Manuale di Gestione Documentale

redatto ai sensi dell'art. 5
del dPCM 3 dicembre 2013

Data ultimo aggiornamento: 22 settembre 2016

Il manuale di gestione documentale dell'IC E.Fermi di Carvico 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 tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

SOMMARIO

PREMESSA

Il Manuale di Gestione documentale (di seguito “Manuale”), di cui all’art. 5 del dPCM. 3 dicembre 2013 recante “Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del Codice dell’amministrazione digitale di cui al decreto legislativo n 82 del 2005”, descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. In tale contesto, il protocollo informatico realizza le condizioni operative per gestire il flusso informativo e documentale anche ai fini dello snellimento delle procedure e di una maggiore trasparenza dell’azione amministrativa.

Nell’Istituto Comprensivo “E. Fermi” di Carvico (di seguito “Istituto”) è attiva una sola area organizzativa omogenea (di seguito, AOO), a cui si riferiscono tutti gli uffici operanti nell’Istituto. L’Istituto nomina con decreto dirigenziale il responsabile del servizio di gestione informatizzata dei flussi documentali e l’amministratore di protocollo della AOO; assicura l’adozione e l’aggiornamento del Manuale; definisce tempi, modalità, misure organizzative e tecniche per la eliminazione dei protocolli settoriali e dei relativi registri, soprattutto se ancora cartacei.

Una volta adottato il manuale, esso va aggiornato periodicamente effettuando il censimento delle attività e delle prassi in essere, la razionalizzazione delle stesse, l’individuazione e la definizione degli aspetti organizzativi e gestionali in termini di fasi, tempi e risorse umane impegnate nell’automazione dei flussi documentali nel rispetto della normativa vigente.

SEZIONE 1 – DEFINIZIONI, RIFERIMENTI NORMATIVI E AMBITO DI APPLICAZIONE

1.1 Glossario

Per quanto non previsto dal glossario che segue, si rimanda a quello allegato ai seguenti atti:

- dPCM 3 dicembre 2013 recante Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (14A02097);
- dPCM 3 dicembre 2013 recante Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. (14A02098) pubblicati entrambi nella GU n. 59 del 12-3-2014 - Suppl. Ord. n. 20;
- dPCM 13 novembre 2014 recante Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (15A00107) pubblicato in GU Serie Generale n.8 del 12-1-2015.

ASP	Application Server Provider
AT	Ambito Territoriale
AA.GG.	Autorità Giudiziarie
D.G. o D.R.	Direzione Generale o Regionale
DPR	Decreto del Presidente della Repubblica
D.Lgs.	Decreto Legislativo
AOO	Area Organizzativa Omogenea
DURC	Documento Unico di Regolarità Contributiva
CAD	Codice dell'Amministrazione Digitale (D. Lgs. n. 82/2005)
S.I.	Sistema Informativo del M.I.U.R.
FF.OO.	Forze dell'Ordine
GdL	Gruppo di Lavoro
TUDA	Testo Unico sul Documento Amministrativo (DPR n. 445/2000)
MIUR	Ministero dell'Istruzione, dell'Università e della Ricerca
PdP	Prodotto di Protocollo informatico
PEC	Posta Elettronica Certificata
PEO	Posta Elettronica Ordinaria
SIDI	Sistema Informativo dell'Istruzione

1.2 Estremi del documento

TITOLO	MANUALE DI GESTIONE DOCUMENTALE
REDATTORE DEL DOCUMENTO	Dott. Andrea Quadri
STATO DELDOCUMENTO	APPROVATO
PROPONENTE	Il Responsabile della conservazione Dott. Andrea Quadri
DATA APPROVAZIONE da parte del Consiglio d'Istituto	26 settembre 2016
DATA ULTIMA REVISIONE	22 settembre 2016

1.3 Introduzione

Il dPCM richiamato in premessa prevede che le pubbliche amministrazioni redigano ed adottino un manuale per la gestione del protocollo, dei flussi documentali e degli archivi, per ciascuna Area Organizzativa Omogenea.

L'Istituto Comprensivo "E.Fermi" di Carvico adotta il presente manuale di Gestione Documentale che - *ex lege* – indica regole e principi della formazione, registrazione, classificazione, fascicolazione e archiviazione di documenti nonché la definizione delle linee strategiche legate al *recordkeeping system* (cioè al sistema archivistico) e al *workflow management* (cioè al sistema di flusso di lavoro e delle procedure ad esso collegate) che saranno progressivamente implementate nell'ambito del processo di dematerializzazione.

Il Manuale è vincolante per tutti gli operatori e le figure dell'Istituto.

In definitiva, il Manuale:

- definisce regole e principi della gestione documentale
- fissa termini e modalità d'uso dell'applicativo di protocollo informatico, della posta elettronica (certificata e non), della firma digitale e degli strumenti di dematerializzazione e digitalizzazione delle procedure, in uso presso il MIUR;
- individua ruoli e responsabilità connesse all'attuazione e monitoraggio delle misure ivi descritte.

Il Manuale richiama, in quanto compatibili, le procedure del Manuale di Gestione MIUR adottato con DDG 240 del 9 ottobre 2015.
Il Manuale è stato adottato con delibera n.178 del 14 settembre 2015 del Consiglio d'Istituto ed è rivisto, in conformità alla medesima delibera, con Decreto dirigenziale.
Esso è pubblicato sul sito internet dell'Istituto alla sezione Amministrazione trasparente.

