ISTITUTO COMPRENSIVO STATALE "Ermanno Olmi"
Cod. Mecc. MIIC8FP00T - C.F. 97667360156
e-mail: miic8fp00t@istruzione.it pec: miic8fp00t@pec.istruzione.it

Scuola Secondaria Primo Grado Via Maffucci, 60 - 20158 MILANO
☎02/88447160 – 02/88447164 fax
Scuola Primaria "M. Curie" Via Guicciardi,1 -20158 MILANO
☎02/88446931 – 02/39320412 fax
Scuola Primaria "G. Leopardi" . V.le Bodio, 22 -20158 MILANO
☎02/88446840 – 02/88446842 fax

Milano, 20 dicembre 2022
Protocollo vedi timbratura

Alla Pubblicità Legale (Albo online) di istituto
Alla Amministrazione Trasparente di istituto

Oggetto: **Adozione del Titolario di classificazione, del Massimario di conservazione e scarto, e del Manuale di gestione documentale.**

IL DIRIGENTE SCOLASTICO

- Visto dall'art. 44, comma 2), lettera h), del DPCM 2 dicembre 2019, n. 169;
- Viste le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate dall'AgID con Determinazione n. 407/2020 del 9 settembre 2020 ed in seguito aggiornate con Determinazione n. 371/2021 del 17 maggio 2021;
- Vista la circolare Ministero Istruzione 3868 del 10/12/2021;
- Vista la Circolare n. 8 del 24 gennaio 2017 del Ministero dei Beni e delle Attività Culturali e del Turismo in cui il titolario Titulus Scuola viene indicato come lo strumento per la classificazione dei documenti, nonché nella corretta formazione e gestione degli archivi delle Scuole;
- Rilevata in data odierna la mancanza della disposizione dirigenziale di adozione del Titolario di classificazione, del Massimario di conservazione e scarto, e del Manuale di gestione documentale
- Considerato che la pubblicazione del documento era prevista entro il 31 Dicembre del 2021

DISPONE

Ora per allora l'adozione del Titolario di classificazione, del Massimario di conservazione e scarto, e del Manuale di gestione documentale.
Sono allegati al presente provvedimento, e ne costituiscono parte integrante e sostanziale:

- Titolario di classificazione;
- Massimario di conservazione e scarto;
- Manuale di gestione documentale.

Il suddetto manuale sarà aggiornato periodicamente in funzione dell'attuazione del processo di "Transizione Digitale" e dell'attuazione delle misure di sicurezza digitale.

I documenti adottati saranno ratificati al prossimo Consiglio di Istituto.

Il Dirigente Scolastico
ROBERTA COLOMBO

Firmato da:
COLOMBO ROBERTA
Dirigente scolastica IC Statale "E.Olmi" - Milano
20/12/2022 16:02:36

ISTITUTO	**Istituto Comprensivo Ermanno Olmi**
INDIRIZZO	**Via Maffucci, 60**
CAP / CITTA'	**20158 Milano (MI)**
CODICE MECCANOGRAFICO E CODICE FISCALE	**MIIC8FP00T - 97667360156**
SITO WEB	**https://www.icmaffucci.edu.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

Allegato 25: Programma triennale per la trasparenza e l'integrità

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		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 Ermanno Olmi[5] composta dall'insieme di tutte le sue unità organizzative come da elenco allegato (Allegato n. 2). Il codice identificativo dell'area è[6] A63D830.

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.
Il Responsabile della conservazione, di concerto con il Responsabile dei sistemi informativi

[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.

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 dei

[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

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 l'etichettatrice.

- 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 giuridicii 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).

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 successivamente

[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.

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].

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

[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.
[46] Alcuni esempi di software gestionali che possono essere legati al sistema di protocollo riguardano la gestione SUAP, SUE. Altri

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].

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 [60].

[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] Ogni anno si costituiscono fascicoli standard all'interno di ogni classe del titolario (es. il fascicolo del bilancio preventivo, il

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 archivistiche. In presenza di documenti cartacei da inserire in fascicoli informatici, dovrà essere prodotta copia per immagine degli stessi secondo la normativa vigente.

---

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.

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 responabili.

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*

Ogni anno il responsabile del servizio di gestione documentale provvede ad effettuare il censimento dei

[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..

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.

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

[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

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 pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti, fatti salvi i diversi termini previsti dalla

[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.
[85] Indicare i tipi di formato aperto.

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".

[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[87] Istituto Comprensivo Ermanno Olmi, 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 Ermanno Olmi**
Codice identificativo assegnato all'Amministrazione	MIIC8FP00T
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	Via Maffucci 60 – Milano (MI)
Elenco delle AREE ORGANIZZATIVE OMOGENEE – AOO	A63D830

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

Determinazione prot. n. 5065 del 20.12.2022

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	Istituto Comprensivo Ermanno Olmi
INDIRIZZO	Via Maffucci 60
CITTA'	20158 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 nella Dott.ssa Arconti Alessandra Maria, 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 la signora Dott.ssa Arconti Alessandra Maria, 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 signor Arconti Domenico 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. Fabio Cavallo, in qualità di Amministratore della società:

SOCIETA'	INTERSCREEN
INDIRIZZO	Viale Martesana 115
CITTA'	Vimodrone (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. 5066 del 20.12.2022

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

In data odierna, nell'amministrazione di

ISTITUTO	Istituto Comprensivo Ermanno Olmi
INDIRIZZO	Via Maffucci 60
CITTA'	20158 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 nella signora Dott.ssa Arconti Alessandra Maria, in servizio presso la Segreteria di questaIstituzione, 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 la Dott.ssa Alessandra Maria Arconti, quale Responsabile del Servizio di conservazione a norma coni 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. 5067 del 20.12.2022

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

In data odierna, nell'amministrazione di

ISTITUTO	Istituto Comprensivo Ermanno Olmi
INDIRIZZO	Via Maffucci 60
CITTA'	20158 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. 5065 del 20.12.2022 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 nella signora Dott.ssa Arconti Alessandra Maria, 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 la Dott.ssa Alessandra Maria Arconti, 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 5del 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 ilPdP;
- 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 (Easyteam.org via Walter Tobagi, 2 Tribiano (MI) 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 uno 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 dala Circolare AgID 2/2017, 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 Filomena Madonna, 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 protocolloi 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 chesi 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

MASSIMARIO DI CONSERVAZIONE E SCARTO PER LE ISTITUZIONI SCOLASTICHE

STRUTTURA DEL MASSIMARIO

Al fine di garantire l'integrazione del massimario con il sistema di classificazione, la struttura del massimario si articola su tre livelli: il primo e il secondo livello corrispondono rispettivamente al titolo (I livello) e alla classe (II livello) del titolario di classificazione. Il terzo livello definisce le tipologie documentarie associate a ciascuna classe; per ciascuna tipologia documentaria sono fornite indicazioni in merito ai tempi di conservazione.

Ciò premesso, al fine di agevolare la consultazione del documento, si riporta di seguito la struttura del massimario.

I. AMMINISTRAZIONE

I.1 Normativa e disposizioni attuative
I.2 Organigramma e funzionigramma
I.3 Statistica e sicurezza di dati e informazioni
I.4 Archivio, accesso, privacy, trasparenza e relazioni con il pubblico
I.5 Registri e repertori di carattere generale
I.6 Audit, qualità, carta dei servizi, valutazione e autovalutazione
I.7 Elezioni e nomine
I.8 Eventi, cerimoniale, patrocini, concorsi, editoria e stampa

II. ORGANI E ORGANISMI

II.1 Consiglio di istituto, Consiglio di circolo e Consiglio di Amministrazione
II.2 Consiglio di classe e di interclasse
II.3 Collegio dei docenti
II.4 Giunta esecutiva
II.5 Dirigente scolastico DS
II.6 Direttore dei servizi generali e amministrativi DSGA
II.7 Comitato di valutazione del servizio dei docenti
II.8 Comitato dei genitori, Comitato studentesco e rapporti scuola-famiglia
II.9 Reti scolastiche
II.10 Rapporti sindacali, contrattazione e Rappresentanza sindacale unitaria (RSU)
II.11 Commissioni e gruppi di lavoro

III. ATTIVITÀ GIURIDICO-LEGALE

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

IV. DIDATTICA

IV.1 Piano triennale dell'offerta formativa PTOF
IV.2 Attività extracurricolari
IV.3 Registro di classe, dei docenti e dei profili
IV.4 Libri di testo
IV.5 Progetti e materiali didattici
IV.6 Viaggi di istruzione, scambi, stage e tirocini
IV.7 Biblioteca, emeroteca, videoteca e sussidi
IV.8 Salute e prevenzione
IV.9 Attività sportivo-ricreative e rapporti con il Centro Scolastico Sportivo
IV.10 Elaborati e prospetti scrutini

V. STUDENTI E DIPLOMATI

V.1 Orientamento e placement
V.2 Ammissioni e iscrizioni
V.3 Anagrafe studenti e formazione delle classi
V.4 Cursus studiorum
V.5 Procedimenti disciplinari
V.6 Diritto allo studio e servizi agli studenti (trasporti, mensa, buoni libro, etc.)

