitale, dall'Area di Sviluppo software o dall'Area di Produzione;
- **Help Desk 2° Livello**, prende in carico la richiesta dall'Help Desk di primo livello e provvedono alla gestione della problematica secondo la propria competenza ed eventualmente in team con altre competenza multidisciplinari.

Gestione e conservazione dei log

Il sistema di conservazione integra applicativamente la tracciatura tramite un sistema di log di tutte le chiamate/eventi sul sistema. I dati tracciati sono:

- Livello LOG: indica il tipo di informazione tracciata, Debug, Warning, Info.
- Messaggio: informazioni descrittive dell'operazione eseguita.
- Note: i parametri applicativi inviati per l'operazione considerata
- Operazione: la descrizione dell'evento applicativo eseguito
- Utente: il nome dell'utente che ha richiesto l'operazione
- Indirizzo IP: l'eventuale indirizzo IP da dove proviene la richiesta
- Data Creazione: la data di creazione del Log.

I log sono conservati per oltre dieci anni dal Conservatore.

Monitoraggio del sistema di conservazione

Il sistema di conservazione *LegalSolutionDOC* implementa numerosi sotto processi dediti al controllo e al monitoraggio del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al personale incaricato dal Responsabile del Servizio di Conservazione.
Tutte le componenti del sistema sono dotate di un proprio file di log nel quale sono tracciate tutte le operazioni eseguite dal componente e le altre informazioni che permettono di tenere traccia delle attività svolte e facilitare la diagnosi di eventuali anomalie e/o incident.
Il sistema di monitoring adottato SysAid è descritto più dettagliatamente nel Capitolo 9.1.

Change management;

Il processo di change management sul servizio è istanziato dal Cliente attraverso la piattaforma di ticketing, e gestito dall'Area di Assistenza Dematerializzazione e Sicurezza Digitale di 2C Solution e prevede l'avvio del processo attraverso l'aggiornamento e la condivisione di una nuova versione della "Specificità del Contratto". Tale documento recepisce le specifiche di change di servizio e solo se espressamente accettato e condiviso tramite mail dal Produttore dei Documenti, permette di attivare la successiva fase implementativa del change (dal collaudo fino alla messa in produzione).
Il change management dell'infrastruttura di erogazione del servizio, invece, è gestito e descritto dal conservatore 2C Solution secondo la proceduta definita dal SGSI ISO/IEC 27001:2013.

Verifica periodica di conformità a normativa e standard di riferimento

Con periodicità almeno semestrale il Responsabile del servizio di Conservazione effettua un riesame generale del servizio insieme ai soggetti incaricati nell'organigramma per la conservazione, al fine di accertare la conformità del sistema al livello di servizio 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, non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, ecc.). Con periodicità almeno annuale, in accordo con le funzioni interne, il Responsabile del Servizio di Conservazione pianifica processi di audit che coinvolgono aspetti normativi, di processo, organizzazione, tecnologici e logistici, anche con l'intervento di consulenze specifiche.
L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto con i produttori dei documenti, alla documentazione generale del servizio, ai principi che ispirano il sistema qualità e al presente manuale.

Periodicamente sono, inoltre, eseguite delle verifiche di audit sulle funzionalità del sistema di conservazione, principalmente su:

- verifica funzionalità di creazione e mantenimento dei rapporti di versamento, dei pacchetti di archiviazione, ecc.
- verifica funzionalità di distribuzione di pacchetti e documenti ai fini di esibizione e produzione delle copie;
- mantenimento e disponibilità di un archivio del software dei programmi in gestione nelle eventuali diverse versioni, per permettere il ripristino;
- verifica della corretta configurazione delle varie anagrafiche (produttore, responsabile della conservazione, altri soggetti, classi documentali, metadati, privilegi utenti, ecc.)
- verifica del corretto funzionamento delle procedure di sicurezza utilizzate per garantire l'apposizione della firma digitale e della validazione temporale;
- verifica sulla corretta predisposizione e mantenimento della documentazione relativa alla conservazione, anche a fronte di variazione delle condizioni di servizio o a eventi di cui si deve tenere traccia, quali adeguamenti normativi, evoluzioni tecnologiche, subentro di personale in attività previste dalla conservazione, evoluzioni tecnologiche e software, ecc.

Le predette attività di verifica sono riepilogate in un verbale di audit.

Gestione della sicurezza e valutazione del rischio

Per la descrizione della gestione della sicurezza aziendale, dell'analisi dei rischi e della continuità operativa si rimanda a tutta la documentazione relativa al SGSI, certificato ISO/IEC 27001:2013.

Torna al sommario

9 MONITORAGGIO E CONTROLLI

La strategia adottata da 2C Solution prevede che la pianificazione, la struttura organizzativa a supporto e gli strumenti di continuità operativa sviluppati comprendono tutte le misure funzionali, tecnologiche, organizzative e infrastrutturali necessarie per assicurare qualità, sicurezza e affidabilità ai servizi erogati per il produttore dei documenti.