SEZIONE 2 – ORGANIZZAZIONE DEL SERVIZIO

2.1 Area Organizzativa Omogenea

Ai sensi dell'art. 50 del DPR 445 del 28 dicembre 2000, è individuata una sola area organizzativa omogenea denominata Istituto Comprensivo Statale "Enrico Fermi" composta dall'insieme di tutte le sue unità organizzative come da elenco allegato **(Allegato n. 1)**.

Il codice identificativo IPA dell'area è **istsc_bgic83600g**.

Il sito web istituzionale è **www.iccarvico.gov.it**

Ai sensi dell'art.18 c.2 del DPCM 3 dicembre 2013, la casella di posta elettronica certificata associata al registro di protocollo dell'unica AOO è **bgic83600g@pec.istruzione.it**

Sono individuate le seguenti figure:

1. ai sensi dell'art. 3 c.1 lett. b) del DPCM 3 dicembre 2013, il **Responsabile della gestione documentale** è individuato nel Direttore dei Servizi Generali e Amministrativi. Il vicario è individuato nel sostituto del Direttore dei Servizi Generali e Amministrativi, per i casi di vacanza, assenza o impedimento del primo.
   Il Responsabile della gestione documentale, al fine d agevolare l'assolvimento dei compiti assegnatigli dalla normativa vigente e dal presente Manuale, può individuare per specifiche attività un suo delegato, definendo il contesto organizzativo e l'ambito della delega;
1. il **Referente per l'Indice delle Pubbliche Amministrazioni**, nella figura dell'A.A. incaricato dell'UO Ufficio contratti;
2. il **Referente per la PEC e la PEO** per il coordinamento e la gestione dei sistemi di posta elettronica istituzionale.

Le figura di sistema di cui ai punti 2. e 3. sono nominati con decreto del Dirigente, su proposta del Direttore dei Servizi Generali e Amministrativi. In caso di assenza di nomina le funzioni si intendono svolte dal Direttore dei Servizi Generali e Amministrativi.

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

Nell'ambito dell'area organizzativa omogenea di cui al punto 1.3, è individuata una sola struttura di protocollo e archivio.

Ai sensi dell'articolo 61, comma 1, del D.P.R. 445/2000, si provvederà alla costituzione del Servizio archivistico per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi, nell'ambito dell'UO Ufficio del DSGA.

Il servizio, ai sensi dell'articolo 61, comma 3, del DPR 445/2000 ha competenza sulla gestione dell'intera documentazione archivistica, ovunque trattata, distribuita o conservata dell'Amministrazione, ai fini della sua corretta registrazione, classificazione, conservazione, selezione e ordinamento.

Il **Responsabile del servizio**, ai sensi dell'articolo 4 del DPCM 3 dicembre 2013 svolge le funzioni attribuitegli dai citati DPCM 3 dicembre 2013 e DPR 445/2000.

Ai sensi del DPCM 3 dicembre 2013 è individuato il **Responsabile del procedimento di conservazione della documentazione** generata in formato digitale nella figura del Dirigente dell'Istituto.

2.3 Unicità del protocollo informatico

La numerazione delle registrazioni di protocollo è unica, progressiva, corrisponde all'anno solare ed è formata da un intero, tuttavia a norma dell'articolo 53, comma 5 del DPR 445/2000 sono possibili registrazioni particolari (Allegato n.2). L'Amministrazione non riconosce validità a registrazioni particolari che non siano quelle individuate nell'elenco allegato (Allegato n.2). Ad ogni documento è assegnato un solo numero, composto da sette cifre, che non può essere utilizzato per la registrazione di altri documenti.

2.4 Indirizzi di posta elettronica

L'indirizzo PEC è utilizzato per la gestione del servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Essa è pubblicata sull'indice delle Pubbliche Amministrazioni (iPA).

La casella PEC costituisce l'indirizzo virtuale della sede legale dell'Istituto.

Inoltre l'Istituto è dotato di una casella di posta elettronica ordinaria istituzionale (di seguito, PEO) utili a gestire i messaggi di posta elettronica con annessi documenti ed eventuali allegati, aventi rilevanza amministrativa.

Ogni dipendente dell'Istituto è dotato di una casella di posta elettronica @iccarvico.it

Le disposizioni vincolanti per i dipendenti inerenti i termini e modalità d'uso delle PEC e delle PEO sono pubblicate sulla Intranet dell'Istituto.

Il responsabile della gestione documentale è il custode delle credenziali di accesso alle caselle di posta elettronica istituzionali (certificate e non) dell'Istituto.

SEZIONE 3 – PIANO DI SICUREZZA

La presente sezione riporta i riferimenti delle misure di sicurezza adottate perché l'esercizio del servizio per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, sia coerente alle norme sulla protezione dei dati personali.

Nel periodo di transizione fra la gestione analogica e quella digitale dei documenti e degli atti dell'Istituto sono mantenute espressamente in vigore le misure e le procedure descritte nel Documento Programmatico della Sicurezza valido per l'A.S. 2015/16.

3.1 Tutela dei dati personali

Di seguito sono riportate le azioni adottate per garantire il rispetto della norme di cui al D.Lgs. 30 giugno 2003 n. 196 in materia di protezione dei dati personali. Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo, vengono incaricati dal Responsabile della Gestione documentale.

Gli applicativi di gestione documentale adottato dall'Istituto consentono di registrare le informazioni derivanti da certificati e documenti scambiati con altre pubbliche amministrazioni con diversi livelli di riservatezza: a tal fine è presente un registro di protocollo riservato, il cui accesso è consentito solo a personale specificamente abilitato

In relazione alla protezione dei dati personali trattati al proprio interno, si richiamano le misure e le disposizioni del Regolamento sulla tutela dei dati personali.