V.7 Tutela della salute e farmaci
V.8 Esoneri
V.9 Prescuola e attività parascolastiche
V.10 Disagio e diverse abilità – DSA

VI. FINANZA E PATRIMONIO

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

VII. PERSONALE

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

I LIVELLO: Amministrazione

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.1	**Normativa e disposizioni attuative**	I.1.1	Leggi, regolamenti e tutta la documentazione relativa a: - istituzione della scuola - intitolazione - eventuali accorpamenti e trasformazioni (ad es. in istituto comprensivo)	ILLIMITATI
		I.1.2	Norme e regolamenti interni (regolamento dell'istituto, carta dei servizi, regolamenti della biblioteca, dei laboratori e direttive varie ecc.)	ILLIMITATI
		I.1.3	Norme e disposizioni Economato	ILLIMITATI
		I.1.4	Norme e disposizioni relative al personale e CCNL	50 anni dall'entrata in vigore
		I.1.5	Circolari e ordinanze interne esplicative e direttive	ILLIMITATI di almeno 1 esemplare per circolare/ordinanza
		I.1.6	Norme e disposizioni relative all'archivio	ILLIMITATI
		I.1.7	Norme e disposizioni relative a pensione e trattamento di quiescenza	Scartabile dopo 10 anni dalla decadenza
		I.1.8	Regolamenti delle biblioteche dell'Istituto (dei docenti, degli alunni, ecc)	ILLIMITATI
I.2	**Organigramma e funzionigramma**	I.2.1	Documentazione relativa a organico dell'autonomia, organico docenti, organico ATA	ILLIMITATI
I.3	**Statistica e sicurezza di dati e informazioni**	I.3.1	Documento programmatico di sicurezza dati (DPS)	ILLIMITATI
		I.3.2	Inchieste, indagini (ambientali, socio-economiche, sanitarie, ecc.)	ILLIMITATI
		I.3.3	Statistiche	ILLIMITATI
I.4	**Archivio, accesso, privacy, trasparenza e relazioni con il pubblico**	I.4.1	Documenti relativi alla privacy e alla protezione dei dati	ILLIMITATI
		I.4.2	Titolari di classificazione d'archivio (compresi quelli non più in uso)	ILLIMITATI
		I.4.3	Scarto di atti d'archivio (procedure, elenchi, autorizzazioni e verbali di distruzione…)	ILLIMITATI
		I.4.4	Registri di protocollo (generali e riservati)	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.4	**Archivio, accesso, privacy, trasparenza e relazioni con il pubblico**	I.4.5	Repertori dei fascicoli d'archivio	ILLIMITATI
		I.4.6	Rubriche alfabetiche del protocollo	ILLIMITATI
		I.4.7	Registro della posta in partenza e/o documentazione attestante la spedizione o la ricezione (anche a mano o mediante affissione in bacheca)	10 anni dalla data dell'ultima registrazione (salvo contenziosi in corso)
		I.4.8	Richiesta di accesso ai documenti	Scartabili dopo 1 anno, conservando illimitatamente eventuali registri delle richieste (salvo contenziosi in corso)
		I.4.9	Richieste di copie di atti e relativo rilascio	Scartabili dopo 1 anno, conservando illimitatamente eventuali registri delle copie rilasciate
		I.4.10	Richieste di certificati e loro trasmissione	Scartabili dopo 6 anni
		I.4.11	Bollettario di richiesta degli stampati	Scartabile dopo 6 anni
		I.4.12	Richieste di consultazione dell'archivio della scuola per finalità storico-culturali	Scartabili dopo 6 anni, conservando illimitatamente il registro delle consultazioni
I.5	**Registri e repertori di carattere generale**	I.5.1	Registro verbali riunioni per contrattazione d'istituto	ILLIMITATI
		I.5.2	Registri dei verbali del Consiglio o Staff di Presidenza	ILLIMITATI
		I.5.3	Registri dei verbali degli Organi collegiali (Consiglio di circolo o di istituto, Giunta esecutiva, Collegio docenti, Consigli di classe o di interclasse) e degli eventuali gruppi di lavoro derivati (es. dipartimenti, commissioni, ambiti disciplinari ecc)	ILLIMITATI
		I.5.4	Registro delle deliberazioni	ILLIMITATI
		I.5.5	Registri dei contratti per fornitura di materiali, espletamento di servizi, assunzione personale	ILLIMITATI
		I.5.6	Registro cronologico dei contratti	ILLIMITATI
		I.5.7	Registri dei verbali della cassa scolastica	ILLIMITATI
		I.5.8	Registri dei materiali di facile consumo	Scartabili dopo 10 anni

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.5	**Registri e repertori di carattere generale**	I.5.9	Registro delle tasse e dei contributi scolastici (iscrizione, diploma…)	Scartabile dopo 10 anni dall'ultima registrazione, conservando a campione una annata ogni dieci
		I.5.10	Registro dei verbali dei Revisori dei conti	ILLIMITATI
		I.5.11	Inventari patrimoniali (registri inventariali) dei beni mobili; registri di entrata della biblioteca; registri di entrata dei sussidi multimediali; inventari e repertori dell'archivio	ILLIMITATI
		I.5.12	Registro di magazzino	Scartabile dopo 6 anni
		I.5.13	Registro licenze software	ILLIMITATI
		I.5.14	Registro delle tessere di riconoscimento (Mod. AT)	ILLIMITATI
		I.5.15	Registri delle autorizzazioni ad impartire lezioni private	Scartabili dopo 6 anni dall'ultima registrazione
		I.5.16	Registri dello stato personale	ILLIMITATI
		I.5.17	Registro degli stipendi ed altri assegni	ILLIMITATI
		I.5.18	Registri degli infortuni	ILLIMITATI
		I.5.19	Registri dei certificati di servizio rilasciati dalla scuola	ILLIMITATI
		I.5.20	Registri assenze	Scartabili dopo 50 anni
		I.5.21	Registri di immatricolazione e/o di iscrizione degli alunni	ILLIMITATI
		I.5.22	Registri generali dei voti, delle valutazioni	ILLIMITATI
		I.5.23	Registri dei certificati di studio rilasciati dalla scuola	ILLIMITATI
		I.5.24	Registri e verbali del debito formativo	Scartabili dopo 10 anni, conservando illimitatamente un anno a campione ogni 5
		I.5.25	Registro riunioni per materia	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.5	**Registri e repertori di carattere generale**	I.5.26	Registro riunioni per dipartimento	ILLIMITATI
		I.5.27	Registri dei verbali degli scrutini	ILLIMITATI
		I.5.28	Registri dei verbali degli esami e delle relative prove	ILLIMITATI
		I.5.29	Registri di carico e scarico dei diplomi	ILLIMITATI
		I.5.30	Registri di consegna dei diplomi	ILLIMITATI
I.6	**Audit, qualità, carta dei servizi, valutazione e autovalutazione**	I.6.1	Certificazioni di qualità e accreditamenti (es. ministeriali e regionali, ecc.)	ILLIMITATI
		I.6.2	Verbali di ispezione	ILLIMITATI
		I.6.3	Relazioni finali di istituto	ILLIMITATI
		I.6.4	Questionari e monitoraggio	Scartabili dopo un anno, conservando illimitatamente una copia in bianco del questionario e i suoi risultati sintetici
		I.6.5	Valutazioni, rilevazioni dati, e relazioni sull'attività della scuola, redatte sia da personale interno sia da esterni (INVALSI, OCSE- PISA, ecc.)	ILLIMITATI
I.7	**Elezioni e nomine**	I.7.1	Verbali delle Commissioni Elettorali. Atti di nomina degli Organi collegiali a livello di circolo e di istituto	ILLIMITATI
		I.7.2	Atti delle elezioni degli Organi collegiali: - verbale di consegna di materiale elettorale - liste candidati - elenchi elettori - certificati elettorali - scheda votazioni - prospetti per il calcolo dei voti - tabelle scrutinio	Scartabili dopo 6 anni dalle elezioni conservando 1 campione di scheda non utilizzata per ciascuna elezione e per ciascuna categoria di elettori
		I.7.3	Atti di nomina di commissioni, comitati, e gruppi di lavoro	ILLIMITATI
I.8	**Eventi, cerimoniale, patrocini, concorsi, editoria e stampa**	I.8.1	Documentazione relativa a cerimonie, inaugurazioni e relazioni esterne	Scartabili dopo 10 anni
		I.8.2	Giornalini di classe o d'istituto	ILLIMITATI di almeno un esemplare

