Istituto Comprensivo di Vergiate
21029 Vergiate (VA) – Largo Lazzari, 2
Tel. 0331 946 297– Cod. Meccanografico VAIC83400C
Cod. Fisc. 82014720120 CUF: UFIFMP
e-mail : vaic83400c@istruzione.it - vaic83400c@pec.istruzione.it
sito web : www.comprensivovergiate.edu.it

Manuale per la Gestione dei Flussi Documentali, aggiornato alle Linee Guida AGID

Nome documento:	Manuale per la Gestione dei Flussi Documentali, aggiornato alle Linee Guida AGID
Codice documento:	Manuale Flussi Documentali Ver 1-0
Nome file:	Manuale Flussi Documentali Ver 1-0.doc
Stato documento:	Definitivo
Versione:	1.0
Data creazione:	7 giugno 2021
Data ultimo aggiornamento	29 dicembre 2021

PREMESSA

Le "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID, prevedono l'obbligo per le Pubbliche Amministrazioni di redigere con provvedimento formale e pubblicare sul proprio sito istituzionale il ***Manuale di gestione documentale***.

Il presente Manuale di gestione documentale, adottato dall'Istituzione scolastica **Istituto Comprensivo Statale di Vergiate con sede in Largo Lazzari 221029 Vergiate (VA)**, al fine di adeguarsi alle disposizioni di cui sopra, descrive il sistema di gestione 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.

Nel dettaglio, il Manuale descrive il modello organizzativo adottato dalla scuola per la gestione documentale e il processo di gestione del ciclo di vita del documento, oltre a fornire specifiche istruzioni in merito al documento amministrativo ed al documento informatico, al protocollo informatico e alle tematiche di accesso, trasparenza e *privacy*.

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti. Pertanto, il presente documento si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con gli organi dell'Istituto.

GLOSSARIO

ACRONIMI

AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005 e ss.mm.ii.)
D.L.	Decreto-legge
D.Lgs.	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
D.P.R.	Decreto del Presidente della Repubblica
DSGA	Direttore dei Servizi Generali e Amministrativi
GDPR	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
iPA	Indice delle Pubbliche Amministrazioni
PEC	Posta Elettronica Certificata
PEO	Posta Elettronica Ordinaria
RPD	Responsabile della protezione dei dati
RPCT	Responsabile per la prevenzione della corruzione e della trasparenza
RUP	Responsabile unico del procedimento

UOR	Unità Organizzativa Responsabile

1. IL MANUALE DI GESTIONE DOCUMENTALE

Il presente manuale descrive il sistema di produzione e gestione dei documenti, anche ai fini della conservazione.

In coerenza con il quadro normativo di riferimento, il manuale è volto a disciplinare le attività di creazione, acquisizione, registrazione, classificazione, assegnazione, fascicolazione e archiviazione dei documenti informatici, oltre che la gestione dei flussi documentali e archivistici dell'Istituzione scolastica, nonché, seppur in via residuale, la gestione dei documenti non informatici. Tali attività sono finalizzate alla corretta identificazione e reperibilità dei documenti acquisiti e creati dalla scuola nell'ambito dell'esercizio delle proprie funzioni amministrative.

Il manuale, dunque, costituisce una guida dal punto di vista operativo per tutti coloro che gestiscono documenti all'interno dell'Istituzione scolastica, in modo tale da facilitare un corretto svolgimento delle operazioni di gestione documentale.

1.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO

Il Responsabile della gestione documentale[1] si occupa della predisposizione del manuale, che è adottato con provvedimento dal Dirigente Scolastico.

Il manuale deve essere aggiornato periodicamente effettuando il censimento delle attività/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.

Ogni evento suscettibile di incidere sull'operatività ed efficacia del manuale medesimo deve essere tempestivamente segnalato al Responsabile della gestione documentale, al fine di prendere gli opportuni provvedimenti in ordine all'eventuale modifica e/o integrazione della procedura stessa.

1.2 FORME DI PUBBLICITÀ E DIVULGAZIONE

In coerenza con quanto previsto nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*"[2] (a seguire, anche "Linee Guida"), adottate dall'AgID con Determinazione n. 407/2020 ed in seguito aggiornate con Determinazione n. 371/2021 (da attuare entro il 1° gennaio 2022), ovvero che il manuale sia reso pubblico mediante la pubblicazione sul sito istituzionale in una parte chiaramente identificabile dell'area "Amministrazione trasparente", prevista dall'art. 9 del D.Lgs. 33/2013[3], il presente manuale è reso disponibile alla consultazione del pubblico mediante la diffusione sul sito istituzionale dell'Istituzione scolastica.

[1] Per ulteriori dettagli in merito a tale figura, si veda il par. "2.2. - Ruoli e responsabilità".

[2] Si ricorda che le Linee Guida AgID hanno carattere vincolante, come precisato dal Consiglio di Stato - nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al D.Lgs. 82/2005 n. 2122/2017 del 10.10.2017. Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2, del citato D.Lgs. 82/2005, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'art. 17 del medesimo Codice.

[3] L'art. 9, comma 1, del D.lgs. 33/2013, prevede che: "*Ai fini della piena accessibilità delle informazioni pubblicate, nella home page dei siti istituzionali è collocata un'apposita sezione denominata «Amministrazione trasparente», al cui interno sono contenuti i dati, le informazioni e i documenti pubblicati ai sensi della normativa vigente. Al fine di evitare eventuali*

2. IL MODELLO ORGANIZZATIVO

2.1. AREA ORGANIZZATIVA OMOGENEA

L'art. 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 "*Testo unico delle disposizioni legislative e regolamentari in materia di regolamentazione amministrativa*" stabilisce che "*Ciascuna Amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse*".

L'Istituzione scolastica individua al proprio interno un'unica Area Organizzativa Omogenea (AOO), alla quale corrisponde un Registro unico di protocollo, denominato Protocollo Informatico.

L'AOO può essere sotto-articolata in Unità Organizzative Responsabili (UOR), ovvero l'insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.

Alla data di ultimo aggiornamento del presente documento, l'AOO non è stata suddivisa in UOR, pertanto non è stato prodotto l'Allegato 1.

Laddove presente, l'Allegato 1 è suscettibile di modifiche. L'inserimento/cancellazione/aggiornamento delle UOR deve essere formalizzato con provvedimento a firma del Responsabile della gestione documentale e recepito nel presente manuale.

2.2. RUOLI E RESPONSABILITÀ

L'Istituzione scolastica, allo scopo di assicurare un trattamento uniforme dei documenti, una puntuale applicazione delle disposizioni ed un periodico monitoraggio delle modalità d'uso degli strumenti di gestione documentale, deve prevedere le seguenti figure:

- il **Responsabile della gestione documentale** ed il suo vicario[4];
- il **Responsabile della conservazione**;
- il **Responsabile per la prevenzione della corruzione e della trasparenza**;
- il **Responsabile della protezione dei dati**, ai sensi dell'art. 37 del Regolamento UE 679/2016.

Inoltre, in aggiunta alle figure sopra elencate, è importante di individuare il **Referente per l'indice delle Pubbliche Amministrazioni** (iPA), soggetto a cui il Dirigente Scolastico affida il compito, sia organizzativo che operativo, di interagire con il gestore dell'iPA per l'inserimento e la modifica dei dati dell'Istituzione scolastica, nonché per ogni altra questione riguardante la presenza della stessa presso l'iPA[5].

duplicazioni, la suddetta pubblicazione può essere sostituita da un collegamento ipertestuale alla sezione del sito in cui sono presenti i relativi dati, informazioni o documenti, assicurando la qualità delle informazioni di cui all'articolo 6. Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione «Amministrazione trasparente»".

[4] Come definito nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID "*Le Pubbliche Amministrazioni, nell'ambito del proprio ordinamento, provvedono a: […] nominare, in ciascuna delle AOO, il responsabile della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche*".

[5] Le *"Linee Guida dell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi* (IPA)", adottate dall'AgID, al paragrafo 2.2, stabiliscono che "*Il Responsabile dell'Ente nell'istanza di accreditamento nomina un Referente IPA che ha il compito di interagire con il Gestore IPA per l'inserimento e la modifica dei dati, nonché per ogni altra questione riguardante la presenza dell'Ente nell'IPA*".

Il **Responsabile della gestione documentale** è il soggetto in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

Tenuto conto di quanto sopra, il Responsabile della gestione documentale è individuato, all'interno dell'Istituzione scolastica, nella persona del soggetto (o dei soggetti) che materialmente effettuano la protocollazione dei documenti in entrata e che producono il pacchetto di versamento ed effettuano il trasferimento del suo contenuto nel sistema di conservazione. Il vicario è individuato nella persona che in caso di assenza o indisponibilità del soggetto che effettua la protocollazione dei documenti in entrata, svolge tale compito.

Il Responsabile della gestione documentale ed il suo vicario sono nominati con apposito provvedimento del Dirigente Scolastico.

Il **Responsabile della conservazione** è il soggetto in possesso di idonee competenze giuridiche, informatiche ed archivistiche, che opera secondo quanto previsto dall'art. 44, comma 1-*quater*, del D.Lgs. 82/2005 (di seguito anche "CAD")[6].

In particolare, il Responsabile della conservazione:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli *standard* internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;

[6] L'art. 44, comma 1-*quater*, del CAD prevede che: "*Il responsabile della conservazione, che opera d'intesa con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis*".

j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali[7];
m) predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al Responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in *outsourcing* dalle Pubbliche Amministrazioni.

Il ruolo del Responsabile della conservazione può essere svolto dal Responsabile della gestione documentale o anche da altre figure. Il ruolo di Responsabile della conservazione è stato affidato, ai sensi ed in ottemperanza a quanto previsto dall'art. 28 del GDPR, ad una Ditta esterna, cui riferimenti precisi sono pubblicati nella sezione "***Amministrazione Trasparente***" dell'Ente, nella sezione "***Bandi di gara e contratti***"

Il Responsabile della conservazione è nominato con apposito decreto del Dirigente Scolastico.

Il **Responsabile per la prevenzione della corruzione e della trasparenza** (RPCT) è il soggetto al quale può essere presentata l'istanza di accesso civico, qualora la stessa abbia ad oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013[8].

Il RPCT, oltre a segnalare i casi di inadempimento o di adempimento parziale degli obblighi in materia di pubblicazione previsti dalla normativa vigente, si occupa delle richieste di riesame dei richiedenti ai quali sia stato negato totalmente o parzialmente l'accesso civico generalizzato, ovvero che non abbiano avuto alcuna risposta entro il termine stabilito (si veda, per maggiori dettagli, quanto specificato nel paragrafo 6.2.2).