3.2 Obiettivi del piano di sicurezza

Il Piano, contenente le misure di sicurezza applicative/infrastrutturali relative anche al protocollo informatico, garantisce che:
i documenti e le informazioni trattati dall'Istituto 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.

Il Piano contenente le misure di sicurezza applicative/infrastrutturali relative anche al protocollo informatico - allegato al presente manuale (allegato n. 6) – va coordinato con il Piano di sicurezza e *disaster recovery* del gestore del sistema di gestione documentale per la parte di relativa competenza.

SEZIONE 4 - MODALITA' DI UTILIZZO DI STRUMENTI INFORMATICI PER LA FORMAZIONE DEI DOCUMENTI INFORMATICI

4.1 Modalità di formazione dei documenti e contenuti minimi

Sono in fase di analisi e di revisione i procedimenti interni all'amministrazione, al fine di una loro automazione e adattamento alla formazione di documenti informatici.

Si prevede l'adozione di modelli standard inseriti nel sistema informatico di gestione documentale, nel rispetto della normativa vigente in materia.

Un documento può essere inserito in più fascicoli.

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

- la denominazione dell'amministrazione;

- codice Area Organizzativa Omogenea (AOO);

- codice Registro di Protocollo;

- numero registrazione di protocollo;

- data di registrazione del protocollo;

- oggetto del documento ;

- eventuali allegati;

- estremi identificativi del referente del procedimento (ai sensi della L. 241/90);

- sottoscrizione elettronica con firma digitale o qualificata dell'organo competente ad emanare l'atto ovvero del responsabile di gestione.

4.2 Formato dei documenti informatici

I formati utilizzati sono selezionati sulla base del criterio di maggior garanzia del principio di interoperabilità e nel rispetto delle caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo e diffusione, secondo le indicazioni del DPCM 3 dicembre 2013 e dell'Agenzia per l'Italia Digitale (www.agid.gov.it).

Ai fini dell'archiviazione e della conservazione si utilizzano preferibilmente i formati PDF e PDF/A.

I messaggi email sono archiviati in formato .eml e gli allegati sono mantenuti nel formato originale in cui sono pervenuti all'istituzione scolastica.

L'elenco dei formati accettati è riportato nell'allegato 5.

4.3 Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma digitale o avanzata conforme alle disposizioni di legge. I titolari di firma digitale (Allegato 3) sono abilitati all'utilizzo del dispositivo di firma solo ed esclusivamente nell'esercizio delle proprie funzioni istituzionali, secondo le disposizioni dell'Amministrazione centrale del MIUR.

4.4 Verifica delle firme digitali

La sequenza delle operazioni previste per la verifica di integrità del documento firmato digitalmente avviene attraverso un applicativo specifico che consente la verifica della validità del certificato e della corrispondenza delle impronte del documento.

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

Le eventuali modifiche alle tipologie di documentazione sottoposta a trattamento specifico e a registrazione particolare sono evidenziate nell'allegato elenco (Allegato n.4).

SEZIONE 5 - RICEZIONE DEI DOCUMENTI

5.1 Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono arrivare all'istituzione scolastica attraverso:

a) il servizio postale;

b) la consegna diretta agli uffici;

c) fax.

L'Istituto si riserva il diritto a non accettare documenti pervenuti via fax se non sono univocamente riferibili ad un mittente individuato e non sono accompagnati dalla trasmissione di una copia del documento di identità.

I documenti, esclusi quelli non soggetti a registrazione di protocollo, devono pervenire al protocollo (postazioni adibite presso l'area amministrativa) per la loro registrazione (vedi Allegato n.4). Quelli arrivati via fax sono soggetti alle stesse regole di registrazione degli altri documenti cartacei se rispondono a parametri di autenticità, leggibilità e integrità previsti dalla normativa vigente; in presenza di un sistema informatico che ne consenta l'acquisizione in formato elettronico (fax management) si applicano le procedure previste per la ricezione dei documenti informatici.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema ha già attribuito ad altri documenti, anche se questi sono strettamente correlati tra loro.

Non è pertanto consentito, in nessun caso, l'utilizzo di un unico numero di protocollo per il documento in arrivo e il documento in partenza.

Non è ammessa la ricezione di corrispondenza di carattere personale. Il Responsabile della gestione documentale è in ogni caso tenuto a verificare il contenuto della corrispondenza pervenuta.

A chi richieda ricevuta di un documento consegnato, compatibilmente con le possibilità del servizio, verrà consegnata l'apposita stampa ottenibile dal sistema informatico o redatto apposito documento analogico.

La corrispondenza in arrivo viene aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata. Laddove, per esigenze interne all'ufficio, non sia possibile registrare la totalità dei documenti pervenuti, il Responsabile della gestione individua la corrispondenza prioritaria da protocollare immediatamente; i restanti documenti verranno registrati entro il giorno lavorativo successivo.

5.2 Ricezione dei documenti informatici

Un documento informatico viene registrato a protocollo se è stato spedito all'indirizzo di posta elettronica certificata (PEC) dell'Istituzione scolastica.

Tale casella istituzionale è integrata con il sistema di gestione documentale ed è accessibile solo agli uffici dell'AOO.

Gli indirizzi della casella di posta elettronica istituzionale e della casella di posta elettronica certificata sono reperibili sul sito web dell'amministrazione (www.iccarvico.gov.it).