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.8	**Eventi, cerimoniale, patrocini, concorsi, editoria e stampa**	I.8.3	Annuari, rassegna stampa e pubblicazioni varie della scuola	ILLIMITATI di almeno un esemplare degli annuari e delle pubblicazioni e della rassegna stampa
		I.8.4	Locandine e manifesti di qualsiasi tipo pubblicati o stampati dalla o per conto della scuola	Scartabili dopo 10 anni

I LIVELLO: Organi e organismi

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
II.1	**Consiglio di istituto, Consiglio di circolo e Consiglio di Amministrazione**	II.1.1	Verbali Consiglio di Istituto e Consiglio di circolo	ILLIMITATI
		II.1.2	Verbali del Consiglio di Amministrazione	ILLIMITATI
		II.1.3	Convocazioni riunioni Consiglio di istituto e Consiglio di circolo	Scartabili dopo 6 anni
II.2	**Consiglio di classe e di interclasse**	II.2.1	Verbali Consiglio di classe e di interclasse	ILLIMITATI
		II.2.2	Convocazioni riunioni Consiglio di classe e di interclasse	Scartabili dopo 6 anni
II.3	**Collegio dei docenti**	II.3.1	Verbali Collegio dei docenti	ILLIMITATI
		II.3.2	Convocazioni riunioni Collegio dei docenti	Scartabili dopo 6 anni
II.4	**Giunta esecutiva**	II.4.1	Verbali Giunta esecutiva	ILLIMITATI
		II.4.2	Convocazioni riunioni Giunta esecutiva	Scartabili dopo 6 anni
II.5	**Dirigente scolastico DS**	II.5.1	Determinazioni dirigenziali (raccolte in serie cronologiche)	ILLIMITATI
		II.5.2	Piano delle attività dei docenti	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
II.6	**Direttore dei servizi generali e amministrativi DSGA**	II.6.1	Ordini di servizio generali	ILLIMITATI
		II.6.2	Piano delle attività del personale ATA	ILLIMITATI
II.7	**Comitato di valutazione del servizio dei docenti**	II.7.1	Verbali di valutazione dei docenti	ILLIMITATI
		II.7.2	Convocazione riunioni Comitato di valutazione	Scartabili dopo 5 anni
II.8	**Comitato dei genitori, Comitato studentesco e rapporti scuola-famiglia**	II.8.1	Comunicazioni da parte di Comitato studentesco, Comitato dei genitori e famiglie	Scartabili dopo 5 anni
		II.8.2	Verbali di Comitato studentesco e Comitato dei genitori	ILLIMITATI
		II.8.3	Convocazione riunioni Comitato studentesco e Comitato dei genitori	Scartabili dopo 5 anni
II.9	**Reti scolastiche**	II.9.1	Convenzioni e accordi di rete (con scuole, con enti ecc.)	ILLIMITATI
II.10	**Rapporti sindacali, contrattazione e Rappresentanza sindacale unitaria (RSU)**	II.10.1	Contrattazione d'istituto	ILLIMITATI
		II.10.2	- Rapporti con organizzazioni sindacali e rappresentanze interne - Scioperi	ILLIMITATI
II.11	**Commissioni e gruppi di lavoro**	II.11.1	Verbali, documenti istruttori e deliberativi di Commissioni e gruppi di lavoro	ILLIMITATI
		II.11.2	Convocazione riunioni delle Commissioni e gruppi di lavoro	Scartabili dopo 5 anni

I LIVELLO: Attività giuridico-legale

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
III.1	**Contenzioso**	III.1.1	Documentazione prodotta e acquisita nel corso di transazioni, conciliazioni e ricorsi amministrativi e giurisdizionali	ILLIMITATI
		III.1.2	Azioni legali collettive del personale	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
III.2	**Violazioni amministrative e reati**	III.2.1	Documentazione relativa a violazioni amministrative e reati (denunce alle forze dell'ordine, sanzioni amministrative, ecc.)	ILLIMITATI
III.3	**Responsabilità civile, penale e amm.va**	III.3.1	Recupero retribuzione dipendenti assenti dal lavoro per responsabilità di terzi	Scartabile dopo 50 anni
III.4	**Pareri e consulenze**	III.4.1	Relazioni su collaborazioni con (o consulenze da parte di): - istituzioni socio-assistenziali - enti locali - cooperative ed associazioni - Tribunale dei minori - servizio sanitario nazionale	ILLIMITATI
		III.4.2	Pareri legali	ILLIMITATI

I LIVELLO: Didattica

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
IV.1	**Piano Triennale dell'Offerta Formativa PTOF**	IV.1.1	Piano Triennale dell'Offerta Formativa (PTOF)	ILLIMITATI
IV.2	**Attività extracurricolari**	IV.2.1	Attività formative (teatro, musica, interventi di recupero, inserimento alunni stranieri, patentino ecc.)	ILLIMITATI
		IV.2.2	Progetti operativi nazionali (PON); Progetti operativi regionali (POR);	ILLIMITATI
		IV.2.3	Documentazione per programmazione ed attuazione di attività scolastiche anche esterne (manifestazioni teatrali, ecc.)	Scartabile dopo 6 anni, conservando illimitatamente a campione un'annata ogni 10
IV.3	**Registro di classe, dei docenti e dei profili**	IV.3.1	Recupero orario: relazioni, dichiarazioni e autocertificazioni	Scartabili dopo 10 anni
		IV.3.2	Orari delle lezioni	ILLIMITATI di un esemplare dell'orario di ciascuna classe di tutte le sezioni, scartando dopo un anno eventuali copie d'uso e dopo 6 anni gli atti relativi alla definizione dell'orario

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
IV.3	**Registro di classe, dei docenti e dei profili**	IV.3.3	Registri dei profili degli alunni redatti dai Consigli di classe	ILLIMITATI
		IV.3.4	Registri di classe	ILLIMITATI
		IV.3.5	Registri personali dei docenti	ILLIMITATI fino all'anno scolastico 1969/70. Successivamente scartabili dopo 10 anni, conservando illimitatamente un anno ogni 5
		IV.3.6	Registri delle assenze degli alunni (e relativa documentazione)	Scartabili dopo 6 anni
IV.4	**Libri di testo**	IV.4.1	Verbali e relazioni riguardanti l'adozione dei libri di testo	ILLIMITATI
IV.5	**Progetti e materiali didattici**	IV.5.1	Piani di lavoro, Programmi, Relazioni finali di classe	ILLIMITATI
		IV.5.2	Piano Educativo Individualizzato (PEI)	ILLIMITATI nel fascicolo personale dell'alunno
		IV.5.3	Programmi d'esame	ILLIMITATI
		IV.5.4	Documenti prodotti da docenti e studenti in preparazione e nel corso di attività didattiche (dispense, percorsi, sussidi, sperimentazioni multidisciplinari, testi teatrali, sceneggiature cinematografiche ecc.)	ILLIMITATI di almeno un esemplare
		IV.5.5	Progetti curricolari	ILLIMITATI
IV.6	**Viaggi di istruzione, scambi, stage e tirocini**	IV.6.1	Pratiche per assistenza e soggiorni climatici /colonie	ILLIMITATI
		IV.6.2	Borse di studio / stage: bandi, studi e relazioni	ILLIMITATI
		IV.6.3	Documentazione per programmazione ed attuazione di attività scolastiche anche esterne (gite, visite di studio ecc.)	Scartabile dopo 6 anni, conservando illimitatamente a campione un'annata ogni 10
		IV.6.4	Documentazione relativa ai PCTO (Percorsi per le Competenze Trasversali e l'Orientamento)	ILLIMITATI
IV.7	**Biblioteca, emeroteca, videoteca e sussidi**	IV.7.1	Contributi per biblioteca scolastica (documentazione relativa)	Scartabili dopo 6 anni, conservando illimitatamente il registro cronologico di entrata (vedi I.5.11)
		IV.7.2	Cataloghi e regolamenti delle biblioteche dell'Istituto (dei docenti, degli alunni, ecc)	ILLIMITATI
IV.8	**Salute e prevenzione**	IV.8.1	Educazione alla salute: progetti, interventi e convenzioni	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
IV.9	**Attività sportivo-ricreative e rapporti con il Centro Scolastico Sportivo**	IV.9.1	Autorizzazioni all'uso di locali scolastici e impianti sportivi	Scartabili dopo 6 anni, conservando eventuali atti riassuntivi
		IV.9.2	Progetti formativi relativi a sport	ILLIMITATI
		IV.9.3	Registri attività del Gruppo sportivo	Scartabili dopo 10 anni
IV.10	**Elaborati e prospetti scrutini**	IV.10.1	Elaborati delle prove scritte, grafiche e pratiche degli alunni (esclusi quelli prodotti per l'esame di Stato)	Scartabili dopo un anno, conservando illimitatamente a campione una annata ogni 10
		IV.10.2	Elaborati delle prove scritte, grafiche per gli esami di Stato	ILLIMITATI nel plico dell'esame
		IV.10.3	Elaborati delle prove pratiche per gli esami di Stato	Scartabili dopo un anno conservando nel plico dell'esame le fotografie dei manufatti
		IV.10.4	Elaborati delle prove Invalsi	Scartabili dopo un anno, conservando illimitatamente a campione una annata ogni 10
		IV.10.5	Prospetti scrutini trimestrali o quadrimestrali	ILLIMITATI
		IV.10.6	Prospetti scrutinio finale	ILLIMITATI