Per il raggiungimento di questo obiettivo le procedure e gli strumenti di monitoraggio e controllo descritti nel seguito sono essenziali.

Torna al sommario

9.1 Procedure di monitoraggio

Il servizio di conservazione di documenti informatici *LegalSolutionDOC* viene costantemente controllato da un sistema di monitoring che rileva malfunzionamenti, anomalie ma anche situazioni critiche che rischiano di degenerare e causare problemi di funzionamento dei moduli che compongono l'intero sistema.

L'area organizzative di Produzione e di Sviluppo Software di 2C Solution sono responsabili dell'infrastruttura e dei sistemi, pertanto effettuano il monitoring on-line e le attività di controllo delle componenti applicative e di impianto con cui vengono erogati i servizi, tramite gli indicatori e i controlli identificati sul Sistema di Gestione della Sicurezza delle Informazioni.

In particolare, il conservatore 2C Solution effettua le attività di controllo avvalendosi della **piattaforma SySAid** sistema di asset management e ticketing, il quale al verificarsi di un evento anomalo legato alle risorse hardware o ai servizi applicativi crea ticket in automatico e li assegna al Responsabile dei sistemi informativi o altro operatore deputato, il quale entro un tempo prestabilito (SLA servizio) deve effettuare le opportune manutenzioni per chiudere l'anomalia, il sistema inoltre prevede delle policy di escalation verso i supervisori nel caso in cui il ticket non venga preso in carico nei tempi prefissati. Il ticket una volta lavorato viene chiuso dall'operatore inserendo le attività effettuate per chiudere l'incidente. Tutti i ticket gestiti rimangono storicizzati nel sistema e costituiscono la base per la creazione dei report di monitoraggio e controllo.

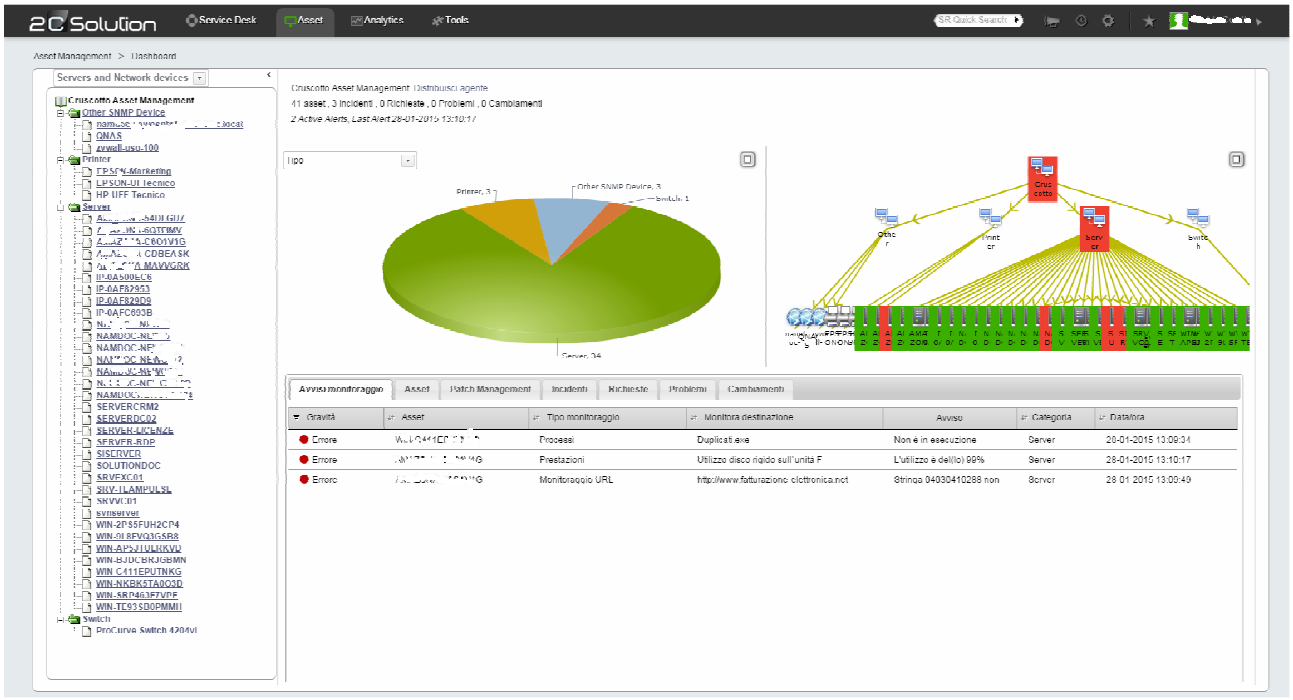

Figura 6 Sistema di Asset Management SysAid Dashborad di controllo

Gli utenti del sistema di conservazione *LegalSolutionDOC* usano la stessa piattaforma per aprire i ticket per richiedere supporto al help desk del servizio. Tali ticket riportano tutte le fasi di gestione del ticket:

- presa in carico della richiesta
- assegnazione
- tutti i messaggi scambiati con l'operatore
- la chiusura del ticket
- le attività effettuate
- il sistema inoltre tiene traccia delle date e ore di gestione.