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti. Il personale degli uffici dell'AOO controlla quotidianamente i messaggi pervenuti nelle caselle di posta istituzionale certificata e posta istituzionale non certificata e verifica se il documento ricevuto è da protocollare, secondo le regole stabilite dalla normativa vigente (sono documenti esclusi dalla protocollazione le gazzette ufficiali, i bollettini ufficiali e notiziari della PA, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni, i documenti già soggetti a registrazione particolare dell'amministrazione).

La casella di posta associata all'AOO è esclusivamente la casella di posta elettronica certificata.

Conseguentemente a questa operazione si potrà aprire una pratica o attribuirne una già esistente al documento e relativo fascicolo di appartenenza. Il sistema supporterà progressivamente la gestione mediante processi automatici di workflow tra le varie figure coinvolte nel processo.

5.3 Ricevute attestanti la ricezione dei documenti

La ricevuta della consegna di un documento cartaceo può essere costituita dalla fotocopia del primo foglio del documento stesso con un timbro che attesti il giorno della consegna.

A chi ne fa domanda, compatibilmente con le esigenze del servizio, deve essere anche riportato il numero di protocollo assegnato al documento, in questo caso l'operatore deve provvedere immediatamente alla registrazione dell'atto e alla sua acquisizione in formato digitale.

Nel caso di ricezione dei documenti informatici tramite Posta Elettronica Certificata, la notifica al mittente dell'avvenuto ricevimento è assicurata dal sistema informatico.

5.4 Apertura della posta

Il Responsabile della gestione documentale apre tutta la corrispondenza cartacea pervenuta all'ente salvo i casi particolari specificati nella Sezione n. 5, compresa la posta elettronica istituzionale e la PEC. Le buste dei documenti pervenuti non si inoltrano agli uffici destinatari e si conservano per 24 ore; le buste delle assicurate, corrieri, espressi, raccomandate etc. si inoltrano insieme ai documenti.

5.5 Orari di apertura per il ricevimento della documentazione cartacea

Per la protocollazione dei documenti cartacei in ingresso, l'Ufficio protocollo è aperto con i gli orari indicati sul sito web (http://www.iccarvico.gov.it)

SEZIONE 6 - REGISTRAZIONE DEI DOCUMENTI

6.1 Documenti soggetti a registrazione di protocollo

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

6.2 Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo:

- bollettini ufficiali, notiziari della pubblica amministrazione;

- note di ricezione delle circolari e altre disposizioni;

- materiale statistico e certificazioni anagrafiche;

- atti preparatori interni;

- giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti i documenti che per loro natura non rivestono alcuna rilevanza giuridico - amministrativa presente o futura;

- tutte le comunicazioni e tutti i documenti utilizzati nell'ambito dell'Ente aventi rilevanza esclusivamente interna, siano essi predisposti in forma cartacea che in formato elettronico.

6.3 Registrazione di protocollo dei documenti ricevuti e spediti

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

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

b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;

c) mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;

d) oggetto del documento, registrato in forma non modificabile;

e) data e numero di protocollo dei documenti ricevuti, se disponibili;

f) impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;

g) classificazione: categoria, classe, fascicolo (si veda titolario allegato);

h) assegnazione;

Inoltre possono essere aggiunti:

i) data di arrivo;

j) allegati (numero e descrizione);

k) estremi provvedimento differimento termini di registrazione;

l) mezzo di ricezione/spedizione (lettera ordinaria, prioritaria, raccomandata, corriere, fax ecc.);

m) ufficio di competenza;

n) tipo documento;

o) livello di riservatezza;

p) elementi identificativi del procedimento amministrativo, se necessario.

6.4 Registrazione dei documenti interni informali

Per i documenti privi di rilevanza esterna, a titolo d'esempio quelli a carattere temporaneo, preparatorio o informativo, ci si avvale dei sistemi di comunicazione interna, senza che sussista obbligo di protocollazione. E' fatta tuttavia salva la facoltà del Responsabile di Gestione di provvedere alla registrazione a protocollo anche di tali atti, qualora lo ritenga necessario.

6.5 Segnatura di protocollo

La segnatura di protocollo apposta o associata al documento analogico è effettuata contemporaneamente alla registrazione di protocollo per mezzo di timbri.

Le informazioni apposte o associate ai documenti informatici, registrati nel registro di protocollo, sono espresse nel seguente formato:

a) codice identificativo dell'amministrazione;

b) codice identificativo dell'area organizzativa omogenea;

c) codice identificativo del registro;

d) data di protocollo;

e) progressivo di protocollo.

I dati relativi alla segnatura di protocollo di un documento trasmesso da una area organizzativa omogenea sono associati al documento stesso e contenuti, nel messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition), definito e aggiornato periodicamente dall'Agenzia per l'Italia digitale con provvedimento reso disponibile sul proprio sito.

6.6 Annullamento delle registrazioni di protocollo

Le registrazioni di protocollo possono essere annullate con una specifica funzione del sistema di gestione informatica dei documenti e con autorizzazione del Responsabile della gestione documentale, a seguito di motivata richiesta scritta o per iniziativa dello stesso responsabile.

Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema. Il sistema durante la fase di annullamento registra gli estremi del provvedimento autorizzativo redatto dal Responsabile della gestione documentale.

Il documento è conservato, all'interno del fascicolo di competenza, a cura del Responsabile del procedimento. Il Responsabile della gestione documentale mantiene comunque un'attività di controllo sull'operato dei Responsabili di procedimento.