Alla data di ultima pubblicazione del presente documento, con decreto del Ministero dell'Istruzione, dell'Università e della Ricerca prot. n. 325 del 26 maggio 2017 – Nomina Responsabili della prevenzione della corruzione e per la trasparenza nelle istituzioni scolastiche statali, il Ministero dell'Istruzione dell'Università e della Ricerca ha nominato i Direttori Generali degli Uffici scolastici regionali Responsabili per la Prevenzione della Corruzione e per la Trasparenza (RPCT) nelle Istituzioni Scolastiche statali di competenza.

[7] L'art. 41, comma 1, del Codice dei beni culturali prevede che: "*Gli organi giudiziari e amministrativi dello Stato versano all'archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre trent'anni, unitamente agli strumenti che ne garantiscono la consultazione. Le liste di leva e di estrazione sono versate settant'anni dopo l'anno di nascita della classe cui si riferiscono. Gli archivi notarili versano gli atti notarili ricevuti dai notai che cessarono l'esercizio professionale anteriormente all'ultimo centennio*".
[8] Art. 5, comma 3, lett. d), D.Lgs. 33/2013.

Il **Responsabile della protezione dei dati** (RPD) è il soggetto nominato con apposito decreto del Dirigente Scolastico, che ha il compito di sorvegliare sull'osservanza della normativa in materia di protezione dei dati personali, ossia il Regolamento UE 679/2016 (di seguito, anche "GDPR") e il D.Lgs. 196/2003 (di seguito, anche "Codice *privacy*"), come modificato dal D.Lgs. 101/2018.

Il Responsabile della protezione dei dati deve essere coinvolto in tutte le questioni che riguardano la gestione e la protezione dei dati personali e ha il compito sia di informare e sensibilizzare il personale della scuola riguardo agli obblighi derivanti dalla citata normativa sia di collaborare con il Titolare e il Responsabile del trattamento, laddove necessario, nello svolgimento della valutazione di impatto sulla protezione dei dati[9].

Sul punto, le "*Linee Guida sui responsabili della protezione dei dati*", adottate dal WP29 il 13 dicembre 2016, emendate in data 5 aprile 2017, precisano che "*Assicurare il tempestivo e immediato coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile del trattamento. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento*".

Per ciò che concerne le modalità attraverso le quali il Responsabile della protezione dei dati si interfaccia con il Responsabile della gestione documentale e con il Responsabile della conservazione in merito all'adozione delle misure di sicurezza del sistema di gestione informatica dei documenti, si rimanda a quanto descritto nel dettaglio al paragrafo 6.1.

2.3. MODELLO ORGANIZZATIVO ADOTTATO

Il sistema di protocollazione adottato dall'Istituzione scolastica è "parzialmente accentrato", per cui tutte le comunicazioni giungono al punto unico di accesso mentre possono essere trasmesse e protocollate in uscita da ciascun operatore abilitato. In dettaglio:

- le **comunicazioni in ingresso**, indipendentemente dalla tipologia di comunicazione (via PEC, PEO o formato cartaceo) giungono presso il punto unico di accesso, dove vengono registrate a protocollo e smistate ai diversi uffici/persone a seconda della competenza;
- le **comunicazioni in uscita** sono trasmesse in uscita dai singoli uffici o persone.

Le UOR e i soggetti abilitati per la ricezione, l'assegnazione, la consultazione, la protocollazione, la classificazione e l'archiviazione dei documenti sono individuati dal Responsabile della gestione documentale mediante atti organizzativi interni.

[9] La figura del Responsabile della protezione dei dati è disciplinata dal Considerando n. 97 e dagli artt. 37 – 39 del Regolamento UE 679/2016, nonché dalle Linee guida sui responsabili della protezione dei dati, già richiamate nel testo (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287*). Tale figura ha il compito di: valutare i rischi di ogni trattamento; collaborare con il Titolare/Responsabile del trattamento, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati; informare e sensibilizzare il Titolare o il Responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati; cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento; supportare il Titolare o il Responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento. Il Responsabile della protezione dei dati è individuato tra i soggetti in possesso di specifici requisiti, competenze professionali e conoscenze specialistiche in materia di protezione dei dati, in linea con le funzioni che è chiamato a svolgere e che deve poter adempiere in piena indipendenza e in assenza di conflitti di interesse.

2.4. CASELLE DI POSTA ELETTRONICA

L'Istituzione scolastica è dotata di una casella di Posta Elettronica Certificata (PEC) istituzionale per la gestione del servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. L'indirizzo PEC deve essere pubblicato sull'indice delle Pubbliche Amministrazioni.

La casella di cui sopra costituisce l'indirizzo virtuale della sede legale dell'AOO.

L'Istituzione scolastica è dotata anche di una casella di Posta Elettronica Ordinaria (PEO) istituzionale, utile a gestire i messaggi di posta elettronica con annessi documenti ed eventuali allegati, aventi rilevanza amministrativa.

Inoltre, l'Istituzione scolastica si avvale di caselle di Posta Elettronica Ordinaria interne ("di servizio") da affidare alla gestione di una UOR o del singolo operatore[10].

Le disposizioni vincolanti inerenti ai termini e modalità d'uso delle PEC e delle PEO sono pubblicati sul sito istituzionale dell'Istituzione scolastica.

3. IL CICLO DI VITA DEL DOCUMENTO

Il ciclo di vita del documento è articolato nei processi di produzione, gestione e conservazione:

- il **processo di produzione** del documento si sostanzia principalmente nell'acquisizione di documenti cartacei, informatici e/o telematici ovvero nella creazione degli stessi;
- il **processo di gestione** interessa tutte le attività a partire dalla registrazione del documento, alla classificazione, assegnazione e fascicolazione/archiviazione corrente;
- il **processo di conservazione** si sostanzia nel trasferimento dei documenti dall'archivio corrente all'archivio di deposito (dal quale possono eventualmente seguire l'attività di scarto e di delocalizzazione) e dall'archivio di deposito all'archivio storico.

Nei paragrafi successivi si riporta una panoramica dei processi suddivisi per:

- processo di produzione e gestione;
- processo di conservazione.

3.1. PROCESSO DI PRODUZIONE E GESTIONE

Il processo di produzione e gestione fornisce una sintesi delle attività da porre in essere con riferimento sia alla produzione del documento, sia alle fasi di gestione dello stesso. Il processo di produzione è suddiviso in "Processo di produzione – Acquisizione" e "Processo di produzione – Creazione", al fine

[10] Ai sensi della Direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie, "*Appare, perciò, necessario che le pubbliche amministrazioni provvedano a dotare tutti i dipendenti di una casella di posta elettronica (anche quelli per i quali non sia prevista la dotazione di un personal computer) e ad attivare, inoltre, apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza.*"

di distinguere rispettivamente le attività relative ai documenti in entrata da quelle relative ai documenti elaborati dall'Istituzione scolastica.

Con riferimento alla gestione del documento, si fornisce un dettaglio delle seguenti fasi: classificazione, fascicolazione, archiviazione.

3.1.1. PROCESSO DI PRODUZIONE E GESTIONE - ACQUISIZIONE

Il "Processo di produzione e gestione – Acquisizione" è descritto differenziando il caso in cui l'*input* sia un documento cartaceo dal caso in cui sia informatico, dato che i documenti provenienti dall'esterno possono essere di natura cartacea o informatica.

Nel caso di **documento cartaceo in ingresso**, nella fase di acquisizione, l'Istituzione scolastica ricevente:

- rilascia una ricevuta timbrata, qualora il documento dovesse essere consegnato a mano[11];
- verifica la competenza del documento stesso.

Nel caso di documenti pervenuti erroneamente all'Istituzione scolastica ma indirizzati ad altri soggetti, il documento:

- si restituisce per posta;

oppure

- se la busta che lo contiene viene aperta per errore, è protocollato in entrata e in uscita, inserendo nel campo oggetto e nel campo di classificazione la nota "Documento pervenuto per errore", ed è rinviato al mittente apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

Se il documento è di competenza dell'Istituzione scolastica ricevente, segue la fase di registrazione in cui l'operatore addetto alla protocollazione:

- valuta se il documento è da protocollare (cfr. par. "4.8. - Protocollabilità di un documento");
- nel caso in cui il documento sia da protocollare, procede alla scansione e alla successiva verifica di conformità all'originale della copia informatica (cfr. par. "5.10. - Modalità di svolgimento del processo di scansione");
- verifica la presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016, ai fini dell'attuazione delle misure di sicurezza previste al paragrafo 6.1;
- provvede alla classificazione del documento sulla base del titolario di classificazione;
- provvede alla protocollazione in ingresso del documento;
- appone il timbro contenente i dati contenuti nella segnatura di protocollo tramite l'apposita funzionalità del servizio di protocollo informatico ovvero, solo in caso di impossibilità, procede manualmente.

Nella fase di assegnazione, l'operatore addetto alla protocollazione provvede all'assegnazione del documento al personale competente secondo le seguenti modalità e regole di assegnazione: assegnazione del documento all'ufficio competente. Il Responsabile della gestione documentale, ovvero il vicario, può, in ogni caso, rettificare l'assegnatario del documento.

[11] Il servizio protocollo non rilascia, di regola, ricevute per i documenti che non sono soggetti a regolare protocollazione. La semplice apposizione del timbro datario sulla copia non ha alcun valore giuridico e non comporta alcuna responsabilità del personale amministrativo della scuola in merito alla ricezione ed all'assegnazione del documento.

Successivamente alle fasi di registrazione, classificazione e assegnazione, è necessario procedere con la fase di fascicolazione/archiviazione del documento.

Caso di conservazione ibrida*:*

Per i documenti cartacei, si provvede alla conservazione ibrida, in cui è prevista la conservazione sia del documento analogico originale sia della copia informatica. Pertanto, il Responsabile della gestione:

- inserisce il documento cartaceo in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente cartaceo;
- inserisce il documento informatico in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente elettronico.

Caso di conservazione sostitutiva*:*

Per i documenti cartacei, si provvede alla conservazione sostitutiva, con la quale è garantita nel tempo la validità legale di un documento informatico, inteso come una rappresentazione di atti o fatti e dati su un supporto, sia esso analogico o informatico. Pertanto, il Responsabile della gestione:

- attesta la conformità del documento informatico al documento cartaceo, ai sensi dell'art. 22, comma 2, del CAD;
- può distruggere il documento cartaceo;
- inserisce il documento informatico in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente elettronico.