Il sistema di monitoraggio mantiene i ticket salvati nel proprio data base almeno per 10

anni. In particolare, attraverso il sistema di SysAid, vengono controllati costantemente:

- processi e web services
- La raggiungibilità del servizio da parte dell'utente
- processi di acquisizione documentali (PdV)
- servizio sFTP
- servizi di scheduling (es. processi generazione RdV, PdA, PdD, ecc.)
- servizi di supporto (es. antivirus, servizio di firma, servizio di time stamping)
- occupazione, latenza e performance storage
- processi, transazioni e performance DB
- log del sistema di gestione delle repliche del DB
- servizio di pubblicazione web
- log servizio di pubblicazione web
- log di sistema e funzionalità risorse

- log di procedura e consistenza
- servizio di rotazione legale dei log
- processi backup, replica geografica e DR
- funzionamento sistema di backup e DR
- funzionamento e performance HSM.

Il sistema di gestione degli asset e log management SysAid. rileva grazie all'installazione di un agent sulle macchine di produzione del servizio di conservazione i seguenti dati:

- accesso amministratori di sistema
- hardware e software installato sul server
- uso della CPU, RAM, SPAZIO disco monitorato con intervalli di 5 minuti.

Il sistema inoltre genera in automatico dei report inviati periodicamente al Responsabile dei sistemi informativi e al responsabile della sicurezza. Il dettaglio degli indicatori è riportato nella documentazione del SGSI ISO/IEC 27001:2013.

Ulteriori ed eventuali procedure aggiuntive di monitoraggio e controllo richieste dal soggetto Produttore sono descritte nell'allegato DocumentoSpecificità del contratto".

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Il processo di verifica dell'integrità dei pacchetti informativi e dei documenti nell'ambito del servizio prevede:

- la verifica di corrispondenza sul numero documenti (verifica tra il numero di documenti effettivi presenti nel sistema di conservazione e il numero dei records presenti all'interno della struttura del DB per un determinato produttore);
- Il controllo dell'integrità degli strumenti di validazione apposti sui documenti e sugli Indici dei pacchetti (verifica della firma e della marca temporale su una percentuale prescelta rispetto al totale dei documenti ed indici XML (IPdA) presenti all'interno del sistema di conservazione per un determinato produttore dei documenti).

Per quanto riguarda la verifica di leggibilità, nel sistema di conservazione *LegalSolutionDOC* sono attivi degli automatismi che periodicamente effettuano una serie di controlli su base campionaria estratta tramite un algoritmo pseudocasuale considerando l'insieme degli Id presenti nell'insieme dei documenti conservati. Il campione prodotto da sottoporre a verifica è tale per cui nell'arco dei 5 anni sia garantita la verifica di un campione significativo che rappresenti la totalità dei documenti conservati per ciascun produttore. I controlli eseguiti su questi documenti sono i seguenti:

- verifica di integrità: attraverso il calcolo automatico dell'hash del documento e relativa comparazione con l'hash registrato in fase di creazione del PdA;
- verifica human-readable: sull'insieme dei documenti estratti per la verifica di integrità verrà ulteriormente creato un sottoinsieme di documenti nella percentuale del 1% visualizzati da un operatore delegato che verificherà se il documento è correttamente leggibile ad occhio umano.

A seguito di ogni operazione di controllo verrà prodotto un Verbale di controllo firmato digitalmente dal Responsabile del servizio di Conservazione e conservato nel sistema di conservazione *LegalSolutionDOC*. Ulteriori ed eventuali procedure aggiuntive richieste dal soggetto Produttore sono descritte nell'allegato Documento "Specificità del contratto".

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Le fasi dello schema qui sotto rappresentato il riferimento per tutte le attività della Business Continuity Plan, per la gestione delle anomalie sul sistema di conservazione.