6.7 Differimento dei termini di protocollazione

La registrazione della documentazione pervenuta avviene nell'arco della giornata. Il responsabile della gestione documentale, con apposito provvedimento motivato, può autorizzare la registrazione in tempi successivi, fissando un limite di tempo entro il quale i documenti devono essere protocollati.

Il sistema informatico mantiene traccia del ricevimento dei documenti.

6.8 Registro giornaliero di protocollo

Il registro giornaliero di protocollo viene trasmesso al sistema di archiviazione dell'Istituzione scolastica. Delle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.

6.9 Requisiti minimi di sicurezza dei sistemi di protocollo informatico

Il sistema di protocollo informatico assicura:

a) l'univoca identificazione ed autenticazione degli utenti;

b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;

c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;

d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Il sistema di protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.

Il sistema di protocollo informatico deve consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Le registrazioni di cui ai commi 1, lettera d) , e 3 devono essere protette da modifiche non autorizzate.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Il sistema di protocollo rispetta le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

6.10 Registro di emergenza

Il Responsabile della gestione documentale autorizza lo svolgimento delle operazioni di protocollo su un registro di emergenza, a norma dell'articolo 63 del D.P.R. 445/2000, su supporto cartaceo da archiviare a cura del Responsabile della gestione documentale unitamente alla propria copia del registro annuale di protocollo e provvede successivamente a impartire le disposizioni per il riversamento dei dati nel protocollo informatico, tramite le procedure previste dal manuale operativo del sistema informatico e dalla guida all'attivazione del registro. All'inizio di ogni anno, il Responsabile della gestione documentale provvede a istituire il registro di emergenza su supporto cartaceo.

SEZIONE 7 - DOCUMENTAZIONE PARTICOLARE

Determinazioni dirigenziali

Determinazioni dirigenziali e decreti sono 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.

I contratti del personale vengono gestiti attraverso la piattaforma SIDI.

Documentazione di gare d'appalto

Le offerte di gare d'appalto sono registrate al protocollo.

SEZIONE 8 - REGOLE DI GESTIONE DELLA POSTA ELETTRONICA

Si rinvia ai regolamenti già adottati dall'Istituto in materia.

SEZIONE 9 - COOPERAZIONE APPLICATIVA

9.1 Contratti e fatture elettroniche

Il Direttore dei Servizi Generali e Amministrativi è responsabile della gestione dei contratti e delle fatture per l'intero ciclo di lavorazione, dall'acquisizione tramite i sistemi messi a disposzione dall'Amministrazione centrale alla loro protocollazione e lavorazione tramite il gestionale del bilancio sino agli adempimenti relativi alla certificazione dei crediti su PCC e agli obblighi di conservazione sostitutiva.

9.2 Sistema di gestione dei contratti

Il Direttore dei Servizi Generali e Amministrativi sovrintende a tutte le fasi del workflow documentale dei contratti sulle piattaforme SIDI e NoiPA, garantendo il corretto adempimento degli obblighi giuridici ad esso connessi.

SEZIONE 10 - ASSEGNAZIONE DEI DOCUMENTI E WORKFLOW DOCUMENTALE INTERNO

10.1 Assegnazione dei documenti

L'assegnazione dei documenti ai responsabili e ai referenti di procedimento è effettuata dal Responsabile della gestione documentale sulla base degli uffici della AOO.

10.2 Modifica delle assegnazioni

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

10.3 Consegna dei documenti analogici

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

10.4 Consegna dei documenti informatici

I documenti informatici e/o le immagini digitali dei documenti cartacei sono resi disponibili agli uffici, o ai responsabili di procedimento, tramite il sistema informatico di gestione documentale. Per i documenti contenenti dati sensibili devono essere previsti opportuni sistemi di cifratura.

SEZIONE 11 - CLASSIFICAZIONE E FASCICOLAZIONE DI DOCUMENTI

11.1 Classificazione dei documenti

E' stato adottato il nuovo titolario approvato dalla Sovrintendenza con Nota acquisita con Prot. 525 del 23 gennaio 2016.

11.2 Formazione e identificazione dei fascicoli

La fascicolazione digitale avviene attraverso l'assegnazione del documento informatico ad apposite unità di aggregazione supportate dal sistema di gestione documentale.

11.3 Processo di formazione dei fascicoli

Ogni fascicolo deve corrispondere ad un unico procedimento amministrativo.

11.4 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 archivistico che provvede a correggere le informazioni del sistema informatico e del repertorio dei fascicoli e inoltra successivamente il fascicolo al responsabile del procedimento di nuovo carico. Delle operazioni di riassegnazione, e degli estremi del provvedimento di autorizzazione, è lasciata traccia nel sistema informatico di gestione dei documenti o sul repertorio/elenco cartaceo dei fascicoli.

11.5 Fascicolo ibrido

Il fascicolo è composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un unico procedimento amministrativo.

Alla chiusura del fascicolo, il Responsabile della gestione documentale valuta se:

1) provvedere alla stampa e alla produzione di copia conforme cartacea dell'originale informatico;

2) provvedere alla scansione e copia conforme informatica dell'originale cartaceo.

Il Responsabile della gestione documentale appone pertanto la propria firma autografa in caso di produzione di copia conformi cartacee oppure la propria firma digitale/avanzata in caso di copie conformi informatiche.

11.6 Tenuta dei fascicoli dell'archivio corrente

I fascicoli dell'archivio corrente sono formati a cura dei responsabili o dei referenti di procedimento e conservati, fino al trasferimento nell'archivio di deposito, presso gli uffici di competenza.