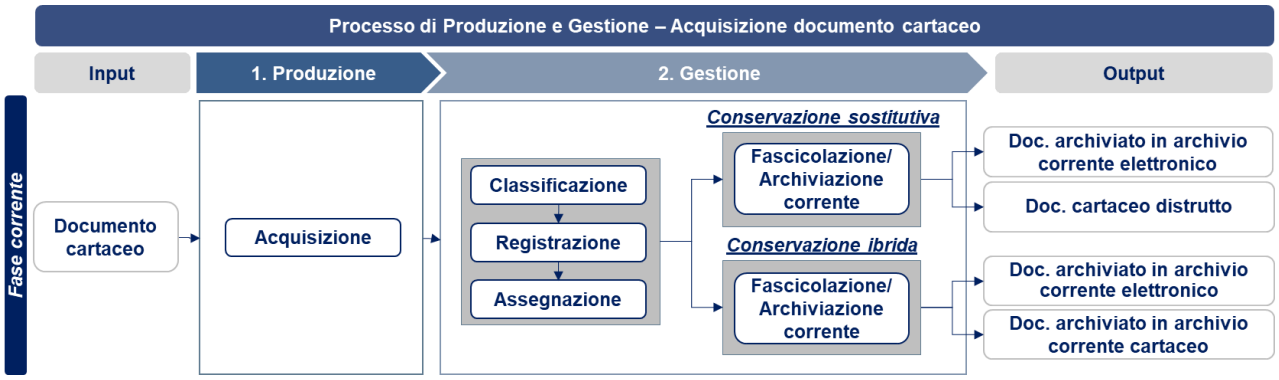
Si precisa che non possono essere distrutti i documenti elencati dal DPCM 21 marzo 2013[12], per i quali rimane l'obbligo della conservazione del cartaceo anche nel caso di conservazione sostitutiva.

In entrambi i casi (conservazione ibrida e conservazione sostitutiva)*:*

Per tali attività, il Responsabile della gestione può disporre apposita delega all'assegnatario o ad altro personale appositamente individuato.

Di seguito si fornisce la rappresentazione grafica del processo sopra descritto.

[12] L'Allegato al DPCM 21 marzo 2013 avente ad oggetto "*Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*", riporta tra i documenti analogici originali unici per i quali permane l'obbligo della conservazione dell'originale cartaceo, i seguenti:
a) atti contenuti nella Raccolta ufficiale degli atti normativi della Repubblica;
b) atti giudiziari, processuali e di polizia giudiziaria per i venti anni successivi;
c) opere d'arte;
d) documenti di valore storico – artistico, ivi compresi quelli in possesso delle forze armate;
e) documenti, ivi compresi quelli storico – demaniali, conservati negli archivi, nelle biblioteche e nelle discoteche di Stato, ivi compresi gli atti e documenti conservati nella biblioteca storica dell'ex Centro Studi Esperienze della Direzione Centrale per la prevenzione e la Sicurezza Tecnica del Dipartimento dei V.V.F., de soccorso pubblico e della difesa civile;
f) atti notarili;
g) atti conservati dai notai ai sensi della legge 16 febbraio 1913, n. 89, prima della loro consegna agli Archivi notarili;
h) atti conservati presso gli Archivi notarili.



Nel caso di **documento informatico in ingresso**, nella fase di acquisizione, l'Istituzione scolastica ricevente verifica la competenza del documento.

Nel caso di documenti pervenuti erroneamente sulla casella PEC o PEO dell'Istituzione scolastica, l'operatore di protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore – non di competenza di questa Amministrazione". Inoltre, se il documento è stato erroneamente protocollato, l'addetto al protocollo provvede ad annullare la registrazione, secondo le modalità descritte nel presente manuale, oppure a protocollare il documento in uscita indicando come oggetto "Protocollato per errore".

Se il documento è di competenza dell'Istituzione scolastica ricevente, segue la fase di registrazione in cui l'operatore addetto al protocollo:

- valuta se il documento è da protocollare (cfr. par. "4.8. - Protocollabilità di un documento");
- nel caso in cui il documento sia da protocollare procede alla verifica di validità della firma (se presente)[13];
- verifica la presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016, ai fini dell'attuazione delle misure di sicurezza di cui al paragrafo 6.1;
- provvede alla classificazione del documento sulla base del titolario di classificazione[14];
- provvede alla protocollazione in ingresso.

Nella fase di assegnazione l'operatore addetto al protocollo provvede ad assegnare il documento al personale competente. Il Responsabile della gestione documentale può, in ogni caso, rettificare l'assegnatario del documento.

Qualora l'ordinamento giuridico preveda, per particolari categorie di documenti elettronici, degli obblighi relativamente all'uso di formati di file specifici ovvero di vincoli aggiuntivi su formati generici, le Istituzioni scolastiche, assolvendo tali obblighi, accettano i suddetti documenti elettronici solo se prodotti nei formati o con i vincoli aggiuntivi obbligatori.

Con la conservazione digitale si esegue la fase di fascicolazione/archiviazione corrente in cui gli utenti opportunamente abilitati provvedono all'inserimento del documento informatico o in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente elettronico.

Di seguito si fornisce la rappresentazione grafica del processo sopra descritto.

[13] Per ulteriori approfondimenti, si veda il cap. "4. - Il documento amministrativo".
[14] Nel caso di dubbi in merito alla voce del titolario da attribuire al documento, l'operatore addetto al protocollo si confronta con il Responsabile della gestione documentale in merito alla corretta classificazione.

3.1.2. PROCESSO DI PRODUZIONE E GESTIONE - CREAZIONE

Nel "Processo di produzione e gestione – Creazione", si considera come *input* del processo esclusivamente il documento di natura informatica (cfr. par. "4.6. - Documento informatico").

Nella fase di creazione, il documento:

- è elaborato dal personale competente ed inviato al Dirigente o altro personale responsabile (ad es. DSGA) per la revisione dello stesso, ovvero è elaborato dal Dirigente stesso;
- è successivamente approvato o dal Dirigente o da altro personale responsabile in base alla competenza.

Nella fase di elaborazione e revisione, è possibile fare circolare il documento tra i soggetti interessati registrandolo come "bozza".

I documenti informatici prodotti, indipendentemente dal *software* utilizzato per la loro creazione, prima della loro sottoscrizione con firma digitale, sono convertiti in uno dei formati *standard* previsti dalla normativa vigente[15], al fine di garantire la loro non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

È possibile utilizzare formati diversi da quelli elencati nell'Allegato 2 "*Formati di file e riversamento*" delle Linee Guida, effettuando una valutazione di interoperabilità, svolta in base alle indicazioni previste nel medesimo Allegato[16].

I formati utilizzati dall'Istituzione scolastica, secondo la valutazione di interoperabilità, sono: PDF, XML e TIFF.

Nella fase di registrazione l'operatore di protocollo provvede:

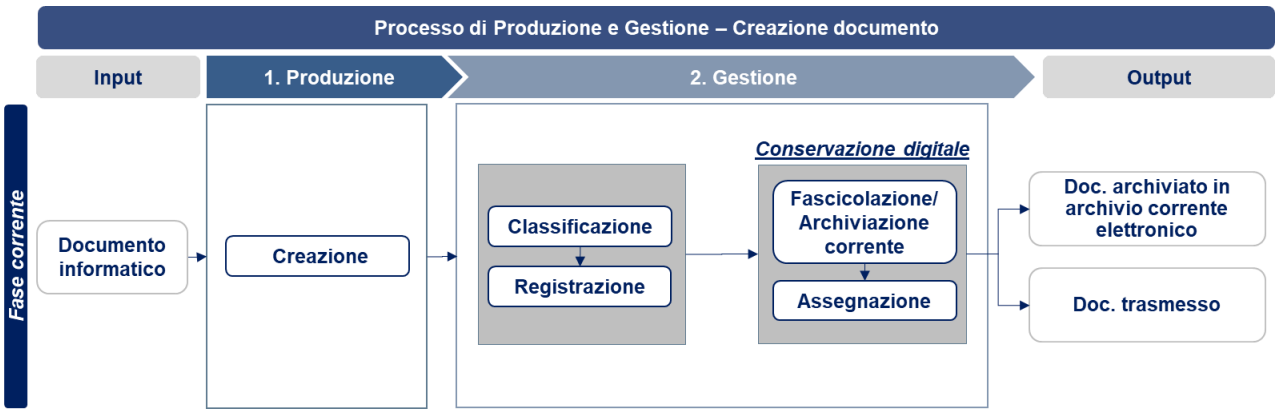
- alla verifica della presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016;
- alla classificazione del documento sulla base del titolario di classificazione[17];
- alla registrazione di protocollo.

Nella fase di fascicolazione/archiviazione corrente l'operatore di protocollo provvede all'inserimento del documento informatico in un fascicolo già esistente o, nel caso in cui il fascicolo non sia presente, provvede a crearlo oppure a richiederne la creazione all'utente opportunamente abilitato.

[15] Allegato 2 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[16] La valutazione di interoperabilità, in quanto parte della gestione informatica dei documenti, viene effettuata periodicamente e, comunque, ogni anno, allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati. Il manuale di gestione documentale contiene l'elenco dei formati utilizzati e la valutazione di interoperabilità.
[17] Nel caso di dubbi in merito alla voce del titolario da attribuire al documento, l'operatore addetto al protocollo si confronta con il Responsabile della gestione documentale in merito alla corretta classificazione.

Successivamente alla fase di fascicolazione/archiviazione, il documento può essere oggetto di una nuova assegnazione o di pubblicazione.

Di seguito si fornisce la rappresentazione grafica del processo sopra descritto.



3.1.3. PROCESSO DI GESTIONE - CLASSIFICAZIONE

La classificazione è l'operazione obbligatoria che consente di organizzare i documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze dell'Istituzione scolastica. Essa è eseguita a partire dal titolario di classificazione.

Il titolario, di cui all'Allegato 2, è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (titolo/classe/eventuale sottoclasse), stabilite sulla base delle funzioni dell'Amministrazione. Esso è definito con apposito decreto del Dirigente Scolastico ed è unico a livello di Istituzione scolastica. Alla data di ultimo aggiornamento del presente documento il titolario è in fase di revisione ed aggiornamento, e verrà reso disponibile non appena possibile.

Tutti i documenti ricevuti e prodotti dall'Istituzione scolastica, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al titolario di classificazione; mediante tale operazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe e eventuale sottoclasse), anche il numero di repertorio del fascicolo. L'operazione suddetta è obbligatoria all'atto della registrazione di protocollo, ma è possibile effettuare delle successive modifiche.

La classificazione, necessaria e fondamentale, è prodromica all'inserzione di un documento all'interno di un determinato fascicolo.

3.1.4. PROCESSO DI GESTIONE - FASCICOLAZIONE

La fascicolazione è l'attività di riconduzione logica (e, nel caso di documenti cartacei, anche fisica) di un documento all'interno dell'unità archivistica che ne raccoglie i precedenti, al fine di mantenere vivo il vincolo archivistico che lega ogni singolo documento alla relativa pratica.

Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento. I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza sotto-fascicolo, secondo l'ordine cronologico di registrazione.

I fascicoli sono organizzati per[18]:

- **affare**, al cui interno vengono compresi documenti relativi a una competenza non proceduralizzata, ma che, nella consuetudine amministrativa, l'Istituzione scolastica deve

[18] Allegato 5 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.

concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta. Esso, infatti, viene chiuso alla chiusura dell'affare;

- **attività**, al cui interno vengono compresi i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale;
- **persona fisica**, al cui interno vengono compresi tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni;
- **persona giuridica**, al cui interno vengono compresi tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni;
- **procedimento amministrativo**, al cui interno vengono conservati una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo. Il fascicolo viene chiuso al termine del procedimento amministrativo[19].

All'interno dei fascicoli è possibile creare dei sotto-fascicoli.

Ogni ufficio si fa carico di gestire le pratiche di propria competenza. Qualora un documento dia luogo all'avvio di un nuovo procedimento, il soggetto preposto provvede all'apertura di un nuovo fascicolo. Al fine di determinare la tipologia di aggregazione documentale (tipologia di serie e tipologia di fascicoli) da adottare, si fa riferimento al Piano di organizzazione delle aggregazioni documentali, riportato all'Allegato 3. Un documento può essere assegnato anche a più fascicoli. La formazione di un nuovo fascicolo avviene attraverso l'operazione di "**apertura**" che comprende la registrazione di alcune informazioni essenziali. Il fascicolo informatico, infatti, reca l'indicazione[20]:

- dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- delle altre amministrazioni partecipanti;
- del responsabile del procedimento;
- dell'oggetto del procedimento;
- dell'elenco dei documenti contenuti;
- dell'identificativo del fascicolo medesimo.

Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario. In alcuni casi, è possibile utilizzare anche il primo livello (titolo), come per i fascicoli di persona fisica.

In presenza di un documento da inserire in un fascicolo, i soggetti deputati alla fascicolazione stabiliscono, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se esso si colloca nell'ambito di un procedimento in corso, oppure se dà avvio ad un nuovo procedimento:

1. se si colloca nell'ambito di un procedimento in corso:
    - selezionano il relativo fascicolo;
    - collegano la registrazione di protocollo del documento al fascicolo selezionato (se si tratta di un documento su supporto cartaceo, assicurano l'inserimento fisico dello stesso nel relativo carteggio);

[19] A norma dell'art. 41, comma 2, del CAD, "*La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati;* […]".
[20] A norma dell'art. 41, comma 2-*ter*, del CAD.

2. se dà avvio ad un nuovo procedimento:
    - eseguono l'operazione di apertura del fascicolo di cui al paragrafo precedente;
    - assegnano la pratica su indicazione del responsabile del procedimento;
    - collegano la registrazione di protocollo del documento al fascicolo aperto.

Il fascicolo viene chiuso al termine del procedimento. La data di chiusura si riferisce alla data dell'ultimo documento prodotto. Quando si verifica un errore nella assegnazione di un fascicolo, l'utente abilitato all'operazione di fascicolazione provvede 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 che effettua la modifica con la data e l'ora dell'operazione.

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 la scuola 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 ed eventuale sottoclasse);
- il numero di fascicolo (ed altre eventuali partizioni in sotto-fascicoli e inserti);
- la data di chiusura;
- l'oggetto del fascicolo (ed eventualmente l'oggetto dei sotto-fascicoli e inserti);
- 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 di storico o da scartare).

Il repertorio dei fascicoli è costantemente aggiornato.

Oltre ad essere inserito in un fascicolo, un documento può essere inserito in una o più serie documentali, che rappresentano aggregazioni di documenti con caratteristiche omogenee, raggruppati ad esempio in base alla tipologia documentaria (es. delibere, decreti, fatture) o alla provenienza (cioè se prodotti da un medesimo organo, come il Consiglio d'istituto o il Collegio dei docenti) o all'oggetto (es. documenti relativi ad un progetto PON)[21]. I documenti all'interno di una serie, non essendo aggregati utilizzando il titolario di classificazione come nel caso dei fascicoli, possono appartenere a titoli e classi differenti tra loro. La serie documentale stessa, quindi, non viene classificata in base alle partizioni del titolario.

Specifiche indicazioni in merito alle modalità di inserimento dei documenti nelle aggregazioni documentali, sono contenute nell'Appendice "*Focus sulle aggregazioni documentali delle Istituzioni scolastiche*" alle "Linee guida per la gestione documentale nelle Istituzioni scolastiche".

3.1.5. PROCESSO DI GESTIONE - ARCHIVIAZIONE

Le Istituzioni scolastiche definiscono nel proprio manuale la gestione degli archivi rifacendosi alla seguente articolazione archivistica[22]:

- **archivio corrente**: riguarda i documenti necessari alle attività correnti;

[21] Tale definizione di "serie documentale" è basata sul paragrafo 4 dell'Allegato 5 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[22] "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.

- **archivio di deposito**: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- **archivio storico**: riguarda i documenti storici selezionati per la conservazione permanente.

L'archiviazione, per alcune fattispecie di documenti, può avvenire presso archivi gestiti a livello centrale dal Ministero dell'Istruzione. A titolo esemplificativo, le istanze che pervengono alla scuola mediante il Servizio Istanze OnLine, che permette di effettuare in modalità digitale la presentazione delle domande connesse ai principali procedimenti amministrativi dell'Amministrazione, sono protocollate in ingresso dalla AOO appositamente costituita presso il Ministero dell'Istruzione, e sono rese disponibili alle Istituzioni scolastiche.

Tenendo conto che l'archivio corrente è organizzato su base annuale e che il passaggio dall'archivio corrente all'archivio di deposito è possibile solo qualora il fascicolo contenga documenti afferenti a procedimenti conclusi, è necessario verificare quali fascicoli contengono documenti afferenti ad una pratica chiusa. Tale verifica può essere effettuata:

- ad ogni fine anno, in modo tale che i fascicoli delle pratiche non chiuse entro il dicembre precedente vengano "trascinati" nell'archivio corrente del nuovo anno e i fascicoli delle pratiche chiuse vengano "trascinati" nell'archivio di deposito;

oppure,

- in corso d'anno qualora la pratica sia chiusa.

Dato che sarebbe troppo oneroso e pressoché inutile conservare illimitatamente l'archivio nella sua totalità esso deve essere periodicamente sottoposto ad una selezione razionale, che va prevista fin dal momento della creazione dei documenti, e va disciplinata nel piano di conservazione[23] (Allegato 3), a sua volta integrato con il sistema di classificazione. A tal fine si inserisce lo sfoltimento (attività eseguita nell'archivio corrente).

Lo sfoltimento è un'attività propedeutica ad una corretta conservazione documentale: al momento della chiusura del fascicolo, ad esempio, oppure prima del trasferimento dello stesso all'archivio di deposito, l'eventuale carteggio di carattere transitorio e strumentale deve essere selezionato ed estratto dal fascicolo da parte dell'operatore incaricato del trattamento della pratica. Si tratta, cioè, di estrarre dal fascicolo le copie e i documenti che hanno appunto carattere strumentale e transitorio, utilizzati dall'operatore incaricato o dal responsabile del procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad es., appunti, promemoria, copie di normativa e documenti di carattere generale).

Nell'ambito dell'archivio di deposito avviene l'operazione di scarto che non deve essere applicato, salvo diverse indicazioni dettate dalla Soprintendenza archivistica, su documentazione facente parte dell'archivio storico le cui pratiche siano esaurite da oltre 40 anni, mentre può essere sempre effettuato sulla documentazione dell'archivio di deposito, che contiene tutte le pratiche chiuse che non abbiano maturato i 40 anni di conservazione.

La carenza di spazio negli archivi nonché la produzione smisurata e la conservazione di carte anche inutili non possono giustificare la distruzione non autorizzata di documenti e nemmeno la cancellazione di documenti elettronici[24], poiché lo scarto dei documenti dell'archivio della scuola è subordinato

[23] Art. 68, comma 1, del D.P.R. 445/2000.
[24] Art. 169, 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".

all'autorizzazione della Soprintendenza archivistica[25]. È una forma di scarto anche la cancellazione di documenti elettronici.

Fatto salvo quanto sopra, l'operazione di scarto è supportata dal massimario di conservazione e scarto, grazie al quale è prodotto annualmente l'elenco dei documenti e dei fascicoli per i quali è trascorso il periodo obbligatorio di conservazione e che quindi sono suscettibili di scarto archivistico. I documenti selezionati per la conservazione permanente sono depositati contestualmente agli strumenti che ne garantiscono l'accesso nell'Archivio di Stato competente per territorio o trasferiti nella separata sezione di archivio, secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali.

3.2. PROCESSO DI CONSERVAZIONE

Il ciclo di gestione di un documento informatico termina con il suo versamento in un sistema di conservazione che è coerente con quanto disposto dal CAD e dalle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*". Il processo di conservazione prevede quattro fasi:

- versamento in archivio di deposito;
- scarto;
- versamento in archivio storico;
- delocalizzazione.

In questo contesto, si inserisce la figura del Responsabile della conservazione, i cui compiti sono stati descritti al precedente paragrafo 2.2.

Ai sensi dell'art. 34, comma 1-*bis*, del CAD, come modificato dall'art. 25, comma 1, lett. e), del D.L. 76/2020 (c.d. "Decreto Semplificazione"), convertito con Legge n. 120/2020, le Pubbliche Amministrazioni possono procedere alla conservazione dei documenti informatici:

a) all'interno della propria struttura organizzativa;
b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID[26], avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione.

Per la conservazione dei documenti informatici, l'Istituzione scolastica per taluni documenti si avvale del modello interno, mentre per altri documenti si riserva la facoltà di avvalersi del nodello esterno.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo

[25] Art. 21, comma 1, 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".

[26] L'AgID ha adottato con Determinazione n. 455/2021 il "*Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*" e i relativi allegati. L'allegato A, in particolare, fissa i requisiti per l'erogazione del servizio di conservazione per conto delle Pubbliche Amministrazioni. Il regolamento prevede, inoltre, l'istituzione di un *marketplace* per i servizi di conservazione quale sezione autonoma del *Cloud Marketplace* cui possono iscriversi i soggetti, pubblici e privati, che intendono erogare il servizio di conservazione dei documenti informatici per conto delle Pubbliche Amministrazioni. L'iscrizione al *marketplace* non è obbligatoria ma i conservatori che intendono partecipare a procedure di affidamento da parte delle Pubbliche Amministrazioni devono ugualmente possedere i requisiti previsti nel suddetto regolamento e sono sottoposti all'attività di vigilanza di AgID.

superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Ai sensi dell'art. 44, comma 1-*ter*, del CAD, come da ultimo modificato dal D.L. 76/2020, "*In tutti i casi in cui la legge prescrive obblighi di conservazione, anche a carico di soggetti privati, il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida*".