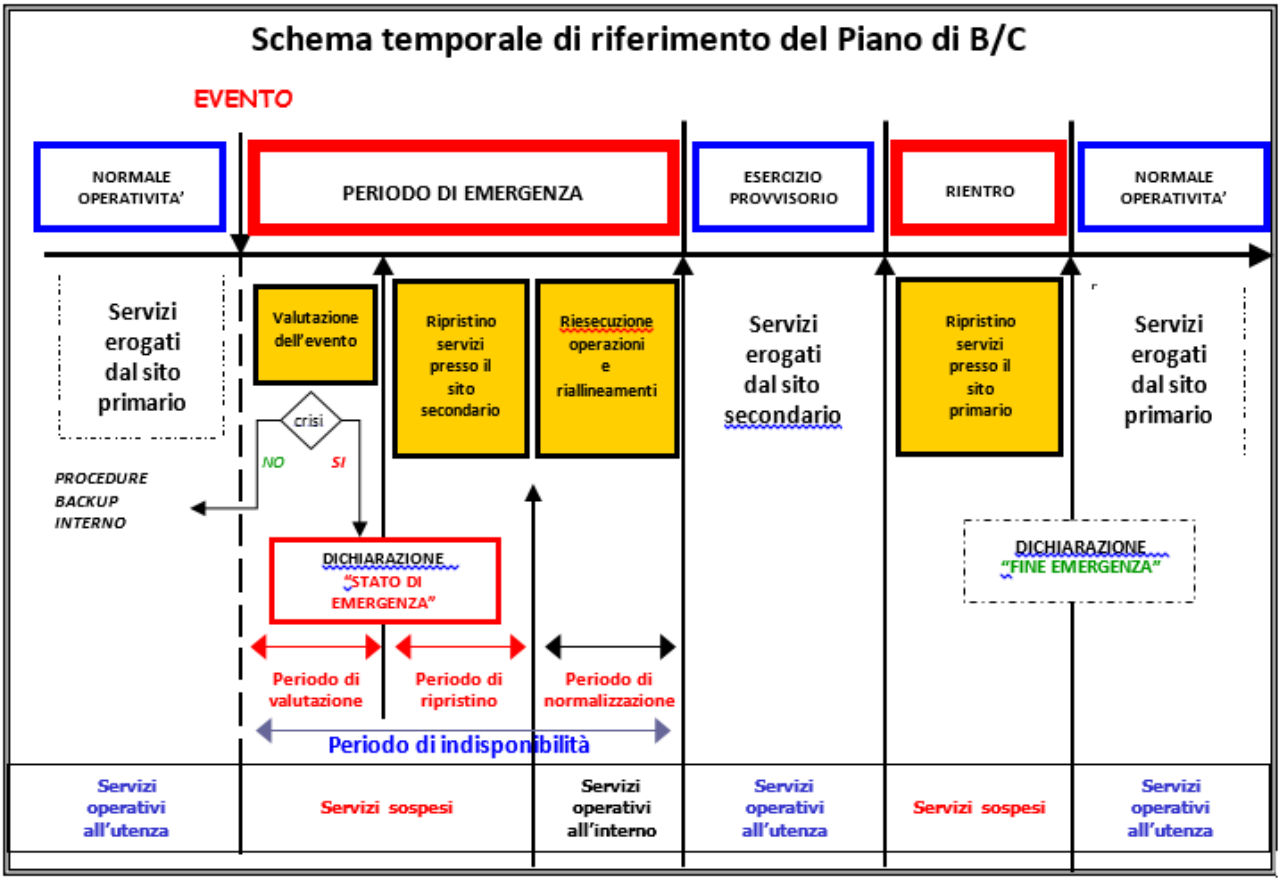

Figura 7 Schema temporale di riferimento del piano di continuità

Normale Operatività: in questa fase vengono gestite tutte le attività che garantiscono la validità del normale operatività. Le attività svolte sono:

- il monitoraggio con idonei strumenti del Sistema di conservazione
- l'apertura di incidenti attraverso la piattaforma di Ticketing, per la loro formalizzazione e gestione
- adeguati processi di comunicazione

Il sistema *LegalSolutionDOC* adotta diversi controlli automatici che garantiscono l'integrità e la coerenza dei dati movimentati dal sistema e durante il processo, i controlli automatici.

Periodo di emergenza: in caso di emergenza 2C Solution seguenti una procedura che rispetta le seguenti fasi:

1. *Valutazione:* in caso di interruzione (totale o parziale) dell'operatività dei servizi erogati, è la fase nella quale si deve decidere se attivare il ripristino presso il Sito Secondario o se è sufficiente avviare le usuali procedure interne per riportare alla normalità l'operatività del Sito Primario.
   Prevede la documentazione dei criteri utilizzati e, se possibile, una stima del danno prodotto dall'interruzione del servizio.
2. *Ripristino: è* la fase durante la quale vengono svolte presso il Sito Secondario le attività di riattivazione e di ricostruzione del sistema informativo se necessario.
3. *Normalizzazione:* è la fase durante la quale viene controllata la validità del sistema informativo ripristinato, con particolare attenzione al contenuto delle basi dati e al funzionamento della connettività tra il Sito Secondario e la rete di utenza.