SEZIONE 12 - SPEDIZIONE DEI DOCUMENTI

12.1 Spedizione dei documenti analogici

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

12.2 Spedizione dei documenti informatici

La spedizione dei documenti informatici avviene all'interno del sistema informatico di gestione dei documenti con le specifiche procedure tecniche previste dal software di gestione documentale.

Valgono i seguenti criteri generali:

1) i documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari abilitato alla ricezione della posta per via elettronica, tramite casella di posta elettronica certificata;

2) per la spedizione l'amministrazione si avvale di una casella di posta elettronica certificata;

3) l'Ufficio protocollo/le postazioni decentrate di protocollo provvedono:

- a effettuare l'invio elettronico utilizzando i servizi di autenticazione e marcatura temporale qualora previsti dalla normativa vigente;

- a verificare l'avvenuto recapito dei documenti spediti per via elettronica;

- ad archiviare le ricevute elettroniche collegandole alle registrazioni di protocollo. Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dall'articolo 49 del CAD D.Lgs 82/05 e ss.mm.ii.

La spedizione di documenti informatici al di fuori dei canali istituzionali descritti non impegna l'Amministrazione verso i terzi.

SEZIONE 13 - CONSERVAZIONE DEI DOCUMENTI

La conservazione sostitutiva di documenti cartacei inizia attraverso la memorizzazione su supporti idonei e si esaurisce con l'apposizione della firma digitale e della marca temporale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo.

La firma digitale garantisce l'autenticità e l'integrità di messaggi e documenti scambiati e archiviati con mezzi informatici; la marca temporale è una sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento.

La distruzione dei documenti analogici soggetti a conservazione obbligatoria, potrà avvenire solo dopo il completamento della conservazione digitale in forma sostitutiva.

I compiti principali del responsabile della conservazione sono di:

• definire i requisiti del sistema di conservazione;

• organizzare il contenuto dei supporti di memorizzazione e gestire le procedure di sicurezza e tracciabilità;

• archiviare e rendere disponibili informazioni relative a documenti garantendo l'accesso alle informazioni;

• definire e documentare le procedure da rispettare per l'apposizione del riferimento temporale.

SEZIONE 14 - DISPOSIZIONI FINALI

14.1 Approvazione del manuale

Il manuale viene approvato dal Consiglio d'Istituto, su proposta del Dirigente scolastico.

14.2 Revisione del manuale

Tenuto conto del carattere dinamico del processo di dematerializzazione e della costante evoluzione dei sistemi di gestione documentale, il Dirigente Scolastico può provvedere alle modifiche del manuale ritenute maggiormente idonee a garantire l'adeguamento delle procedure e dei sistemi informativi alla normativa vigente.

Se sono state apportate modifiche al manuale, con cadenza almeno annuale il Dirigente sottopone la versione rivista del manuale di gestione al Consiglio d'Istituto.

14.3 Pubblicazione del manuale

Il presente manuale è pubblicato sul sito web dell'Istituzione scolastica nella sezione Amministrazione trasparente.

ALLEGATO 1 – UNITÀ ORGANIZZATIVE

Sono attive nell'Istituto le seguenti unità organizzative (uffici):

- Segreteria particolare del Dirigente
- Ufficio amministrativo
- Ufficio contratti
- Ufficio del Direttore dei Servizi Generali e Amministrativi
- Ufficio personale
- Ufficio didattica
- Ufficio Documentazione

ALLEGATO 2 – REGISTRAZIONI PARTICOLARI

Sono ammesse registrazioni particolari:

- per le comunicazioni ordinarie alle famiglie da parte dei Coordinatori di classe e dei moduli;
- per le registrazioni in elenchi e albi tenuti dall'Istituto.

ALLEGATO 3 – TITOLARI DI FIRMA DIGITALE

Sono titolari di firma digitale rilasciata dal MIUR:

- il Dirigente Scolastico
- il Direttore dei Servizi Generali e Amministrativi

ALLEGATO 4 – DOCUMENTI PER I QUALI SI STABILISCONO PARTICOLARI MODALITA' DI TRATTAMENTO

I documenti contenenti dati sanitari o giudiziari o comunque dati sensibili non sono scansionati.

Se in formato elettronico, devono essere previsti opportuni sistemi di crittazione per garantirne la riservatezza.

ALLEGATO 5 – ELENCO DEI FORMATI AMMESSI IN RICEZIONE

Si veda il documento allegato.

ALLEGATO 6 – MISURE DI SICUREZZA

Si veda il documento allegato.

ALLEGATO 7 – REGOLE DI COMPOSIZIONE DELLE PASSWORD

Si veda il documento allegato.

Manuale di Gestione Documentale

redatto ai sensi dell'art. 5
del dPCM 3 dicembre 2013

Allegato 5 - Elenco dei formati ammessi in ricezione

Data ultimo aggiornamento: 28 luglio 2016

Salvo i casi in cui, in relazione a specifici flussi documentali, vi siano particolari previsioni normative, provvedimenti del Responsabile della gestione documentale o istruzioni operative per la fruizione di servizi telematici che dispongano diversamente, l'Istituto assicura l'accettazione dei documenti elettronici inviati ai suoi uffici tramite posta elettronica, posta elettronica certificata e altri canali telematici oppure consegnati direttamente su supporti informatici quando sono prodotti in uno dei seguenti formati:

- .pdf (compreso il formato PDF/A);
- .gif, .jpg, .tif;
- OOOXML - Office Open XML (principali estensioni: .docx, .xlsx, .pptx);
- Open Document Format;
- .txt (codifica Unicode UTF 8);
- .zip (a condizione che i file contenuti all'interno del file compresso siano prodotti in uno dei formati previsti nel presente elenco);
- .p7m (documenti firmati digitalmente con sottoscrizione di tipo CADES e a condizione che i file originali oggetto di sottoscrizione digitale siano prodotti in uno dei formati previsti nel presente elenco).