In ogni caso, i sistemi di conservazione devono consentire la possibilità di eliminare i documenti ove necessario (laddove previsto dalla normativa vigente).

Si tenga conto altresì del periodo di conservazione e di scarto dei documenti che contengono al loro interno dati personali. In base alla normativa vigente in materia di protezione dei dati personali, infatti, tale periodo di tempo non deve essere superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati.

3.2.1. VERSAMENTO IN ARCHIVIO DI DEPOSITO

Nella fase di versamento in archivio di deposito[27] il responsabile per la tenuta degli archivi[28]:

- controlla periodicamente tutte le pratiche fascicolate presenti nell'archivio corrente, sia cartaceo che elettronico, al fine di identificare quelle per cui la lavorazione è già stata conclusa e compila una lista della documentazione presente nelle pratiche chiuse;
- provvede allo sfoltimento eliminando l'eventuale carteggio di carattere transitorio e strumentale presente nel fascicolo;
- provvede al versamento di tutta la documentazione, sia cartacea che elettronica, presente nella lista all'archivio di deposito;
- provvede al versamento nell'archivio corrente del nuovo anno della documentazione delle pratiche appartenenti alle pratiche presenti nell'archivio corrente (ancora in fase di lavorazione).

Di seguito, si fornisce la rappresentazione grafica del processo sopra descritto.

[27] L'art. 67 del D.P.R. 445/2000 disciplina il trasferimento dei documenti all'archivio di deposito, prevedendo, nel dettaglio che "*1. Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione. 2. Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente. 3. Il responsabile del servizio per la gestione dei flussi documentali e degli archivi deve formare e conservare un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito.*".

[28] Il responsabile per la tenuta degli archivi può essere il Dirigente Scolastico o altro personale in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del D.P.R. 28 dicembre 2000, n. 445.

3.2.2. SCARTO

Nell'archivio di deposito si eseguono le attività relative alla fase di scarto in cui 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 massimario di conservazione e scarto;
- procede con la compilazione di una lista della documentazione da scartare e da inviare alla Soprintendenza per l'approvazione e la comunica al Responsabile della gestione documentale;
- invia, in caso di documenti cartacei, la documentazione presente sulla lista al soggetto competente per la distruzione della carta;
- provvede ad eliminare la documentazione elettronica presente nella lista approvata dalla Soprintendenza.

In caso di affidamento esterno del servizio di conservazione, l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione e trasmesso al Responsabile della conservazione che, a sua volta, verificato il rispetto dei termini temporali stabiliti dal massimario di conservazione e scarto, lo comunica al Responsabile della gestione documentale.

3.2.3. VERSAMENTO IN ARCHIVIO STORICO

Nella fase di versamento in archivio storico[29], il responsabile per la tenuta degli archivi:

- verifica se nell'archivio di deposito esistono pratiche esaurite da oltre 40 anni, sia in forma cartacea che elettronica;
- provvede a preparare una lista contenente tutta la documentazione presente nelle pratiche stesse, qualora dovessero essere presenti pratiche esaurite da oltre 40 anni;
- provvede ad inviare la lista della documentazione da versare al personale competente, in caso di documentazione cartacea, che deve individuare un archivio storico con sufficiente spazio per dare seguito al versamento.

3.2.4. DELOCALIZZAZIONE

La fase di delocalizzazione è avviata nel caso in cui, dopo aver effettuato le operazioni di scarto e dopo aver effettuato l'eventuale versamento nell'archivio storico, dalla verifica del grado di saturazione dell'archivio di deposito cartaceo, risulta che l'archivio è saturo. Nel caso in cui l'archivio di deposito cartaceo dovesse essere saturo, il responsabile per la tenuta degli archivi:

- provvede ad individuare la documentazione da delocalizzare selezionandola tra quella più prossima alla data di scarto;
- provvede a stilare la lista dei documenti da delocalizzare.

L'addetto competente:

- analizza la documentazione ricevuta;
- provvede a identificare una struttura con sufficiente spazio negli archivi;

[29] L'art. 69 del D.P.R. 445/2000, rubricato "Archivi storici", prevede che "*I documenti selezionati per la conservazione permanente sono trasferiti contestualmente agli strumenti che ne garantiscono l'accesso, negli Archivi di Stato competenti per territorio o nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali*".

- autorizza la delocalizzazione della documentazione presso una struttura interna nel caso in cui questa sia disponibile.

Il responsabile per la tenuta degli archivi provvede ad inviare la richiesta di autorizzazione alla Soprintendenza competente. Una volta ricevuta l'approvazione dalla Soprintendenza competente, il responsabile per la tenuta degli archivi provvede ad inviare la documentazione da delocalizzare.

4. IL DOCUMENTO AMMINISTRATIVO

Per documento amministrativo, ai sensi dell'art. 1, comma 1, lett. a), del D.P.R. 28 dicembre 2000, n. 445, si intende "*ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa*".

Nell'ambito del processo di gestione documentale, il documento amministrativo dal punto di vista operativo è classificabile in documento:

- ricevuto;
- inviato;
- di rilevanza esterna;
- di rilevanza interna.

In base alla natura, invece, è classificabile in documento:

- analogico;
- informatico.

L'art. 40, comma 1, del CAD, come modificato da ultimo dall'art. 66, comma 1, del D.Lgs. 13 dicembre 2017, n. 217, stabilisce che "*Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le Linee guida*".

Per ciò che concerne la trasmissione dei documenti tra Pubbliche Amministrazioni, ai sensi di quanto disposto dall'art. 47 del CAD, essa deve avvenire:

- attraverso l'utilizzo della posta elettronica[30]; *ovvero*
- in cooperazione applicativa.

Le suddette comunicazioni sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. Il comma 2, del citato art. 47, stabilisce infatti che "*Ai fini della verifica della provenienza le comunicazioni sono valide se: a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata; b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445; c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle Linee guida. È in ogni caso esclusa la trasmissione di documenti a mezzo fax; d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*".

[30] Come riportato nell'Appendice C dell'Allegato 6 alle *Linee Guida per la formazione, gestione e conservazione dei documenti informatici*, l'utilizzo della posta elettronica è *"da intendersi quale modalità transitoria nelle more dell'applicazione delle comunicazioni tra AOO tramite cooperazione applicativa"*. Pertanto, la cooperazione applicativa viene identificata come l'unica modalità a tendere per le comunicazioni di documenti amministrativi protocollati tra AOO.

Specifiche indicazioni in materia di scambio di documenti amministrativi protocollati tra AOO sono contenute nell'Allegato 6 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

4.1. DOCUMENTO RICEVUTO

La corrispondenza in ingresso può essere acquisita dall'Istituzione scolastica con diversi mezzi e modalità in base sia alla modalità di trasmissione scelta dal mittente sia alla natura del documento. Un documento informatico può essere recapitato[31]:

- a mezzo posta elettronica convenzionale (PEO);
- a mezzo posta elettronica certificata (PEC);
- mediante supporto removibile (ad es. CD, *pendrive*).

Un documento analogico, assunto che le principali tipologie di documenti analogici che pervengono alle Istituzioni scolastiche sono telegrammi, documenti per posta ordinaria e raccomandate, può essere recapitato:

- attraverso il servizio di posta tradizionale;
- *pro manibus*.

I documenti, analogici o digitali, di cui non sia identificabile l'autore sono regolarmente aperti e registrati al protocollo (con indicazione "Mittente anonimo"), salvo diversa valutazione del Dirigente Scolastico, che provvederà ad eventuali accertamenti.

I documenti ricevuti privi di firma ma il cui mittente è comunque chiaramente identificabile, vengono protocollati (con indicazione "Documento non sottoscritto") e inoltrati al responsabile del procedimento, che valuterà la necessità di acquisire la dovuta sottoscrizione per il perfezionamento degli atti.

La funzione notarile del protocollo (cioè della registratura) è quella di attestare data e provenienza certa di un documento senza interferire su di esso. Sarà poi compito del responsabile del procedimento valutare, caso per caso, ai fini della sua efficacia riguardo ad un affare o ad un determinato procedimento amministrativo, se il documento privo di firma possa essere ritenuto valido o meno[32].

4.2. DOCUMENTO INVIATO

I documenti informatici sono inviati all'indirizzo elettronico dichiarato dai destinatari, abilitato alla ricezione della posta per via telematica.

4.3. DOCUMENTO DI RILEVANZA ESTERNA

Per documento di rilevanza esterna si intende qualunque documento ricevuto/trasmesso da/a altro Ente o altra persona fisica o giuridica. La gestione è normata dal CAD.

4.4. DOCUMENTO DI RILEVANZA INTERNA

Per documenti di rilevanza interna si intendono tutti quelli che a qualunque titolo sono scambiati tra UOR o persone dell'Istituzione scolastica stessa.

Possono distinguersi in:

[31] Per ciò che riguarda la trasmissione dei documenti tra le Pubbliche Amministrazioni, specifiche indicazioni sono contenute all'interno dell'art. 47 del CAD.
[32] Per approfondimenti in merito alle tipologie di sottoscrizione elettronica, si veda il par. "4.6.1 - Le firme elettroniche".

- **comunicazioni informali tra UOR** (documenti di natura prevalentemente informativa): per comunicazioni informali tra unità si intendono gli scambi di informazioni che non hanno valenza giuridico probatoria, né rilevanza ai fini dell'azione amministrativa. Queste comunicazioni avvengono, di norma, tramite PEO e non sono soggette a protocollazione ed archiviazione;
- **scambio di documenti fra UOR** (documenti di natura prevalentemente giuridico-probatoria): per scambio di documenti fra unità si intendono le comunicazioni ufficiali di un certo rilievo ai fini dell'azione amministrativa e delle quali si deve tenere traccia. Le comunicazioni di questo genere devono comunque essere protocollate.

4.5. DOCUMENTO ANALOGICO

Per documento analogico si intende "*la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*"[33].

Si definisce "originale" il documento cartaceo nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali, comprendente tutti gli elementi di garanzia e di informazione del mittente e del destinatario, stampato su carta intestata e dotato di firma autografa[34].

La sottoscrizione di un documento determina:

- l'**identificazione dell'autore** del documento;
- la **paternità** del documento: con la sottoscrizione l'autore del documento si assume la paternità dello stesso, anche in relazione al suo contenuto. A questo proposito si parla di non ripudiabilità del documento sottoscritto;
- l'**integrità** del documento: il documento scritto e sottoscritto manualmente garantisce da alterazioni materiali da parte di persone diverse da quella che lo ha posto in essere.