I LIVELLO: Studenti e diplomati

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
V.1	**Orientamento e placement**	V.1.1	Progetti formativi relativi a orientamento e placement	ILLIMITATI
V.2	**Ammissioni e iscrizioni**	V.2.1	Elenchi alunni per iscrizioni	Scartabili dopo 10 anni
		V.2.2	Domande e documenti prodotti da alunni e candidati per l'iscrizione ai vari tipi di scuola e per l'ammissione agli esami	Scartabili dopo 6 anni dalla fine dell'appartenenza all'Istituto o dall'iscrizione all'esame
V.3	**Anagrafe studenti e formazione delle classi**	V.3.1	Certificati di nascita	Scartabili dopo 6 anni dalla cessazione dell'appartenenza all'Istituto o dall'iscrizione agli esami, con l'eccezione dei documenti degli allievi stranieri

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
V.3	**Anagrafe studenti e formazione delle classi**	V.3.2	Documentazione relativa alla formazione delle classi	Scartabili dopo 10 anni
V.4	***Cursus studiorum***	V.4.1	Relazioni inerenti le ripetenze degli alunni	ILLIMITATI nei rispettivi fascicoli personali
		V.4.2	Fascicoli personali alunni	ILLIMITATI
		V.4.3	Pagelle scolastiche Schede di valutazione Schede alunni	ILLIMITATI
		V.4.4	Libretti scolastici e altra documentazione relativa agli studi dell'alunno (es. Portfolio)	ILLIMITATI
		V.4.5	Certificazioni delle competenze	ILLIMITATI
V.5	**Procedimenti disciplinari**	V.5.1	Sanzioni disciplinari agli alunni	ILLIMITATI
V.6	**Diritto allo studio e servizi agli studenti (trasporti, mensa, buoni libro, etc.)**	V.6.1	- Elenchi dei buoni libro concessi e documentazione di supporto - Cedole librarie	Scartabili dopo 6 anni, conservando illimitatamente l'elenco dei percipienti ed eventuali relazioni o rendiconti speciali
		V.6.2	Mensa: richieste di iscrizione al servizio mensa ed elenchi presenze	Scartabili dopo 6 anni, conservando illimitatamente contratti, relazioni sull'attività, diete e menu seguiti
		V.6.3	Trasporto alunni: richieste di iscrizione al servizio ed attestazioni di pagamento	Scartabili dopo 6 anni
		V.6.4	Trasporto alunni: richieste per trasporto gratuito	Scartabili dopo 6 anni, conservando elenchi riassuntivi
		V.6.5	Certificazioni per richieste di abbonamenti ferroviari e diversi	Scartabili dopo 1 anno
		V.6.6	Documentazione riguardante assistenza scolastica e Patronato scolastico	ILLIMITATI
		V.6.7	Documentazione riguardante il diritto allo studio	ILLIMITATI
		V.6.8	Certificazioni per richieste ai fini della fruizione di assegni di studio	Scartabili dopo 10 anni
V.7	**Tutela della salute e farmaci**	V.7.1	Certificati di vaccinazione	Scartabili dopo 6 anni dalla cessazione dell'appartenenza all'Istituto o dall'iscrizione agli esami, con l'eccezione dei documenti degli allievi stranieri
		V.7.2	Campagne di vaccinazione e disinfestazione, atti e documenti relativi alla loro effettuazione	Scartabili dopo 6 anni, conservando illimitatamente la documentazione e i registri riassuntivi

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
V.8	**Esoneri**	V.8.1	Documentazione relativa ad esoneri	ILLIMITATI nel fascicolo personale
V.9	**Prescuola e attività parascolastiche**	V.9.1	Cooperative di alunni: atti costitutivi, documenti istruttori e deliberativi, corrispondenza	ILLIMITATI
		V.9.2	Convenzioni per attività formative e parascolastiche	ILLIMITATI
V.10	**Disagio e diverse abilità – DSA**	V.10.1	Schede individuali degli alunni (schedario)	ILLIMITATI

I LIVELLO: Finanza e patrimonio

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VI.1	**Entrate e finanziamenti del progetto**	VI.1.1	Partitario delle Entrate	ILLIMITATI
		VI.1.2	Reversali con la relativa documentazione giustificativa (fatture, corrispondenza varia)	Scartabili dopo 10 anni (previa verifica della conservazione dei rispettivi giornali di cassa e partitari) conservando illimitatamente progetti, collaudi, perizie degli impianti e delle manutenzioni straordinarie delle attrezzature durevoli (macchinari tecnici, arredi di particolare interesse, ecc.)
VI.2	**Uscite e piani di spesa**	VI.2.1	Partitario delle Uscite	ILLIMITATI
		VI.2.2	Mandati di pagamento con la relativa documentazione giustificativa (ordinativi di acquisto, buoni d'ordine, fatture, corrispondenza varia)	Scartabili dopo 10 anni (previa verifica della conservazione dei rispettivi giornali di cassa e partitari) conservando illimitatamente progetti, collaudi, perizie degli impianti e delle manutenzioni straordinarie delle attrezzature durevoli (macchinari tecnici, arredi di particolare interesse, ecc.)
		VI.2.3	Registro delle spese su aperture di credito e rendiconto trimestrale	ILLIMITATI
		VI.2.4	Liquidazioni consulenze	Scartabili dopo 50 anni

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VI.2	**Uscite e piani di spesa**	VI.2.5	Copie di delibere e/o di determine di liquidazione	Scartabili dopo 10 anni
VI.3	**Bilancio, tesoreria, cassa, istituti di credito e verifiche contabili**	VI.3.1	Bilanci o programmi annuali e conti consuntivi (in originale o nell'unica copia esistente)	ILLIMITATI
		VI.3.2	Giornale di cassa	ILLIMITATI
		VI.3.3	Convenzione di cassa con Istituto Cassiere	ILLIMITATI
		VI.3.4	Rapporti con Istituto Cassiere (corrispondenza)	Scartabili dopo 10 anni
		VI.3.5	Distinte di trasmissione al Tesoriere di reversali e mandati	Scartabili dopo 10 anni
		VI.3.6	Estratti conto bancari e postali	Scartabili dopo 10 anni
		VI.3.7	Registro delle operazioni di conto corrente postale	Scartabile dopo 10 anni
		VI.3.8	Bollettini di conto corrente postale, ricevute di versamento	Scartabili dopo 10 anni
		VI.3.9	Documentazione riguardante l'insediamento dei Revisori dei conti	ILLIMITATI
VI.4	**Imposte, tasse, ritenute previdenziali e assistenziali, denunce**	VI.4.1	Documentazione riguardante la tassa di raccolta rifiuti e Modello Unico Dichiarazione Ambientale (MUD)	Scartabile dopo 10 anni salvo contenziosi in atto
		VI.4.2	Contributi – modello DM/10- INPS tabulati riepilogativi imponibili, regolarizzazioni contributive – personale, rapporti con INPS MODELLI EMENS (Denunce Retributive Mensili)	Scartabili dopo 50 anni
		VI.4.3	Modello 01/M (copia del datore di lavoro)	Archiviato nel fascicolo personale
		VI.4.4	D.M.A Denuncia mensile analitica	Scartabile dopo 50 anni
		VI.4.5	FONDO ESPERO	Scartabile dopo 50 anni
		VI.4.6	Modelli 101 – Modelli CUD – Modelli CU	Archiviati nel Fascicolo personale
		VI.4.7	Modello 770	Scartabile dopo 50 anni
		VI.4.8	Denunce annuali IRAP	Scartabili dopo 50 anni