Esercizio Provvisorio: è la fase durante la quale i servizi informatici sono erogati dal Sito Secondario.
In tale periodo è in corso la risoluzione nel Sito Primario della situazione di emergenza che ha innescato l'avvio del ripristino. In questa fase vengono erogati i servizi indispensabili per mantenere in vita l'azienda/organizzazione.
La durata di questa fase è stimabile in giorni o in settimane, e dipende dal tempo necessario per rendere nuovamente operativo il sito Primario: tale durata può essere sottoposta a limitazioni dovute a vincoli normativi o legali (ad es.: legislazione vigente o questioni relative ad eventuali coperture assicurative).

Rientro: dopo che è stata risolta l'emergenza nel Sito Primario, è la fase durante la quale l'erogazione del servizio informativo interrotto viene trasferita nuovamente dal Sito Secondario al Sito Primario.
Il rientro avviene in modo adeguatamente pianificato, concordato e preventivamente collaudato.

Per una trattazione più dettagliata dell'argomento, si rimanda ai documenti aziendali specifici in ambito di Incident management oggetto di certificazione ISO/IEC 27001:2013 (in particolare ai documenti 2C Solution "Piano della Sicurezza" e "BCP – Business Impact Analisys & Risk analysis"). Eventuali ulteriori accordi specifici concordati con il soggetto Produttore sono descritti nell'allegato "Scheda Sevizio Cliente - Specificità del contratto".

Torna al sommario

Allegato 21 - Linee guida gestione archivi analogici

Si consultino i capitoli relativi contenuti nell'allegato 18.

Allegato 22 – Massimario di conservazione e di scarto dei documenti

L'individuazione del materiale documentario da scartare è un'operazione delicata, da effettuarsi con la dovuta attenzione, subordinata comunque, in base all'art. 21 del decreto legislativo 22 gennaio 2004, n. 42 (Codice dei beni culturali e del paesaggio), all'autorizzazione della Soprintendenza Archivistica.

In linea generale va tenuto presente che, quanto più in passato l'archivio ha subito dispersioni o scarti indiscriminati, tanto più le operazioni di selezione del materiale da eliminare andranno eseguite con prudenza e oculatezza. Per esempio, nel caso in cui non risultino più presenti in archivio i registri della contabilità, andranno necessariamente conservati i documenti analitici, quali mandati e reversali.

Si sottolinea in ogni caso la necessità di garantire la distruzione (con qualunque mezzo ritenuto idoneo) della documentazione da eliminare, allo scopo di impedirne usi impropri, e l'obbligo di trasmettere alla Soprintendenza Archivistica l'attestazione dell'avvenuta distruzione medesima, quale atto conclusivo della pratica.

Il presente massimario si compone di due parti: la prima indica la documentazione fondamentale che deve essere conservata senza limiti di tempo la seconda, invece, la documentazione che può essere proposta per lo scarto dopo il periodo minimo di conservazione espressamente indicato per le varie tipologie. Si noti però che anche in tale seconda parte viene prevista la conservazione illimitata per atti o documenti che rappresentano la riepilogazione e la sintesi delle notizie contenute nel materiale proponibile per lo scarto, assicurando così la conservazione delle informazioni essenziali.

Il massimario, per la grande varietà di tipologie documentarie presenti nella Scuola, non ha la pretesa di essere completamente esaustivo, di comprendere cioè ogni sorta di atto o documento che possa essere prodotto nel corso della quotidiana attività amministrativa, didattica e di ricerca.

PARTE PRIMA: DOCUMENTAZIONE DA CONSERVARE SENZA LIMITI DI TEMPO

- Atti e documenti del contenzioso legale
- Atti relativi ai lavori pubblici, eseguiti e non eseguiti, limitatamente a: originali dei progetti e dei loro allegati, perizie di spesa, libri delle misure
- Bilanci e consuntivi originali (o nell'unica copia esistente)
- Contratti e Convenzioni originali (Quadro, Protocolli d'Intesa, di Ricerca, CNR, UE, rilevante interesse, attività c/terzi, ecc)
- Corrispondenza generale del servizio esattoria e tesoreria
- Corrispondenza, salvo quanto indicato nella seconda parte
- Dichiarazioni periodiche I.V.A., Redditi, INPS, INAIL e ICI
- Documentazione generale per la richiesta di mutui, anche estinti
- Domande a progetti di rilevante interesse nazionale - PRIN
- Fascicoli degli allievi dei corsi di alta formazione e dei master universitari
- Fascicoli degli allievi ordinari, perfezionandi, dottorandi e di laurea specialistica
- Fascicoli dei componenti il Collegio dei Revisori dei Conti, del Nucleo di Valutazione e dei membri delle commissioni degli organi della Scuola
- Fascicoli del personale in servizio e in quiescenza, di ruolo e non di ruolo (comprensivi anche di visite fiscali, ruoli o stati matricolari, informazioni varie per buona condotta, stato professionale, ecc.)
- Inventari dei beni mobili e immobili della Scuola
- Inventari, schedari, rubriche e repertori dell'archivio, libretti o protocolli di trasmissione di carte tra i vari uffici, anche non più in uso