4.6. DOCUMENTO INFORMATICO

Per documento informatico si intende "*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*"[35]. Il documento informatico, come precisato nel paragrafo 2.1.1. delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate da AgID, è formato mediante una delle seguenti modalità:

"*a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2;*

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

[33] Art. 1, comma 1, lett. p-*bis*), D.lgs. 7 marzo 2005, n. 82, CAD.
[34] Per approfondimenti in merito alla ricezione di documenti privi di firma, si veda il par. "4.1. – Documento ricevuto".
[35] Art. 1, comma 1, lett. p), D.lgs. 7 marzo 2005, n. 82, CAD. La definizione è altresì contenuta all'interno dell'art. 1, comma 1, lett. b), del D.P.R. 445/2000: "*b) DOCUMENTO INFORMATICO: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.*".

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica".

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

A seconda che il documento informatico sia formato secondo una delle modalità sopra riportate, l'immodificabilità e l'integrità sono garantite da una o più delle operazioni indicate nelle citate Linee Guida, al paragrafo 2.1.1. (pag. 13).

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati associati dall'Istituzione scolastica ai documenti informatici e ai documenti amministrativi informatici corrispondono a quelli obbligatori previsti nell'Allegato 5 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*". Potranno essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici, come i documenti soggetti a registrazione particolare.

Se necessari e definiti, gli ulteriori metadati e le particolari tipologie di documenti informatici a cui devono essere associati vengono riportati nell'Allegato 4.

Un documento nativo informatico non può essere convertito in formato analogico prima della sua eventuale acquisizione a sistema di protocollo o archiviazione informatica. Nel caso di documenti soggetti a sottoscrizione, è possibile fare ricorso alla firma elettronica avanzata (FEA), messa a disposizione delle Istituzioni scolastiche dal Ministero. I Dirigenti Scolastici ed i Direttori dei Servizi Generali ed Amministrativi delle Istituzioni Scolastiche statali di ogni ordine e grado possono, inoltre, fare ricorso alla firma digitale, tramite l'apposita funzione presente sul SIDI. Le suddette modalità di firma vengono delineate ed analizzate nel paragrafo successivo.

4.6.1. LE FIRME ELETTRONICHE

La firma elettronica costituisce la modalità ordinaria di firma dei documenti informatici.

In particolare, la normativa vigente in materia individua diverse tipologie di sottoscrizione elettronica:

- firma elettronica, ovvero l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzata come metodo di autentificazione (art. 3, n. 10, Reg. UE n. 910/2014);
- firma elettronica avanzata, ovvero l'insieme dei dati allegati o connessi ad un documento informatico che consentono l'identificazione del firmatario e garantiscono la connessione univoca con quest'ultimo (art. 3, n. 11, Reg. UE n. 910/2014);
- firma elettronica qualificata, ovvero una firma elettronica avanzata che si basa su un certificato qualificato (art. 3, n. 12, Reg. UE n. 910/2014);
- firma digitale, ovvero una particolare firma elettronica qualificata che si basa su un certificato qualificato e su un sistema di chiavi crittografiche (art. 1, comma 1, lett. s), CAD).

In considerazione del tipo di tecnologia utilizzata, la firma digitale rappresenta la tipologia di firma più sicura. Essa è disciplinata dall'art. 24 del CAD il quale, ai commi 1, 2, 3 e 4, prevede che "*1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata. 2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente. 3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento*

della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso. 4. Attraverso il certificato qualificato si devono rilevare, secondo le Linee guida, la validità del certificato stesso, nonché gli elementi identificativi del titolare di firma digitale e del certificatore e gli eventuali limiti d'uso. Le linee guida definiscono altresì le modalità, anche temporali, di apposizione della firma".

Si tenga conto, altresì, che secondo quanto stabilito dall'art. 24, comma 4-*bis*, del CAD, qualora ad un documento informatico sia apposta una firma digitale o un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso, il documento si ha come non sottoscritto, salvo che lo stato di sospensione sia stato annullato. Ad ogni modo, l'eventuale revoca o sospensione, comunque motivata, ha effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

Si rappresenta, inoltre, che l'articolo 20, comma 1-*bis*, del CAD, come modificato dall'art. 20, comma 1, lett. a) del D.Lgs. 13 dicembre 2017, n. 217, stabilisce che "*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida*".

Ai sensi dell'art. 20, commi 1-*ter* e 1-*quater*, del CAD, introdotti dall'art. 20, comma 1, lett. b), del D.lgs. 13 dicembre 2017, n. 217: "(1-*ter*) *L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria. (1-quater) Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa, anche regolamentare, in materia di processo telematico*".

Dalle disposizioni sopra riportate, risulta possibile individuare quale sia l'efficacia probatoria del documento informatico, sulla base del tipo di firma apposta sullo stesso. Nel dettaglio:

- i **documenti sottoscritti con firma elettronica "semplice"** soddisfano il requisito della forma scritta e il loro valore probatorio è liberamente valutabile in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità della firma stessa;
- i **documenti sottoscritti con firma elettronica avanzata, firma elettronica qualificata e firma digitale** soddisfano il requisito della forma scritta e hanno l'efficacia prevista dall'art. 2702 c.c.[36], ovvero fanno piena prova fino a querela di falso;
- i **documenti sottoscritti con firma digitale con certificato revocato, scaduto o sospeso** fanno piena prova fino a disconoscimento, ai sensi di quanto disposto dall'art. 2712 c.c.[37].

[36] L'art. 2702 c.c. stabilisce che "*La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta*".

[37] L'art. 2712 c.c. stabilisce che "*Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime*".

Si rileva, inoltre, che l'art. 25 del CAD, rubricato "*Firma autenticata*", prevede che la firma elettronica o qualsiasi altro tipo di firma elettronica avanzata, autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato, si ha per riconosciuta ai sensi dell'art. 2703 c.c.[38].

Il CAD[39] stabilisce, altresì, che gli atti elencati ai numeri da 1 a 12 dell'art. 1350 c.c. debbano essere sottoscritti con firma elettronica qualificata o digitale, a pena di nullità. Gli atti di cui al n. 13, del citato art. 1350 c.c., invece, oltre ai tipi di firma sopra menzionati, possono essere sottoscritti anche con firma elettronica avanzata o devono essere formati con le ulteriori modalità di cui all'articolo 20, comma 1-*bis*, primo periodo[40].

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore di protocollo ha verificato la validità della firma digitale con apposita funzione sul sistema di protocollo.

Fatto salvo quanto sopra rappresentato, i documenti informatici possono essere anche senza firma e in tal caso si seguirà la disciplina contenuta al par. "4.1. – Documento ricevuto"[41].

Da ultimo, si rappresenta che, in tutti gli atti cartacei che provengono e che sono generati da sistemi automatizzati, la firma sul documento cartaceo del funzionario responsabile può essere sostituita dalla dicitura dalla "*Firma autografa sostituita a mezzo stampa, ai sensi dell'art. 3, comma 2, Legge 39/1993*".

4.7. CONTENUTI MINIMI DEI DOCUMENTI

Occorre che i documenti amministrativi, sia analogici che informatici, aventi rilevanza esterna, contengano le seguenti informazioni:

- denominazione e logo dell'amministrazione mittente;
- indirizzo completo dell'amministrazione (via, numero, CAP, città, provincia);
- indirizzo di posta elettronica certificata dell'Istituzione scolastica;
- indicazione dell'Istituzione scolastica e dell'UOR che ha prodotto il documento;
- il numero di telefono dell'UOR e del RUP (facoltativo, a piè di pagina se previsto);
- C.F., P.IVA, Codice iPA, Codice univoco per la F.E.

Inoltre, il documento deve recare almeno le seguenti informazioni:

- luogo e data (gg/mm/anno) di redazione del documento;
- numero di protocollo;
- oggetto del documento.

[38] L'art. 2703 c.c. stabilisce che "*1. Si ha per riconosciuta la sottoscrizione autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato. 2. L'autenticazione consiste nell'attestazione da parte del pubblico ufficiale che la sottoscrizione è stata apposta in sua presenza. Il pubblico ufficiale deve previamente accertare l'identità della persona che sottoscrive*".
[39] Art. 21, comma 2-*bis*, del CAD.
[40] L'art. 1350 c.c. stabilisce che "*Devono farsi per atto pubblico o per scrittura privata, sotto pena di nullità: 1) i contratti che trasferiscono la proprietà di beni immobili; 2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta; 3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti; 4) i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione; 5) gli atti di rinunzia ai diritti indicati dai numeri precedenti; 6) i contratti di affrancazione del fondo enfiteutico; 7) i contratti di anticresi; 8) i contratti di locazione di beni immobili per una durata superiore a nove anni; 9) i contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato; 10) gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite dello Stato; 11) gli atti di divisione di beni immobili e di altri diritti reali immobiliari; 12) le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti; 13) gli altri atti specialmente indicati dalla legge*".
[41] Per approfondimenti in merito alla ricezione di documenti privi di firma, si veda il par. "4.1. – Documento ricevuto"

Esso non deve contenere il riferimento al numero di fax, coerentemente a quanto disposto dall'art. 14, comma 1-*bis*, del decreto-legge 21 giugno 2013, n. 69, così come modificato dalla legge 9 agosto 2013, n. 98, recante "*Misure per favorire la diffusione del domicilio digitale*", il quale stabilisce che, ai fini della verifica della provenienza delle comunicazioni, è in ogni caso esclusa la trasmissione di documenti a mezzo fax tra Pubbliche Amministrazioni. È facoltà del Responsabile della gestione documentale aggiungere a quelle fin qui esposte altre regole per la determinazione dei contenuti e per la definizione della struttura dei documenti informatici. Si evidenzia, altresì, che in tema di accesso ai documenti amministrativi[42], a ciascuna Istituzione scolastica spetta l'onere di specificare con precisione gli estremi di registrazione di un documento sui propri sistemi di protocollo.

L'indicazione di tali elementi (tra cui l'oggetto) deve essere rispondente agli *standard* indicati nel presente manuale[43]. Ciò perché prerequisito essenziale del pieno godimento del diritto all'accesso agli atti è la reperibilità di quest'ultimi che è assicurata da una corretta e standardizzata definizione/trascrizione dell'oggetto.

4.8. PROTOCOLLABILITÀ DI UN DOCUMENTO

Sono oggetto di registrazione obbligatoria, ai sensi dell'art. 53, comma 5, del D.P.R. n. 445 del 2000, i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici[44].