In ogni caso i documenti elettronici inviati o consegnati all'Istituto dovranno essere privi di elementi attivi, tra cui macro e campi variabili.

L'Istituto si riserva comunque la facoltà di non accettare documenti informatici prodotti in formati che consentano la modifica dei contenuti (.doc, .txt et alia).

Manuale di Gestione Documentale

redatto ai sensi dell'art. 5
del dPCM 3 dicembre 2013

Allegato 6 - Misure di sicurezza del servizio per la formazione, gestione, trasmissione, accesso e conservazione dei documenti informatici

Data ultimo aggiornamento: 28 luglio 2016

Manuale di Gestione Documentale

redatto ai sensi dell'art. 5
del dPCM 3 dicembre 2013

Allegato 7 - Regole di composizione delle password

Data ultimo aggiornamento: 28 luglio 2016

Le misure di sicurezza per la gestione dei documenti informatici conservati sull'applicativo di protocollo informatico e sul sistema di gestione documentale riguardano, tra altro, anche l'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.

Il cambio delle password avviene con frequenza al massimo semestrale durante la fase di esercizio. I dati personali o le *user_id* di accesso di cui sopra, 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 utilizzati saranno consultati solo in caso di necessità dal Responsabile della gestione documentale e dal titolare dei dati e, ove previsto, dalle Forze dell'Ordine ed Autorità giudiziarie.

Le credenziali di accesso al sistema sono del tutto personali e il loro uso ricade sotto la responsabilità di ciascun utente cui sono assegnate. Il personale abilitato è tenuto alla diligente custodia delle credenziali che ai sensi dell'art. 1 co. 1 lett. p del CAD sono assimilabili ad una firma elettronica e quindi incedibili.

Per accedere al sistema ogni utente deve disporre di:

• PROFILO: autorizzazioni concesse dal responsabile del servizio;

• USER_ID: identifica l'utente mediante i dati personali;

• PASSWORD: stringa segreta e riservata all'utente che, in combinazione con il ruolo, consente di accedere al sistema. Essa è associata allo *user_id*. Resta inteso che ogni persona fisica può ricoprire più ruoli mantenendo comunque, la stessa password di accesso legata, quest'ultima, al proprio *user_id*.

Il controllo degli accessi è pertanto, assicurato utilizzando le credenziali di accesso e un sistema di autorizzazione basato sulla profilatura degli utenti in via preventiva.

Le regole per la composizione delle password sono le seguenti:

• essere composta da almeno un carattere maiuscolo, uno minuscolo, uno speciale ed uno numerico;

• avere lunghezza minima di 6 caratteri;

• ammettere i caratteri speciali elencati in parentesi: ($*.);

• risultare *case sensitive* (i caratteri maiuscoli sono percepiti DIVERSI dagli analoghi minuscoli. Es.: M diverso da m);

• essere diversa dalle 6 password precedenti.

Non è consentito cedere a terzi le credenziali personali di accesso alla propria postazione di lavoro, alla posta elettronica ed agli applicativi di gestione dei flussi documentali. Eventuali eccezioni vanno segnalate ed opportunamente formalizzate, informando sempre gli interessati.

Indice dei contenuti

GENERALITÀ

Il piano di sicurezza definisce misure che riguardano la/il:

• 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 semestrale 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, se possibile, lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita i server del sistema di gestione documentale;

• 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;

• 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 o le user ID di accesso, 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 utilizzati saranno consultati solo in caso di necessità dal Responsabile della Gestione documentale e dal titolare dei dati e, ove previsto, dalle Forze dell'Ordine ed Autorità giudiziarie.

Nel periodo di transizione fra la gestione analogica e quella digitale dei documenti e degli atti dell'Istituto sono mantenute espressamente in vigore le misure e le procedure descritte nel Documento Programmatico della Sicurezza valido per l'A.S. 2015/16.

1. ASPETTI DI SICUREZZA INERENTI LA FORMAZIONE DEI DOCUMENTI

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 altre amministrazioni.

I documenti informatici prodotti dall'AOO con l'ausilio di applicativi di videoscrittura o 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 riservatezza, il documento va sottoscritto con firma digitale. Nel caso in cui il documento informatico sia prodotto in modo automatico dal Sistema Informativo dell'Istituto, la sottoscrizione dello stesso avviene "a mezzo stampa" ai sensi dell'art. 3 comma 2 della L. n. 39/1993.

Per attribuire una data certa a un documento informatico prodotto all'interno dell'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 novembre 2014 (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.

2. ASPETTI DI SICUREZZA INERENTI LA GESTIONE DEI DOCUMENTI

I sistemi che ospitano i documenti sono configurati 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 sistema di gestione informatica dei documenti:

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

• garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;

• fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;

• 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.

3. 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'Istituto.