- Libri contabili obbligatori in base alle leggi fiscali
- Libri infortuni o documentazione equivalente
- Libri mastri, libri giornale (relativamente alle spese minute dei Centri di spesa), verbali di chiusura dell'esercizio finanziario (Registro Inventariale e Situazione Patrimoniale)
- Ordinanze e circolari della Scuola, ivi compresi gli ordini di servizio e lettere circolari dei Centri di spesa
- Originali dei Contratti per la stampa di pubblicazioni
- Originali dei Decreti e dei Provvedimenti
- Originali dei verbali dei seggi e delle commissioni elettorali
- Originali dei verbali del Nucleo di valutazione
- Originali dei verbali della Commissione Ricerche e della Commissione Brevetti
- Originali dei verbali delle aste e delle gare
- Originali dei verbali delle commissioni di concorso
- Originali dei verbali di Contrattazione Decentrata (Collettiva)
- Originali dei verbali di riunioni (Centri di Spesa, Commissioni varie istituite dagli organi di governo della Scuola)
- Originali della documentazione inerente i rapporti con i Ministeri (MIUR, Ministero dell'Economia, ecc.)
- Originali delle convocazioni ed ordini del giorno delle sedute degli organi della Scuola, delle Commissioni e dei Gruppi di Lavoro della Scuola, di Contrattazione Decentrata e di ogni altra riunione dalla quale scaturisce un verbale
- Originali delle richieste di accesso ai documenti amministrativi della Scuola e minute delle risposte
- Originali di nomine di referenti e deleghe del Direttore
- Per i corsi di alta formazione e dei master universitari: originali dei verbali delle Commissioni scientifiche, dei rapporti delle verifiche, delle prove di verifica ingresso/intermedie/finali, delle riunioni gruppo di progettazione, della discussione della relazione di tirocinio
- Posizioni previdenziali, stipendiali, tributarie dei dipendenti quando non integralmente conservate nei fascicoli personali
- Programma delle attività annuali dei Centri di Spesa
- Programmi triennali e pluriennali
- Protocolli della corrispondenza in entrata ed in uscita (Protocollo Ufficiale ed ex Protocollo dei Presidi delle Classi)
- Qualunque atto o documento per il quale una legge speciale imponga la conservazione illimitata.
- Rapporti annuali dei Centri di Spesa
- Registri degli atti repertoriati
- Registri dei certificati rilasciati a qualsiasi titolo
- Registri dei Decreti e dei Provvedimenti
- Registro dei diplomi e degli attestati: dei Master universitari, dei corsi di alta formazione, dei corsi di formazione/aggiornamento ai dipendenti della Scuola
- Registro delle non conformità
- Registro delle Note (relativo ad incassi per attività istituzionale)
- Regolamenti e capitolati d'oneri
- Relazione annuale del Direttore amministrativo
- Rilevazioni di carattere statistico non pubblicate
- Ruoli riassuntivi del personale e Libri matricola
- Statuto, Regolamenti, Manuali e Disciplinari (così dette Fonti Interne dalla prima emanazione alle modifiche successive)
- Verbali delle deliberazioni destinate a formare la raccolta ufficiale degli organi di della Scuola

(ex Consiglio direttivo, Consiglio di Amministrazione, Senato Accademico, Consigli delle Classi Accademiche)
- Carteggi relativi ad attività culturali promosse dalla Scuola
- Carteggi relativi ad attività di orientamento
- Carteggi relativi ad attività editoriali su stampa radio e tv
- Carteggi relativi ad attività promozione e illustrativa della Scuola
- Carteggi relativi ai brevetti della Scuola
- Carteggi relativi all'attivazione di Corsi di alta formazione e Master universitari
- Carteggi inerenti la gestione e la contabilizzazione dei lavori svolti dall'Ufficio Tecnico
- Carteggio valutazione dei rischi dei vari immobili
- Carteggio attività di gestione del s Servizio Prevenzione e Protezione
- Carteggio attività sorveglianza sanitaria su lavoratori
- Carteggio interlocutorio e copia di atti per mutui estinti ed accettazioni di eredità
- Carteggio rapporti con enti erogatori di servizi
- Carteggio rapporti Osservatorio Lavori Pubblici
- Carteggio verifiche funzionali impianti