Inoltre, l'art. 40-*bis* del CAD, come modificato dagli artt. 37, comma 1, e 66, comma 1, del D.lgs. 13 dicembre 2017, n. 217, prevede che formano oggetto di registrazione di protocollo ai sensi dell'articolo 53[45] del D.P.R. n. 445 del 2000, "*le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle Linee guida*".

Sono invece esclusi dalla registrazione obbligatoria[46]:

- le gazzette ufficiali;
- i bollettini ufficiali e i notiziari della Pubblica Amministrazione;
- 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;
- tutti i documenti già soggetti a registrazione particolare dell'Amministrazione.

Nel caso in cui sia necessario attribuire una data certa a un documento informatico non soggetto a protocollazione prodotto all'interno dell'Istituzione scolastica, si applicano le regole per la "validazione

[42] Nell'ambito della disciplina di accesso, l'art. 1, comma 1, lett. d), della L. 241/1990 definisce il documento amministrativo come "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale*".
[43] Per ulteriori approfondimenti, si veda il par. "5.2. - Scrittura di dati di protocollo".
[44] Le *"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici",* emanate dall'AgID, prevedono che "*La registrazione informatica dei documenti è rappresentata dall'insieme di dati in forma elettronica allegati o connessi al documento informatico al fine dell'identificazione univoca di tutti i documenti prodotti e acquisiti. Per la Pubblica Amministrazione vale quanto disposto ai sensi dell'articolo 53, comma 5, del TUDA*".
[45] L'art. 53, comma 5, del D.P.R. 445/2000, al primo periodo prevede che "*Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici*".
[46] Art. 53, comma 5, del D.P.R.445/2000.

temporale" di cui al DPCM del 22 febbraio 2013 "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*".

In particolare, la "validazione temporale" consente di stabilire il momento temporale in cui il documento informatico è stato formato ed è definita come il risultato di una procedura informatica in grado di offrire un riferimento temporale opponibile a terzi.

Lo strumento per ottenere questo risultato è la "marca temporale"[47], ovvero "*il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo*".

5. IL PROTOCOLLO INFORMATICO

5.1. PROTOCOLLAZIONE

Per protocollazione si intende l'attività di registrazione di protocollo mediante la quale è eseguita l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

I documenti che devono essere registrati a protocollo sono indicati nel paragrafo "4.8. - Protocollabilità di un documento amministrativo".

Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immodificabile. Quindi non è consentito:

- protocollare un documento già protocollato;
- apporre manualmente la segnatura di protocollo, salvo i casi in cui l'apposizione tramite l'applicativo possa deteriorare le informazioni fondamentali del documento (ad es. sovrapposizione del timbro in ingresso al timbro in uscita, presenza di etichetta adesiva plastificata che verrebbe annerita dalla stampante);
- in caso di spedizione ed arrivi massivi, apporre una segnatura del tipo es.: 1741/1, 1741/2, 1741/3, ecc. oppure attribuire ad essi lo stesso numero di protocollo;
- protocollare sul registro ufficiale atti di rilevanza interna senza utilizzare l'apposita modalità di protocollazione interna;
- selezionare un numero di protocollo alla data di ricezione del documento al fine di effettuare l'operazione di protocollazione in una data successiva;
- apporre la firma sul documento successivamente alla protocollazione;
- associare ad una precedente registrazione ulteriori allegati prodotti o ricevuti successivamente.

La protocollazione per ogni documento è effettuata mediante la memorizzazione dei seguenti elementi[48]:

- numero di protocollo del documento 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;

[47] Art. 1, comma 1, del DPCM 22 febbraio 2013.
[48] Tali elementi sono definiti nell'art. 53, comma 1, del D.P.R. 445/2000.

- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari, in grado di identificarne univocamente il contenuto, registrata in forma non modificabile;
- informazioni inerenti all'assegnazione interna all'amministrazione e la eventuale classificazione[49].

L'operazione di protocollazione, così come appena descritta, deve essere effettuata solo **dopo** aver caricato sul sistema il documento principale e i suoi allegati (che devono riportare tutti il medesimo numero di protocollo).

5.2. SCRITTURA DI DATI DI PROTOCOLLO

La gestione informatizzata dei flussi documentali dell'Istituzione scolastica necessita una particolare attenzione alla qualità delle informazioni associate, in fase di protocollazione, ai documenti interessati, al fine di evitare che questi risultino non reperibili o difficilmente rintracciabili.

A tal fine, sono di seguito riportate le regole cui gli utilizzatori del sistema di protocollo informatico devono attenersi, per la redazione dei seguenti dati:

TIPO DI DATI	REGOLE
Nomi di persona	- Prima il nome e poi il cognome - Tutto maiuscolo **Esempio**: MARIO ROSSI
Titoli professionali e/o istituzionali	Sempre omessi
Nomi di città e di stati	In lingua italiana, per esteso e senza puntare **Esempio**: San Vitaliano (Na) e non S. Vitaliano (Na)
Nomi di ditte e società	- Se riportano nomi di persona valgono le precedenti regole - Usare sigle, in maiuscolo e senza punti o, in alternativa, acronimi - La forma societaria senza punti **Esempio**: GIUSEPPE BIANCO, ACME SpA
Enti e associazioni in genere	Usare sigle in maiuscolo e senza punti, laddove disponibili
Ministeri	Usare la forma ridotta e puntata della sola parola Ministero, oppure l'acronimo **Esempio**: MIN. ISTRUZIONE, oppure MI
Enti di secondo livello	Usare la forma estesa o acronimi noti

[49] Tale elemento è previsto dalle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.

TIPO DI DATI	REGOLE
Sigle in genere	In maiuscolo e senza punti **Esempio**: MI
Virgolette e apici	- Digitare il carattere direttamente dalla tastiera - Non eseguire la funzione copia e incolla di *Windows*
Date	Usare il seguente formato numerico: GG-MM-AAAA o GGMMAAAA **Esempio**: 20-07-2020 o 20072020 e non 20/07/2020

5.3. SEGNATURA 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. L'operazione di segnatura è effettuata dall'applicativo automaticamente e contemporaneamente all'operazione di registrazione di protocollo[50]. Essa consente di individuare ciascun documento in modo inequivocabile.

Le informazioni minime previste nella segnatura di protocollo sono[51]:

- il progressivo di protocollo[52];
- la data di protocollo;
- l'identificazione in forma sintetica dell'Amministrazione o dell'Area Organizzativa individuata.

L'operazione di segnatura di protocollo può includere ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo. Quando il documento è indirizzato ad altre Amministrazioni ed è formato e trasmesso con strumenti informatici, la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.

La segnatura di protocollo dell'Istituzione scolastica, in ottemperanza alle regole tecniche precedentemente esposte, adotta il *set* di informazioni minime ed utilizza quale identificativo dell'Amministrazione il codice con cui l'Istituzione scolastica è univocamente identificata sull'indice delle Pubbliche Amministrazioni.

5.4. DIFFERIMENTO DELLA REGISTRAZIONE DI PROTOCOLLO

Le registrazioni di protocollo dei documenti pervenuti all'Istituzione scolastica sono effettuate nella giornata di arrivo e comunque non oltre tre giorni lavorativi dal ricevimento di detti documenti. Qualora nei tempi sopra indicati non possa essere effettuata la registrazione di protocollo, il Responsabile della gestione può autorizzare la registrazione in tempi successivi fissando comunque un limite di tempo e conferendo valore, nel caso di scadenze predeterminate, al timbro datario d'arrivo, esplicitandone l'autorizzazione attraverso apposite note interne. Il protocollo differito consiste nel differimento dei termini di registrazione e si applica ai documenti in arrivo.

[50] Art. 55, comma 2, D.P.R. 445/2000 e "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID, pag. 20.
[51] Tali informazioni sono definite all'art. 55 del D.P.R. 445/2000.
[52] Ai sensi dell'art. 57, comma 1, del D.P.R. 445/2000 44 "*Il numero di protocollo è progressivo e costituito da almeno sette cifre numeriche. La numerazione è rinnovata ogni anno solare*.".

5.5. RICEVUTA DI AVVENUTA PROTOCOLLAZIONE

La ricezione dei documenti via PEC comporta l'invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, una al servizio di protocollazione informatica. Nel caso di ricezione di documenti informatici mediante PEC, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata, utilizzato dall'Istituzione scolastica con gli *standard* specifici.

In caso di documenti pervenuti via PEO, è inviata una conferma di ricezione con relativa segnatura informatica in formato XML del documento attraverso apposita funzione ("Inoltro" o "Rispondi").

5.6. REGISTRO GIORNALIERO DI PROTOCOLLO

Il registro di protocollo è lo strumento attraverso cui è possibile identificare in modo univoco e certo i documenti ricevuti e spediti mediante la registrazione di determinati elementi che caratterizzano ogni singolo documento. Per tale motivo, il registro di protocollo svolge una fondamentale funzione giuridico probatoria, attestando l'esistenza di un determinato documento all'interno del sistema di gestione documentale e garantendone l'autenticità.

Dunque, in coerenza con la normativa vigente, il registro ufficiale di protocollo è unico, sia per la protocollazione in ingresso, che in uscita, che in modalità interna e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo adottato. La numerazione si chiude al 31 dicembre e ricomincia il 1° gennaio successivo. Essa si aggiorna automaticamente e quotidianamente.

Deve essere prodotto automaticamente il registro giornaliero di protocollo costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Esso deve essere inviato automaticamente dal sistema di protocollo, in formato tale da garantirne la non modificabilità. Al fine di garantire la non modificabilità delle operazioni di registrazione, il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione[53].

Si specifica che con riferimento alle protocollazioni effettuate esclusivamente sul Registro ufficiale di protocollo, l'operatore che gestisce lo smistamento dei documenti può definire "riservata" una registrazione di protocollo ed assegnarla per competenza ad un utente assegnatario.

Si ricorda che sono soggetti a protocollazione riservata i seguenti documenti:

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

È possibile impostare una data di scadenza al carattere riservato del documento. Una volta scaduti i termini di riservatezza, il documento diventa visibile a chi è abilitato.

[53] "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID.

5.7. REGISTRO DI EMERGENZA

Nel caso di interruzioni del funzionamento del sistema di protocollo informatico per cause tecniche accidentali o programmate, ai sensi dell'art. 63 del Testo Unico, le registrazioni di protocollo vengono effettuate su un registro di emergenza[54].

Il Responsabile della gestione documentale autorizza con proprio provvedimento la predisposizione del registro di emergenza in forma cartacea oppure in forma digitale e, al ripristino della funzionalità del sistema di protocollo informatico, tutte le registrazioni effettuate vengono inserite a sistema, 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, mantenendo una correlazione con il numero utilizzato in emergenza. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del sistema di protocollo. In questi casi, dovranno essere compilati in ogni loro parte e firmati, i Moduli di Registrazione di Emergenza.