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VI.4	**Imposte, tasse, ritenute previdenziali e assistenziali, denunce**	VI.4.9	Dichiarazione IVA	Scartabili dopo 10 anni
VI.5	**Assicurazioni**	VI.5.1	Documentazione relativa a polizze assicurative	ILLIMITATI
VI.6	**Utilizzo beni terzi, comodato**	VI.6.1	Immobili in uso (di proprietà di altri enti) - atti relativi a locazione e comodati degli immobili (sia di proprietà sia appartenenti ad altri enti) - progetti tecnici, planimetrie, verbali e perizie di collaudo, autorizzazioni e certificazioni relative alla sicurezza e alla messa a norma dei locali e degli impianti (L. 626/94)	ILLIMITATI
		VI.6.2	Immobili in uso (di proprietà di altri enti) - documentazione pervenuta in copia dagli enti proprietari, non compresa in quella descritta al punto A5/2	Scartabile dopo 10 anni
VI.7	**Inventario e rendiconto patrimoniale**	VI.7.1	Verbali di consegna ed elenchi di consistenza di archivi o altri beni inventariati	ILLIMITATI
		VI.7.2	Ricognizioni patrimoniali di scuole confluite	ILLIMITATI
		VI.7.3	Ricognizioni patrimoniali decennali	ILLIMITATI
		VI.7.4	Rivalutazioni patrimoniali quinquennali	ILLIMITATI
		VI.7.5	Verbali dei passaggi di consegna	ILLIMITATI
VI.8	**Infrastrutture e logistica (plessi, succursali)**	VI.8.1	Immobili di proprietà - progetti tecnici, contratti di costruzione, ristrutturazione e manutenzione - verbali e perizie di collaudo, autorizzazioni e certificazioni relative alla sicurezza e alla messa a norma dei locali e degli impianti (L.626/94) - atti relativi a donazioni, acquisti e vendite di immobili di proprietà	ILLIMITATI
VI.9	**DVR e sicurezza**	VI.9.1	Documento valutazione dei rischi (L.626/94) e relativi allegati (es. piani di evacuazione, controlli periodici, nomine, ecc.)	ILLIMITATI
		VI.9.2	Protocolli di sicurezza	ILLIMITATI
VI.10	**Beni mobili e servizi**	VI.10.1	Contratti per fornitura di materiali e per espletamento di servizi	50 anni, conservando illimitatamente il relativo registro (vedi I.5.5)
		VI.10.2	Contratti di prestazione d'opera di varia natura	50 anni, conservando illimitatamente il relativo registro (vedi I.5.6)

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VI.10	**Beni mobili e servizi**	VI.10.3	Buoni d'acquisto, generi di refezione / di consumo	Scartabili dopo 6 anni
		VI.10.4	Abbonamenti e/o acquisti a giornali, riviste e pubblicazioni: corrispondenza relativa	Scartabile dopo 6 anni, conservando illimitatamente gli elenchi dei periodici in abbonamento e delle pubblicazioni acquistate
		VI.10.5	Acquisto di attrezzature, materiale, interventi di manutenzione: corrispondenza relativa	Scartabile dopo 10 anni
		VI.10.6	Acquisto di materiale di consumo: corrispondenza relativa	Scartabile dopo 6 anni, conservando i relativi Registri di materiale facile consumo (vedi I.5.8)
		VI.10.7	Verbali di collaudo di apparecchiature ed attrezzature	Scartabili dopo la dismissione del bene, salvo contenzioso in corso
		VI.10.8	Certificati di garanzia di apparecchiature ed attrezzature	Scartabili dopo la dismissione del bene, salvo contenzioso in corso
		VI.10.9	Dotazioni strumentali: richieste di intervento	Scartabili dopo 6 anni
		VI.10.10	"Libretto di macchina" degli autoveicoli in dotazione presso l'istituto	Scartabile dopo 6 anni
		VI.10.11	Documentazione riguardante le utenze (elettricità, ecc.)	Scartabile dopo 10 anni salvo contenziosi in atto
		VI.10.12	Impianti ed attrezzature durevoli: disegni tecnici, progetti	ILLIMITATA
		VI.10.13	Buoni di carico	Scartabili dopo la dismissione del bene
		VI.10.14	Buoni di scarico	Scartabili dopo 10 anni dalla dismissione del bene o in sede di rinnovo degli inventari
VI.11	**Sistemi informatici, telematici e fonia**	VI.11.1	Documentazione riguardante le utenze di fonia	Scartabile dopo 10 anni salvo contenziosi in atto
		VI.11.2	Registri delle licenze software	ILLIMITATI

I LIVELLO: Personale

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VII.1	**Organici, lavoratori socialmente utili, graduatorie**	VII.1.1	Contratti assunzione personale	50 anni, conservando illimitatamente il relativo registro (vedi I.5.5)
		VII.1.2	Graduatorie interne del personale in servizio	Scartabili dopo 10 anni
		VII.1.3	Graduatorie d'Istituto per supplenze personale docente e non docente	Scartabili dopo 10 anni dalla decadenza di validità
		VII.1.4	Domande di inserimento in graduatoria d'Istituto, con relativa documentazione, inerenti graduatorie non più in vigore	Scartabili dopo 10 anni dalla decadenza di validità della relativa graduatoria conservando a disposizione degli interessati eventuali titoli di studio allegati in originale
		VII.1.5	Domande di supplenza e relative graduatorie in calce	Scartabili dopo 1 anno
		VII.1.6	Decreti di esclusione dalla graduatoria e decreti di rettifica del punteggio	ILLIMITATI
VII.2	**Carriera**	VII.2.1	Fascicoli individuali del personale docente e non docente in servizio, in quiescenza, di ruolo e non di ruolo (ora T.I. e T.D.): - Decreti di nomina e contratti individuali - Presa di servizio - Decreti di trasferimento - Certificati di nascita e residenza del personale di ruolo - Stato di famiglia e relativa documentazione - Certificati di sana e robusta costituzione - Lettere di invito per l'assegnazione della sede - Ordini di servizio individuali - Decreti (per congedi maternità anticipata, ecc.) - Decreti congedi parentali - Decreti congedi straordinari - Permessi - Decreti aspettative - Titoli di studio, attestati di partecipazione a corsi di formazione, aggiornamento, ecc. - Posizioni previdenziali, stipendiali, tributarie - Riscatto periodi assicurativi - Cessione "quinto" dello stipendio - Modello 01/M - Modello 101 e CUD - Richieste accertamenti sanitari (visite fiscali e collegiali, referti)	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VII.2	**Carriera**	VII.2.2	- Accertamenti individuali infortuni e malattie professionali (documentazione sanitaria e tecnica) - Azioni legali del singolo dipendente - Pensione e trattamento di quiescenza - Certificati di servizio - Domande di trasferimento - Permessi di studio - Domande scatti anticipati - Autorizzazioni varie (lezioni private, esercizio a libere professioni, collaborazioni plurime, ecc.) - Rilascio della tessera ministeriale (ferroviaria) - Certificato del casellario giudiziale - Decreto di conferma in ruolo - Domande di ricostruzione di carriera	ILLIMITATI
		VII.2.3	Copie certificati di servizio	Scartabili dopo 5 anni
VII.3	**Trattamento giuridico-economico**	VII.3.1	Tabelle stipendi (nominative) Tabulati mensili riepilogativi retribuzioni	Scartabili dopo 50 anni
		VII.3.2	Compensi per lavoro straordinario, gruppi sportivi, funzioni strumentali e aggiuntive, incarichi specifici, funzioni miste, ore straordinarie per sostituzione colleghi assenti, ore di insegnamento aggiuntive, ore funzionali di non insegnamento, compensi da fondo istituto, o da fondi esterni, ecc.	Scartabili dopo 50 anni
		VII.3.3	Acconti e conguagli per il personale, riepiloghi	Scartabili dopo 50 anni
VII.4	**Assenze**	VII.4.1	Fogli di presenza e altri documenti per la rilevazione delle presenze	Scartabili dopo 10 anni, salvo contenzioso
		VII.4.2	Domande di ferie (congedo ordinario), permessi brevi	Scartabili dopo 6 anni
VII.5	**Formazione, aggiornamento e sviluppo professionale**	VII.5.1	Aggiornamento personale - programmi - relazioni finali - dispense - firme presenza - attestati	ILLIMITATI
VII.6	**Obiettivi, incarichi, valutazione e disciplina**	VII.6.1	Ruoli del personale: documenti istruttori e deliberativi, albi, elenchi, registri, ecc.	ILLIMITATI
		VII.6.2	Sanzioni disciplinari a docenti e personale ATA	ILLIMITATI
VII.7	**Sorveglianza sanitaria**	VII.7.1	Accertamenti sanitari e tecnici: documentazione relativa a malattie professionali, ecc.	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VII.8	**Collaboratori esterni**	VII.8.1	Relazioni su collaborazioni con (o consulenze da parte di) esperti esterni	ILLIMITATI
		VII.8.2	Documentazione relativa agli esperti (CV, dichiarazioni altri incarichi, insussistenza conflitti di interesse, contratto d'incarico, ecc.)	ILLIMITATI