PARTE SECONDA

Documentazione eliminabile dopo cinque anni

- Atti relativi a concorsi a borse di studio e premi (conservando la seguente documentazione: originale degli atti della commissione o dei comitati, gli eventuali rendiconti speciali una copia degli stampati e dei manifesti, il registro delle opere esposte in occasione di mostre artistiche e simili)
- Atti rimessi da altri Enti per notifiche
- Avvisi di convocazione delle commissioni
- Bollettari di prelevamento oggetti dall'Economato
- Bollettari di ricevute dell'esattoria
- Brogliacci di viaggio degli automezzi di proprietà della Scuola
- Carteggi per la richiesta di atti notori e di certificati diversi con eventuale copia degli stessi
- Carteggi relativi alle elezioni: atti generali (atti relativi alla costituzione e all'arredamento dei seggi (conservando il prospetto dei seggi e della loro ubicazione, elenchi degli elettori attivi e passivi, verbali dei Seggi elettorali e delle Commissioni elettorali)
- Carteggi relativi alle spese postali
- Certificazioni per richieste ai fini della fruizione di assegni di studio
- Circolari per l'orario degli uffici e per il funzionamento degli uffici
- Comunicazioni relative a variazioni anagrafiche
- Conto dell'Economato, così dette spese minute (conservando eventuali prospetti generali)
- Copia dei provvedimenti di pagamento di gettoni di presenza ai partecipanti alle commissioni
- Copia di deliberazioni per liquidazione indennità alle Commissioni ed ai Seggi elettorali e ad altre commissioni nominate dalla Scuola
- Copie di attestati di servizio
- Copie di atti notori
- Copie e minute dei progetti, sia realizzati che non realizzati
- Corrispondenza interlocutoria per commemorazioni e solennità civili (conservando carteggi generali per l'organizzazione delle manifestazioni, una copia degli inviti, degli stampati e dei manifesti, gli atti dei comitati, eventuali rendiconti particolari ed eventuali fatture per dieci anni)
- Documenti di carico e scarico dei bollettari delle imposte

- Domande per la richiesta di certificati
- Fascicoli dei docenti esterni per incarichi temporanei di docenza e svolgimento di seminari, lezioni e conferenze (conservando le nomine, i titoli ecc.)
- Lettere di rifiuto di partecipazione alle aste, offerte di ditte non prescelte
- Lettere invito/ringraziamento
- Matrici di bollettari per acquisto materiali di consumo per l'ufficio tecnico
- Registro di carico e scarico dei bollettari
- Rubriche interne per il calcolo dei congedi e delle aspettative
- Solleciti di pagamento fatture pervenuti alla Scuola
- Telegrammi della Prefettura per l'esposizione della bandiera nazionale
- Registri dei materiali di consumo/libri/software
- Registri di cassa delle spese minute
- Registro delle presenze dei Corsi
- Carteggi per l'acquisto di materiali per l'Ufficio tecnico e il magazzino (conservando proposte di spesa, verbali d'asta, contratti)

Documentazione eliminabile dopo sette anni

- Documentazione relativa alle dichiarazioni periodiche I.V.A., Redditi, INPS, INAIL e ICI
- Elenchi sulle modalità di pagamento dei fornitori
- Fogli di lavoro straordinario (conservando eventuali prospetti riassuntivi)
- Fogli di presenza dei dipendenti
- Fogli di presenza dei partecipanti ai corsi di formazione
- Modelli 740 (copia per la Scuola). I sette anni decorrono dall'anno cui si applica la dichiarazione.

Documentazione eliminabile dopo dieci anni

- Atti dei concorsi: copie dei verbali della commissione giudicatrice domande di partecipazione con eventuali titoli e pubblicazioni (ai sensi dei Regolamenti interni) dei candidati (conservando per 40 anni i diplomi originali di studio e/o i documenti militari) copie di manifesti inviate ad altri enti e restituite elaborati scritti e pratici copie di avvisi diversi copie di delibere
- Atti dei corsi di Alta Formazione: copie dei verbali della commissione giudicatrice domande di partecipazione con eventuali titoli e pubblicazioni dei candidati (conservando per 40 anni i diplomi originali di studio e/o i documenti militari) copie di manifesti inviate ad altri enti e restituite elaborati scritti e pratici copie di avvisi diversi copie di delibere
- Atti di liquidazioni di lavoro straordinario per elezioni
- Atti relativi a liquidazione di spese "a calcolo"
- Atti relativi a liquidazione di spese di rappresentanza
- Atti relativi all'alienazione di mobili fuori uso e di oggetti vari
- Buoni di lavoro
- Carteggi di liquidazione delle missioni ai dipendenti, con relative tabelle di missione e documentazione allegata, salvo, se esistenti, prospetti generali
- Carteggi inerenti gli assegni di ricerca
- Copie dei carteggi inerenti la verifica di disponibilità risorse a cofinanziamento
- Copie dei carteggi inerenti le gare di appalto (conservare il verbale delle operazioni d'asta e delle aggiudicazioni, l'elenco delle ditte invitate.)
- Copie dei carteggi inerenti lo stato di avanzamento di lavori pubblici
- Copie dei carteggi per acquisto di attrezzature varie, di mobili e di materiale di cancelleria e