Gli obiettivi di pianificazione, gestione e sviluppo del sistema informativo, tenendo conto delle risorse disponibili, la gestione della sicurezza, la fruibilità e l'accessibilità delle procedure del

sistema informativo saranno affidate ad uno specifico nucleo comprendente il Responsabile della Gestione documentale, l'Animatore digitale e il docente formato come "Pronto Soccorso" Tecnico nell'ambito del Piano Nazionale Scuola Digitale.

La conduzione e la gestione tecnico-operativa del sistema di sicurezza sono attribuibili a specifiche professionalità appartenenti ai gestori del sistema di protocollo, di gestione documentale e di conservazione.

4. COMPONENTE FISICA, LOGICA ED INFRASTRUTTURALE DELLA SICUREZZA

Il Responsabile della gestione documentale è incaricato in particolare di vigilare su:

• controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico e le misure di sicurezza fisica;

• verifica dei requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni acquisite attraverso gli strumenti di gestione documentale (protocollo informatico, PEC e PEO);

• tenuta delle registrazioni di sicurezza (informazioni di qualsiasi tipo - ad es. dati o transazioni - presenti o transitate sul sistema di gestione documentale o sul server principale dell'Istituto) 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.

5. LE REGISTRAZIONI 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 [in particolare i firewall];

• dalle registrazioni del sistema di gestione documentale e delle piattaforme cloud dell'Istituto.

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 Responsabile della Gestione documentale e dal titolare dei dati e, ove previsto dalle Forze dell'ordine e dall'Autorità giudiziaria.

6. ASPETTI DI SICUREZZA INERENTI LA TRASMISSIONE DEI DOCUMENTI

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, trattenere per sé 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 a 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.

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, può essere utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

7. ASPETTI DI SICUREZZA INERENTI L'INTEROPERABILITÀ

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 TUDA).

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla normativa di settore vigente.

8. ASPETTI DI SICUREZZA INERENTI LA TRASMISSIONE DEI DOCUMENTI ALL'INTERNO DELLA AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nelle misure di sicurezza relative alle infrastrutture e riportate nel Documento Programmatico della Sicurezza, in attesa della ristrutturazione dell'edificio della Segreteria dell'Istituto attualmente in corso.

9. ACCESSO AI DOCUMENTI INFORMATICI

Il controllo degli accessi è il processo che garantisce agli utenti autorizzati l'impiego del sistema di protocollo informatico secondo le abilitazioni ad essi assegnate. Le credenziali di accesso al sistema sono del tutto personali e il loro uso ricade sotto la responsabilità di ciascun utente cui sono assegnate. Il personale abilitato è tenuto alla diligente custodia delle credenziali che ai sensi dell'art. 1 co. 1 lett. p del CAD sono assimilabili ad una firma elettronica e quindi incedibili.

Per accedere al sistema ogni utente deve disporre di:

• PROFILO: autorizzazioni concesse dal responsabile del servizio;

• USER_ID: identifica l'utente mediante i dati personali;

• PASSWORD: stringa segreta e riservata all'utente che, in combinazione con il ruolo, consente di accedere al sistema. Essa è associata allo user_id. Avvalendosi dei privilegi amministrativi, il Responsabile della Gestione documentale assegna ad ogni utente un profilo secondo le esigenze eventualmente prospettategli formalmente dal Dirigente.

Resta inteso che ogni persona fisica può ricoprire più ruoli mantenendo comunque, la stessa password di accesso legata, quest'ultima, al proprio user_id. Il controllo degli accessi è pertanto, assicurato utilizzando le credenziali di accesso e un sistema di autorizzazione basato sulla profilatura degli utenti in via preventiva. Le regole per la composizione delle password delle utenze sono in **allegato n. 6.** Non è consentito altresì, cedere a terzi le credenziali personali di accesso alla propria postazione di lavoro, alla posta elettronica ed agli applicativi di gestione dei flussi documentali. Eventuali eccezioni vanno segnalate ed opportunamente formalizzate, informando sempre gl'interessati.

Il Protocollo informatico e sistema di gestione documentale adottato dall'amministrazione:

• consente il controllo differenziato dell’accesso alle risorse del sistema per ciascun utente;

• assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l’individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente del Protocollo informatico e sistema di gestione documentale può accedere solamente ai documenti che sono stati assegnati alla sua Unità Operativa, salvo diversa autorizzazione configurata sull’applicativo di protocollo informatico. 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.

10. ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI ALLA AOO

L’accesso ai registri di protocollo è consentito al personale specificatamente indicato in un dedicato allegato del manuale di AOO. 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. La registrazione di protocollo effettuata da chiunque associa un livello di riservatezza per il documento in esame, applicato automaticamente dal sistema. In modo analogo, l’ufficio che effettua l’operazione di apertura di un nuovo fascicolo ne determina anche il livello di riservatezza. Per quanto concerne i documenti sottratti all’accesso, si rinvia allo specifico regolamento per l’accesso degli atti.

11. UTENTI ESTERNI ALLA AOO - ALTRE AOO/AMMINISTRAZIONI O PRIVATI

Non è consentito l’accesso al sistema di gestione del protocollo informatico e documentale da parte di utenti appartenenti ad altre amministrazioni.

Se la consultazione del Protocollo informatico avviene allo sportello o comunque di fronte all’interessato, a tutela della riservatezza delle registrazioni di protocollo, l’addetto posiziona il monitor 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.

Non è consentito l’accesso al Protocollo informatico da parte di utenti esterni alla AOO non espressamente autorizzati.

Non è consentito autorizzare l’accesso al Protocollo informatico al personale di ditte e società esterne diverse da quelle che gestiscono il Sistema di gestione documentale.