INDICE

- contributi	IV.7.1
- registri di entrata	I.5.11
- regolamenti, norme e cataloghi	I.1.2 - I.1.8 - IV.7.2
Bilanci annuali	IV.3.1
Bollettario di richiesta stampati	I.4.11
Bollettini di c/c postale	VI.3.8
Borse di studio	IV.6.2
Buoni acquisto, generi di refezione / consumo	VI.10.3
Buoni d'ordine	VI.2.2
Buoni di carico	VI.10.13
Buoni di scarico	VI.10.14
Buoni libro, elenco buoni concessi e documentazione di supporto	V.6.1
Campagne di disinfestazione e vaccinazione	V.7.2
Carta dei servizi	I.1.2
Cassa scolastica, registri dei verbali	I.5.7
Cassa, libro/giornale	VI.3.2
Cassiere, Istituto	VI.3.3 - VI.3.4
Cataloghi biblioteca d'Istituto	I.1.8
Cedole librarie	V.6.1
Cerimonie, documentazione relativa	I.8.1
Certificati:	
- garanzie di apparecchiature ed attrezzature	VI.10.8
- nascita alunni	V.3.1
- nascita, residenza, sana e robusta costituzione, servizio del personale	VII.2.1
- richieste	I.4.10
- servizio, registri e copie	VII.2.3
- studio, registri	I.5.23
- vaccinazione alunni	V.7.1
Certificati di nascita e residenza del personale di ruolo	VII.2.1
Certificazioni:	
- delle competenze	V.4.5
- qualità e accreditamenti	I.6.1
- sicurezza locali e impianti (L.626/94) per immobili di proprietà ed immobili in uso	VI.6.1 - VI.8.1
Cessione del quinto dello stipendio	VII.2.1
Circolari interne esplicative e direttive	I.1.5
Collaudo, apparecchiature ed attrezzature, verbali	VI.10.7
Collegio dei Revisori, atti costitutivi	VI.3.9
Colonie, pratiche per assistenza	IV.6.1
Comitati: nomine, verbali, documenti istruttori e deliberativi	I.7.3
Commissioni:	
- elettorali, verbali	I.7.1
- gruppi di lavoro	I.5.3
- nomine, verbali, documenti istruttori e deliberativi	I.7.3
Comodati immobili	VI.6.1
Compensi a vario titolo	VII.3.2
Compiti in classe	IV.10.1
Comunicazioni Comitato studentesco	II.8.1
Conciliazioni, documentazione prodotta e acquisita	III.1.1
Congedi: maternità anticipata, parentali, straordinari, aspettative	VII.2.1
Conguagli per il personale	VII.3.3
Consiglio di Amministrazione e di Presidenza, verbali e registri dei verbali	II.1.2 - I.5.2
Consulenza di istituzioni ed enti vari	III.4.1
Consultazione archivio della scuola, richieste	I.4.12
Conti consuntivi	VI.3.1
Conto corrente postale, registro delle operazioni	VI.3.7
Contrattazione d'Istituto, documentazione preparatoria e registri verbali riunioni	I.5.1 - II.10.1
Contratti:	
- Collettivo Nazionale di Lavoro, norme e disposizioni	I.1.4
- costruzione, immobili di proprietà	VI.8.1
- forniture di materiali, espletamento di servizi	VI.10.1
- individuali	VII.2.1

- prestazione d'opera di varia natura	VI.10.2
- registro	I.5.5
- registro cronologico	I.5.6
Contributi:	
- INPS	VI.4.2
- biblioteca scolastica	IV.7.1
Convenzioni:	
con Istituto Cassiere	VI.3.3 - VI.3.4
- con scuole, enti ecc.	II.9.1
- per attività formative e parascolastiche	V.9.2
- per educazione alla salute	IV.8.1
Convocazioni riunioni:	
- Consiglio di Classe e di interclasse	II.2.2
- Consiglio di Istituto e di Circolo	II.1.3
- Comitato di valutazione	II.7.2
- Comitato studentesco e dei genitori	II.8.3
- Commissioni e gruppi di lavoro	II.11.2
Cooperative di alunni: atti costitutivi, documenti istruttori e deliberativi, corrispondenza	V.9.1
Cooperative ed Associazioni, relazioni su collaborazioni e consulenze	III.4.1
Copie determine e delibere di liquidazione	VI.2.5
Corrispondenza relativa agli acquisti	VI.1.2
Denuncia mensile analitica	VI.4.4
Debito formativo, registri e verbali	I.5.24
Decreti di esclusione dalla graduatoria e decreti di rettifica del punteggio	VII.1.6
Decreti di nomina, di trasferimento e contratti individuali	VII.2.1
Decreti per aspettative, congedi di maternità anticipata, parentali, straordinari	VII.2.1
Deliberazioni, registri	I.5.4
Determinazioni dirigenziali	II.5.1
Dichiarazione IVA	VI.4.9
Dipartimenti, gruppi di lavoro	I.5.3
Diplomi, registri di carico e scarico e di consegna	I.5.29 - I.5.30
Diritto allo studio, documentazione	V.6.7
Disegni, immobili di proprietà	VI.8.1
Disinfestazione, campagne	V.7.2
Dispense:	
- aggiornamento personale	VII.5.1
- documenti prodotti da docenti e studenti in preparazione e nel corso di attività didattiche	IV.5.4
Distinte di trasmissione al tesoriere di reversali e mandati	VI.3.5
Docenti, piano delle attività	II.5.2
Documento programmatico di sicurezza dati - privacy	I.3.1
Documenti relativi alla privacy	I.4.1
Documento valutazione rischi (L. 626/94) e relativi allegati	VI.9.1
Domande:	
- di ferie	VII.4.2
- di supplenze	VII.1.3 - VII.1.4 -VII.1.5
- dei candidati per l'ammissione agli esami e per l'iscrizione alla scuola	V.2.2
Donazioni, immobili di proprietà	VI.8.1
Dotazioni strumentali: richieste di intervento	VI.10.9
Economato, norme e disposizioni	I.1.3
Educazione alla salute	IV.8.1
Elaborati:	
- prove Invalsi	IV.10.4
- prove pratiche per gli esami di Stato	IV.10.3
- prove scritte e grafiche per gli esami di Stato	IV.10.2
- prove scritte, grafiche e pratiche degli alunni (escluse quelle prodotte per gli esami di Stato)	IV.10.1
Elenchi di:	
- alunni per l'iscrizione	V.2.1
- consistenza di archivi o altri beni inventariati	VI.7.1
- personale	VII.6.1
Elezioni degli Organi Collegiali, atti	I.7.2
EMENS modelli denunce retributive mensili	VI.4.2

Enti locali, relazioni su collaborazioni e consulenze	III.4.1
Entrate, partitario	VI.1.1
Esami:	
- di Stato, elaborati prove scritte, grafiche e pratiche	IV.10.2 - IV.10.3
- domande d'ammissione	V.2.2
- registro dei verbali	I.5.28
Esoneri	V.8.1
Esperti esterni, documentazione relativa	VII.8.2
Esperti esterni, relazioni su collaborazioni e consulenze	VII.8.1
Estratti conto bancari e postali	VI.3.6
Fascicoli:	
- individuali del personale docente e non docente in servizio, in quiescenza, di ruolo e non di ruolo (ora T.D. e T.I.)	VII.2.1
- personali degli alunni	V.4.2
Fatture	VI.1.2
Ferie, domande	VII.4.2
Firme presenza, aggiornamento del personale	VII.5.1
Fogli di presenza e altri documenti per la rilevazione delle presenze	VII.4.1
Fondo Espero	VI.4.5
Formazione delle classi, documentazione	V.3.2
Fornitura materiali ed espletamento di servizi, contratti	VI.10.1
Fornitura materiali, registro contratti	I.5.5
Garanzia di apparecchiature ed attrezzature	VI.10.8
Giornali:	
- acquisto o abbonamento	VI.10.4
- di cassa	VI.3.2
Giornalini di classe o d'Istituto	I.8.2
Gite scolastiche	IV.6.3
Graduatorie:	
- d'Istituto	VII.1.3
- in calce	VII.1.5
- interne	VII.1.2
- non più in vigore	VII.1.4
Gruppi di lavoro:	
- derivati dagli Organi Collegiali	I.5.3
- nomine, verbali, documenti istruttori e deliberativi	I.7.3
Gruppo sportivo, registri attività	IV.9.3
Immatricolazione alunni, registri	I.5.21
Immobili:	
- di proprietà	VI.8.1
- in uso, compresa la documentazione pervenuta in copia	VI.6.1 - VI.6.2
Impianti:	
- durevoli, disegni tecnici e progetti	VI.10.12
- sportivi, autorizzazioni all'uso	IV.9.1
Inaugurazioni, documentazione relativa	I.8.1
Inchieste e indagini ambientali e socio-economiche	I.3.2
Infortuni, documentazione e registri	I.5.18 - VII.2.2 - VII.7.1
INPS, contributi	VI.4.2
Inserimento alunni stranieri, progetti formativi	IV.2.1
Interventi:	
- educazione alla salute	IV.8.1
- manutenzione, corrispondenza relativa	VI.10.5
- recupero, progetti formativi	IV.2.1
Intitolazione della scuola	I.1.1
INVALSI:	
- progetto, prospetti riassuntivi	I.6.5
- prove somministrate agli alunni	IV.10.4
Inventari patrimoniali dei beni mobili e d'archivio	I.5.11
IRAP - Denunce annuali	VI.4.8
Iscrizioni a scuola, domande e documenti prodotti	V.2.2
Ispettori scolastici, verbali	I.6.2