pulizia per uffici, laboratori, ecc. (conservando proposte di spesa, verbali d'asta e contratti) (dettagliare le tipologie secondo l'importo gara europea)
- Copie dei carteggi per acquisto di macchine d'ufficio e di materiale per la loro manutenzione e per la cancelleria (conservando proposte di spesa, verbali d'asta e contratti)
- Copie dei carteggi per acquisto di vestiario per specifiche categorie di dipendenti (conservando proposte di spesa, verbali d'asta e contratti)
- Copie dei carteggi per la fornitura di combustibile per riscaldamento (conservando proposte di spesa, verbali d'asta e contratti)
- Carteggi per l'acquisto di carburante per gli automezzi (conservando proposte di spesa, verbali d'asta e contratti)
- Copia dei carteggi per pulizia di locali (conservando proposte di spesa, verbali d'asta e contratti)
- Carteggi rapporti con enti erogatori di servizi
- Copia dei carteggi relativi a incarichi
- Carteggi relativi a ordinaria e straordinaria manutenzione degli uffici (conservando proposte di spesa, progetti originali, verbali d'asta e contratti)
- Carteggi relativi a prestazioni occasionali, coordinate e continuative e professionali (conservando i contratti originali)
- Carteggi relativi a sottoscrizione di abbonamenti a giornali e riviste e ad acquisto di pubblicazioni amministrative (conservando eventuali carteggi autorizzativi con l'organo di tutela)
- Copia dei carteggi relativi ad acquisto beni/servizi
- Copia dei carteggi relativi ai Bandi di concorso degli allievi della Scuola (ordinario, perfezionando, dottorando, borsista, ecc. premi di studio)
- Carteggi relativi all'ente cassiere (conservando i contratti.)
- Copia dei carteggi relativi alla gestione e rendicontazione dei finanziamenti Ministeriali utilizzati con riferimento specifico all'edilizia
- Copia fatture emesse
- Copia verbali Collegio Revisori dei Conti
- Copie dei mandati e delle reversali e dei loro allegati
- Copie dei preventivi e dei consuntivi (conservando il progetto del bilancio e,caso per caso, i carteggi ad esso relativi)
- Domande e certificazioni di ditte per essere incluse nell'albo degli appaltatori
- Fatture liquidate
- Inviti alle sedute degli organi della Scuola (conservando gli ordini del giorno con elenco dei destinatari)
- Matrici dei buoni d'ordine
- Matricole delle imposte (conservando i ruoli restituiti dall'esattoria e, in mancanza di questi, le loro copie)
- Protocollo buoni di lavoro
- Schedari delle imposte
- Copie delle verifiche di cassa
- Copia contratti in regime di lavoro autonomo
- Mandati di pagamento e riscossione (comprese le eventuali fatture e le cosiddette "pezze d'appoggio", ma conservando i registri e l'eventuale carteggio originale come relazioni, perizie, ecc. che talvolta è rimasto allegato al mandato)

Documentazione eliminabile dopo quindici anni

- Carteggi inerenti contratti per attività di ricerca finanziati da enti pubblici e/o privati

- Copia dei carteggi relativi a Progetti di rilevante interesse nazionale (Attestazioni di conformità tra i modelli in rete e i modelli cartacei relativi ai Progetti PRIN.
- Carteggi inerenti i progetti di rilevante interesse nazionale (PRIN), i contratti Unione Europea, contratti per attività c/terzi, progetti FIRB e FISR (comunque conservati fino a 5 anni dopo la fine del contratto/progetto conservando gli originali delle deliberazioni e dei contratti)

Documentazione eliminabile dopo quarant'anni

- Diplomi originali di studio conservati nella documentazione relativa ai concorsi, eventualmente eliminabili prima dei quarant'anni previa emanazione di un'ordinanza con intimazione al ritiro
- Registri degli atti notificati per altri uffici

Allegato 23 – Elenco degli utenti abilitati

Elenco degli utenti abilitati al trattamento dei documenti

COGNOME E NOME	QUALIFICA
Quilici Simona	Dirigente Scolastico
Talarico Anita	D.S.G.A.
Epifani Nicola	Assistente amministrativo
Marmo Rosa Maria	Assistente amministrativo
Sblendido Leonora	Assistente amministrativo
Morgante Luisa	Assistente amministrativo
D'Urso Lucia	Assistente amministrativo
Lazzarotto Chiara	Assistente amministrativo
Chiellino Massimiliano	Assistente amministrativo
Rinaldi Umberto	Assistente amministrativo
	Assistente amministrativo
	Assistente amministrativo
	Assistente amministrativo
	Assistente amministrativo
	Assistente amministrativo

Allegato 24: Regolamento per l'accesso agli atti

Il regolamento per l'accesso civico agli atti archiviati in questo Istituto è pubblicato sul sito istituzionale, nella sezione:

Amministrazione Trasparente – Altri Contenuti – Accesso civico

e mantenuto aggiornato.

Allegato 25: Programma triennale per la trasparenza e l'integrità

Il Programma triennale per la trasparenza e l'integrità è pubblicato sul sito istituzionale, nella sezione:

Amministrazione Trasparente – Disposizioni generali