Istituti:	
- cassiere	VI.3.3 - VI.3.4
- paritari, Statuti e regolamenti	I.1.1
- regolamenti interni e norme	I.1.2
Istituzione della scuola	I.1.1
Istituzioni socio-assistenziali, relazione su collaborazione e consulenze	III.4.1
IVA, dichiarazione	VI.4.9
Laboratori, regolamenti interni e norme	I.1.2
Legge 626/94:	
- documento valutazione rischi e relativi allegati	VI.9.1
- sicurezza locali e impianti degli immobili di proprietà ed in uso	VI.6.1 - VI.8.1
Lezioni private, registro	I.5.15
Libretti scolastici	V.4.4
Libretto degli autoveicoli in dotazione	VI.10.10
Libri di testo, verbali e relazioni per l'adozione	IV.4.1
Libri, acquisto	VI.10.4
Licenze software	I.5.13
Liquidazioni:	
- consulenze	VI.2.4
- copie delibere e determine	VI.2.5
Locali scolastici, autorizzazioni all'uso	IV.9.1
Locandine pubblicate o stampate dalla o per conto della scuola	I.8.4
Locazione immobili, atti relativi	VI.6.1
Malattie professionali	VII.2.2 - VII.7.1
Mandati di pagamento e relativa documentazione giustificativa	VI.2.2
Manifestazioni teatrali	IV.2.3
Manifesti pubblicati o stampati dalla o per conto della scuola	I.8.4
Manutenzione:	
- interventi	VI.10.5
- immobili di proprietà	VI.8.1
Matrici di buoni acquisto, generi di refezione / consumo	VI.10.3
Mensa, elenco presenze e richiesta di iscrizione al servizio	V.6.2
Modelli:	
- 26 C.G.	VI.2.3
- EMENS, denunce retributive mensili	VI.4.2
- 101, CUD, CU	VI.4.6
-770	VI.4.7
- 01/M, copia del datore di lavoro	VI.4.3
Monitoraggio	I.6.4
Musica, progetti formativi	IV.2.1
Norme interne relative a biblioteca, laboratori, Istituto	I.1.2
OCSEA-PISA, progetto	I.6.5
Orari delle lezioni	IV.3.2
Ordinanze interne esplicative e direttive	I.1.5
Ordinativi di acquisto	VI.1.2
Ordini di servizio generali	II.6.1
Organi Collegiali, di Circolo e d'Istituto:	
- atti delle elezioni	I.7.2
- atti di nomina	I.7.1
- convocazioni riunioni	II.1.3
- registri dei verbali	I.5.3
Organico di autonomia, documentazione	I.2.1
Organizzazioni sindacali, rapporti con	II.10.2
Orientamento, progetti formativi	V.1.1
Pagelle scolastiche	V.4.3
Pareri legali	III.4.2
Partitario delle entrate e delle uscite	VI.1.1
Passaggi di consegna, verbali	VI.7.5
Patentino, progetti formativi	IV.2.1
Patronato Scolastico	V.6.6
PCTO, documentazione relativa	IV.6.4

PEI (piano educativo individualizzato)	IV.5.2
Pensione e trattamento di quiescenza	I.1.7 - VII.2.2
Percorsi didattici, documenti prodotti da docenti e studenti	IV.5.5
Perizie su immobili di proprietà ed immobili in uso	VI.6.1 - VI.8.1
Permessi del personale: brevi e di studio	VII.2.2 - VII.4.2
Personale:	
- aggiornamento	VII.5.1
- norme e disposizioni	I.1.4
Personale ATA, piano delle attività	II.6.2
Piani di lavoro	IV.5.1
Pianta organica	I.2.1
Planimetrie di immobili di proprietà ed immobili in uso	VI.6.1 - VI.8.1
POF (piano offerta formativa)	IV.1.1
Polizze assicurative, documentazione	VI.5.1
PON e POR (Progetti Operativi Nazionali e Regionali)	IV.2.2
Portfolio	V.4.4
Posizioni previdenziali, stipendiali, tributarie	VII.2.2
Posta in partenza e in arrivo, registro	I.4.7
Presa di servizio	VII.2.1
Presenze, fogli	VII.4.1
Prestazioni d'opera, contratti	VI.10.2
Privacy - documento programmatico di sicurezza dati	I.3.1
Privacy – documenti relativi	I.4.1
Profili degli alunni, registri	IV.3.3
Progetti:	
- curricolari	IV.5.5
- educazione alla salute	IV.8.1
- formativi	IV.2.1
- operativi	IV.2.2
- tecnici per immobili di proprietà ed in uso	VI.6.1 - VI.8.1
Programmazione e attuazione attività scolastiche anche esterne, documentazione	IV.2.3 - IV.6.3
Programmi:	
- aggiornamento del personale	VII.5.1
- contabili annuali	VI.3.1
- d'esame	IV.5.3
- dei singoli docenti	IV.5.4
Prospetti:	
- scrutini finali	IV.10.6
- scrutini trimestrali o quadrimestrali	IV.10.5
Protocolli della corrispondenza generali e riservati	I.4.4
Protocolli di sicurezza	VI.9.2
Prove esami, registri verbali	I.5.28
Pubblicazioni varie della scuola	I.8.3
Questionari	I.6.4
Quiescenza, trattamento	I.1.7
R.S.U.	II.10.2
Rapporti con organizzazioni sindacali e rappresentanze interne	II.10.2
Rappresentanze sindacali interne	II.10.2
Rassegna stampa della scuola	I.8.3
Recupero orario, documentazione relativa	IV.3.1
Recupero retribuzione dipendenti assenti dal lavoro per responsabilità di terzi	III.3.1
Registri:	
- assenze degli alunni	IV.3.6
- assenze del personale	I.5.20
- attività del Gruppo Sportivo	IV.9.3
- autorizzazioni ad impartire lezioni private	I.5.15
- carico e scarico dei diplomi	I.5.29
- certificati di servizio rilasciati	I.5.19
- certificati di studio	I.5.23
- classe	IV.3.4
- consegna dei diplomi	I.5.30

- conto corrente postale, ricevute di versamento	VI.3.7
- contratti per fornitura di materiali, espletamento di servizi, assunzione di personale	I.5.5
- cronologici dei contratti	I.5.6
- debito formativo	I.5.24
- deliberazioni	I.5.4
- entrata dei sussidi multimediali	I.5.11
- entrata della biblioteca	I.5.11
- generali dei voti	I.5.22
- generali delle valutazioni	I.5.22
- immatricolazione alunni	I.5.21
- infortuni	I.5.18
- inventariali dei beni mobili	I.5.11
- iscrizione alunni	I.5.21
- licenze software	VI.11.2
- magazzino	I.5.12
- materiali di facile consumo	I.5.8
- personali dei docenti	IV.3.5
- posta in partenza	I.4.7
- profili alunni redatti dai Consigli di classe	IV.3.3
- protocollo, generali e riservati	I.4.4
- riunioni per dipartimento	I.5.26
- riunioni per materia	I.5.25
- spese per apertura di credito e rendiconto trimestrale	VI.2.3
- stato del personale	I.5.16
- stipendi ed altri assegni	I.5.17
- tasse scolastiche per iscrizione e diploma	I.5.9
- tessere di riconoscimento (mod. AT)	I.5.14
- verbali degli esami	I.5.28
- verbali degli Organi Collegiali	I.5.3
- verbali degli scrutini	I.5.27
- verbali del Collegio dei Revisori	VI.3.9
- verbali del Consiglio o Staff di Presidenza	I.5.2
- verbali della cassa scolastica	I.5.7
- verbali riunioni per contrattazione d'Istituto	I.5.1
Regolamenti:	
- biblioteche d'Istituto	I.1.8
- e Statuti, Istituti paritari	I.1.1
- interni relativi a biblioteca, laboratori, Istituto	I.1.2
Regolarizzazioni contributive personali	VI.4.2
Relazioni:	
- attività della scuola	I.6.5
- collaborazioni con istituzioni ed enti	III.4.1
- collaborazioni o consulenze con enti esterni	VII.8.1
- esterne, atti	I.8.1
- finali di classe e d'Istituto	I.6.3
- finali, aggiornamento personale	VII.5.1
- ripetenze alunni	V.4.1
Rendiconto trimestrale	VI.2.3
Repertori:	
- archivio	I.5.11
- fascicoli d'archivio	I.4.5
Reti di scuole, convenzioni e accordi	II.9.1
Retribuzione dipendenti, recupero	III.3.1
Reversali di pagamento e relativa documentazione giustificativa	VI.1.2
Revisori	I.5.10 - VI.3.9
Richieste:	
- accesso ai documenti	I.4.8
- certificati	I.4.10
- consultazione archivio della scuola	I.4.12
- copie di atti	I.4.9
- intervento - risorse strumentali	VI.10.9

Ricognizioni patrimoniali:	
- decennali	VI.7.3
- di scuole confluite	VI.7.2
Ricorsi amministrativi e giurisdizionali	III.1.1
Rilevazioni dati sull'attività della scuola	I.6.5
Ripetenze alunni, relazioni	V.4.1
Riscatto periodi assicurativi	VII.2.1
Ristrutturazione immobili di proprietà	VI.8.1
Riunioni Organi Collegiali e verbali degli stessi	I.5.3 - II.1.3
Rivalutazioni patrimoniali quinquennali	VI.7.4
Riviste, abbonamento e acquisto	VI.10.4
Rubriche alfabetiche del protocollo	I.4.6
Ruoli del personale	VII.6.1
Salute, progetti educativi	IV.8.1
Sanzioni disciplinari alunni	V.5.1
Sanzioni disciplinari a docenti e personale ATA	VII.6.2
Scarto di atti d'archivio	I.4.3
Scatti anticipati, domande	VII.2.2
Sceneggiature cinematografiche, documenti prodotti da docenti e studenti	IV.5.4
Schedario degli alunni	V.10.1
Schede alunni, individuali e di valutazione	V.4.3 - V.10.1
Scioperi	II.10.2
Scrutini, prospetti e registri verbali	I.5.27 - VI.4.7
Servizi, espletamento: registri contratti	I.5.5
Servizio Sanitario Nazionale, relazione su collaborazioni e consulenze	III.4.1
Sindacato, rappresentanze	II.10.2
Soggiorni climatici	IV.6.1
Sperimentazioni multidisciplinari, documenti prodotti da docenti e studenti	IV.5.4
Spese, registro	VI.2.3
Sport, progetti formativi	IV.9.2
Staff di Presidenza, registri dei verbali	I.5.2
Stage	IV.6.2
Stampati, richiesta	I.4.11
Statistiche	I.3.3
Stato di famiglia e relativa documentazione	VII.2.1
Statuti e regolamenti, Istituti paritari	I.1.1
Stipendi, registro	I.5.17
Supplenze, domande	VII.1.5
Sussidi multimediali, registri di entrata	I.5.11
Sussidi, documenti prodotti da docenti e studenti	IV.5.4
Tabelle stipendi	VII.3.1
Tabulati:	
- mensili riepilogativi retribuzioni	VII.3.1
- riepilogativi imponibili	VI.4.2
Tassa raccolta rifiuti e Modello Unico Dichiarazione Ambientale	VI.4.1
Tasse scolastiche per iscrizione e diploma	I.5.9
Teatro, progetti formativi	IV.2.1
Tesoriere, distinte di trasmissione	VI.3.5
Tessere:	
- ministeriale	VII.2.2
- di riconoscimento (mod. AT), registro	I.5.14
Testi teatrali, documenti prodotti da docenti e studenti	IV.5.4
Titolari di classificazione d'archivio	I.4.2
Titoli di studio	VII.2.1
Transazioni, documentazione prodotta e acquista	III.1.1
Trasferimento, domande	VII.2.1
Trasformazioni di scuole	I.1.1
Trasporto alunni, richiesta:	
- iscrizione al servizio ed attestazioni di pagamento	V.6.3
- trasporto gratuito	V.6.4
Trattamento di quiescenza	I.1.7

Tribunale dei minori, relazioni su collaborazioni e consulenze	III.4.1
Uscite, partitario	VI.2.1
Utenze:	
- elettricità (ecc.)	VI.10.11
- fonia	VI.11.1
Vaccinazione, campagne	V.7.2
Valutazioni:	
- alunni	V.4.3
- attività della scuola	I.6.5
- registri	I.5.22
Vendite, immobili di proprietà	VI.8.1
Verbali:	
- collaudo di apparecchiature e attrezzature	VI.10.7
- collaudo di immobili di proprietà ed immobili in uso	VI.8.1
- Collegio docenti	II.3.1
- Comitato studentesco e dei genitori	II.8.2
- commissioni e gruppi di lavoro	II.11.1
- commissioni elettorali	I.7.1
- Consiglio d'Amministrazione	II.1.2
- Consiglio di Istituto e Consiglio di Circolo	II.1.1
- Consiglio di Classe e Interclasse	II.2.1
- consegna ed elenchi consistenza di archivi od altri beni inventariati	VI.7.1
- debito formativo	I.5.24
- Giunta esecutiva	II.4.1
- ispettori scolastici	I.6.2
- passaggi di consegna	VI.7.5
- riunioni collegiali	II.3.2
- valutazione docenti	II.7.1
Violazioni amministrative e reati, documentazione	III.2.1
Visite:	
- collegiali e fiscali e relativi referti	VII.2.1
- di studio	IV.6.3

INDICAZIONI PER LA PROCEDURA DI SCARTO

Al fine di svolgere le operazioni di scarto, il responsabile per la tenuta degli archivi:

— verifica periodicamente la tipologia e i tempi di conservazione della documentazione, sia cartacea che elettronica, presente nell'archivio di deposito per individuare quella da scartare applicando le disposizioni del presente massimario di scarto;

— procede con la compilazione di una lista della documentazione da scartare[1] e la comunica al Responsabile della Gestione Documentale;

— trasmette alla Soprintendenza Archivistica, con lettera protocollata, la lista in due copie, entrambe da lui firmate, delle tipologie archivistiche che si ritiene non abbiano più utilità amministrativa, chiedendo l'autorizzazione prevista dall'articolo 21, comma 1, del D.Lgs. 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137".

— una volta restituita la copia della lista da parte della Sovrintendenza Archivistica, vistata con approvazione totale o parziale, provvede a distruggere i documenti da scartare. Qualora ci si avvalga di soggetti esterni (come ditte o organizzazioni di volontariato, ex D.P.R. 8 gennaio 2001, n. 37, articolo 8, che operano nella raccolta della carta) occorre che questi diano attestazione scritta dell'effettiva distruzione (tramite triturazione, incenerimento, macerazione al fine di riciclare il materiale) della documentazione loro conferita.

— trasmette alla Soprintendenza Archivistica copia del verbale attestante le modalità dell'avvenuta distruzione.

[1] L'elenco di scarto viene redatto conformemente al modello (Appendice A) e comprende: (1) la descrizione delle tipologie dei documenti (es. elaborati delle prove in classe, richieste di certificati, ecc.); (2) gli anni di riferimento; (3) la quantità del materiale (in numero di faldoni, scatole, pacchi e in peso approssimativo); (4) i motivi della proposta di eliminazione. In testa all'elenco di scarto, occorre indicare il numero di pagine di cui si compone.

APPENDICE A – Elenco degli atti che si propongono per l'eliminazione

N. d'ordine	Classificazione[1]	Descrizione degli atti[2]	Estremi cronologici	N. pezzi[3]	Peso in Kg[4]	Motivazioni dell'eliminazione[5]

Data_____ Firma[6]_____

[1]Si riporta la classificazione che le unità archivistiche possiedono

[2] Descrizione sintetica di ogni voce, sufficiente a rendere riconoscibili i documenti

[3] Oltre alla quantità, specificare anche la qualità dei contenitori (cartelle, faldoni, scatole, pacchi, sacchi…)

[4] Il peso può anche essere indicato complessivamente per tutte le unità che si propongono per lo scarto

[5] Indicare sinteticamente il motivo dello scarto e/o la documentazione alternativa che viene conservata

[6] Indicare con chiarezza la qualifica e la responsabilità di chi firma, apponendo il timbro dell'Ente