Qualora l'interruzione del funzionamento del sistema di protocollo si prolunghi per più di ventiquattro ore, il Responsabile della gestione documentale, ai sensi della normativa vigente, autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana; in tali casi sul registro di emergenza, oltre alle informazioni di cui sopra, vengono riportati gli estremi del provvedimento di autorizzazione.

5.8. REGISTRI PARTICOLARI

All'interno dell'Istituzione scolastica possono essere istituiti registri particolari che possono essere sottratti alla consultazione da parte di chi non sia espressamente abilitato e per i quali possono essere previste particolari forme di riservatezza e di accesso. Su questi registri vanno di norma caricati solo i documenti informatici o le immagini dei documenti cartacei secondo le istruzioni presenti sul decreto istitutivo del registro particolare.

I documenti che sono soggetti a particolare registrazione dell'Istituzione scolastica e che, ai sensi dell'art. 53, comma 5, del D.P.R. 445/2000, possono essere esclusi dalla protocollazione sono definiti con decreto del Dirigente Scolastico che verrà recepito nelle successive versioni del presente manuale, con indicazione della modalità di gestione dei relativi registri.

Viene data facoltà al Dirigente Scolastico di individuare, eventualmente con Provvedimento che può essere emesso successivamente all'approvazione ed all'adozione del presente Manuale, di individuare

[54] L'art. 63 del D.P.R. 445/2000 prevede che "*1. Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. 2. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. 3. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. 4. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. 5. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza".*

ulteriori tipologie di documenti da assoggettare a registrazione particolare, e le rispettive modalità di gestione.

I registri devono essere gestiti preferibilmente in formato elettronico, e solo in casi eccezionali in formato cartaceo, a seconda delle dotazioni e delle scelte operative di ciascuna istituzione scolastica. In ogni caso (gestione elettronica o cartacea) i registri devono essere gestiti in modo che ne sia garantita l'inalterabilità, l'integrità, la riservatezza e la disponibilità.

Se gestiti in formato elettronico, ai registri devono essere applicate le seguenti misure di sicurezza:

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il

Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Se gestiti in formato elettronico, ai registri devono essere applicate le seguenti misure di sicurezza:

- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

5.9. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

La necessità di modificare anche un solo campo tra quelli obbligatori della registrazione di protocollo registrato 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.

Solo il Responsabile della gestione documentale è autorizzato ad annullare ovvero a dare disposizioni di annullamento delle registrazioni di protocollo. L'annullamento di una registrazione di protocollo deve essere richiesto con specifica e-mail, adeguatamente motivata, indirizzata al Responsabile della gestione documentale che, solo a seguito della valutazione della particolare questione, può autorizzare l'annullamento stesso.

Le informazioni annullate devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura. In tale ipotesi, la procedura per indicare l'annullamento riporta la dicitura "annullato" in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione. Il sistema registra l'avvenuta rettifica, la data e il soggetto che è intervenuto.

Al momento dell'annullamento di una registrazione di protocollo generale l'applicativo richiede la motivazione e gli estremi del provvedimento di annullamento.

5.10. MODALITÀ DI SVOLGIMENTO DEL PROCESSO DI SCANSIONE

Il processo di scansione si articola nelle seguenti fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico *file* in un formato *standard* abilitato alla conservazione;

- verifica della correttezza dell'acquisizione delle immagini e della esatta corrispondenza delle immagini ottenute con gli originali cartacei;
- collegamento delle immagini alla rispettiva registrazione di protocollo, in modo non modificabile;
- memorizzazione delle immagini, in modo non modificabile.

In linea con la certificazione di processo[55], l'operatore di protocollo, a valle del processo di scansione, attesta la conformità del documento scansionato al documento originale.

In breve, la conformità della copia per immagine su supporto informatico di un documento analogico è garantita mediante[56]:

- attestazione di un pubblico ufficiale;
- apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20, comma 1-*bis*, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

L'attestazione di conformità delle copie può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine.

Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

In ogni caso non vengono riprodotti in formato immagine i documenti che per caratteristiche fisiche non possono essere sottoposti a scansione (formati non *standard* o particolarmente voluminosi).

Si precisa che qualora debbano essere protocollati documenti contenenti categorie particolari di dati personali di cui all'art. 9 del Regolamento UE 679/2016, l'operatore di protocollo, dotato delle necessarie abilitazioni, dovrà contrassegnare il documento come contenente dati riservati[57].

6. ACCESSO, TRASPARENZA E PRIVACY

6.1. TUTELA DEI DATI PERSONALI E MISURE DI SICUREZZA

Il sistema di gestione documentale dell'Istituzione scolastica deve adottare un meccanismo di *compliance* e rispetto della normativa in materia di protezione dei dati personali, ai sensi del Reg. UE 679/2016 e del D.Lgs. 196/2003, modificato dal D.Lgs. 101/2018[58], nonché di tutti i Provvedimenti del Garante per la protezione dei dati personali che non siano in contrasto con il GDPR

[55] Si vedano, in merito, gli articoli 22, comma 1-*bis*, e 23-*ter*, comma 1-*bis*, del CAD e l'Allegato 3 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[56] Art. 22 del CAD.
[57] Per ulteriori approfondimenti, si veda il par. "6.1 – Tutela dei dati personali e misure di sicurezza".
[58] "*Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID, stabiliscono che "[…] *il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, in accordo con il responsabile della conservazione di cui al paragrafo 4.6, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR), anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.*".

L'Istituzione scolastica deve intraprendere iniziative volte ad ottemperare a quanto previsto dal Regolamento UE 679/2016, con particolare riferimento:

- al principio di liceità in tutte le operazioni di trattamento dei dati;
- al principio di minimizzazione dei dati[59];
- all'esercizio dei diritti di cui agli artt. 15-22 del GDPR da parte degli interessati;
- alle modalità del trattamento e ai requisiti dei dati;
- alle informative da rendere disponibile agli interessati ed al relativo consenso quando dovuto; si evidenzia comunque che nella maggior parte dei casi, un soggetto pubblico può effettuare tutta una serie di trattamenti senza acquisire il consenso al trattamento dei dati;
- all'analisi dei rischi sui diritti e le libertà dei soggetti interessati;
- all'individuazione del Responsabile della protezione dei dati;
- all'individuazione dei Soggetti autorizzati al trattamento dei dati;
- all'analisi dei rischi sui diritti e le libertà dei soggetti interessati;
- alle misure di sicurezza[60]
- all'obbligo di notificare al Garante per la protezione dei dati personali talune tipologie di violazioni dei dati, entro 72 ore dal momento della conoscenza dell'evento
- all'obbligo di tenuta in ogni caso del registro delle violazioni dei dati e degli incidenti informatici.

Fatto salvo quanto sopra, particolare rilevanza assume il concetto di *accountability* e la capacità di adottare un processo efficace per la protezione dei dati, affinché si riduca al minimo il rischio di una loro possibile violazione.

A tal fine, il Responsabile della gestione documentale, in accordo con il Responsabile della conservazione, con il Responsabile per la transizione digitale, e acquisito il parere del Responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Reg. UE 679/2016, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

Sul punto, il Garante della *privacy* nel Parere sullo schema di "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" del 13 febbraio 2020, ha evidenziato che il mero rinvio alle misure di cui alla circolare AgID del 18 aprile 2017, n. 2/2017, nell'ambito dei requisiti di sicurezza cui sono tenuti i vari soggetti coinvolti nel trattamento, non è di per sé sufficiente ad assicurare l'adozione di misure di sicurezza del trattamento adeguate, in conformità al Regolamento, a norma del quale, occorre invece valutare, in concreto, i rischi che possono derivare, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'Istituzione scolastica è tenuta ad adottare, pertanto, idonee e preventive misure di sicurezza, volte a custodire i dati personali trattati, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della

[59] Art. 5, comma 1, lett. c), del Regolamento UE 679/2016.
[60] Le misure di sicurezza devono "*garantire un livello di sicurezza adeguato al rischio*" del trattamento; in questo senso l'art. 32 par. 1 del Regolamento UE 679/2016 offre una lista aperta e non esaustiva.

raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Nello specifico, le misure di carattere tecnico/organizzativo adottate dall'Istituzione scolastica sono le seguenti:

6.2. MISURE DI SICUREZZA

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Sono inoltre implementate le misure di sicurezza di cui alla Circolare AGID 2/2017, come di seguito riportato:

<< Nome Istituto>>

<< Dati Istituto>>

6.3. MISURE DI SICUREZZA AI SENSI DELLA CIRCOLARE AGID 2/2017

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Come misura di sicurezza preliminare, è stata avviata una attività di ricognizione ed inventariazione delle risorse di tipo hardware e software dell'Istituto, concentrandosi su quelle maggiormente critiche per quantità e tipologia di dati trattati e dei relativi trattamenti di dati effettuati. Le principali tipologie di risorse oggetto di ricognizione sono: - Apparati di tipo server, siano essi fisici o virtuali - Apparati di networking che operano a livello 3 della pila iso/osi (es. router) - Apparati di tipo switch - Apparati di tipo ibrido modem/router per la gestione dell'accesso ad internet in tecnologia adsl/hdsl - Apparati per la protezione perimetrale (firewall) - Apparati / componenti/ sistemi per la gestione del web contenti filtering - Apparati /componenti / sistemi per la gestione dell'autenticazione (es. autenticazione laddove si accede tramite WiFi), del logging e dell'accounting - Apparati di tipo Access Point WiFi - Centralini telefonici

					- Apparati per la rilevazione delle presenze. Come ulteriore misura di sicurezza, di tipo organizzativo, si procederà ad individuare e designare per iscritto il soggetto/i soggetti responsabili della predisposizione dell'inventario e della verifica della sua correttezza, correntezza, completezza, integrità e disponibilità. In una seconda fase si potranno utilizzare strumenti automatizzati per la scansione della rete ed il censimento delle risorse attive, ad esempio utilizzando utility del tipo "ipscan" oppure nmap oppure Zenmap, che permettono di effettuare vali livelli di scansione della rete e di identificazione degli apparati attivi collegati.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Come misura di sicurezza di tipo organizzativo si procederà ad individuare e designare per iscritto il soggetto/i soggetti responsabili della predisposizione dell'inventario e della verifica della sua correttezza, completezza, integrità e disponibilità, nonché del suo tempestivo aggiornamento. Sarà istituito un processo strutturato e tracciabile che prevede tutta una serie di verifiche preliminari che devono essere effettuate prima

					di introdurre una nuova componente hardware o software all'interno del sistema informativo dell'istituto. Le principali verifiche dovranno riguardare i seguenti aspetti: - Conformità al dettato normativo e alla disciplina rilevante in materia di sicurezza e protezione dei dati personali - Conformità a norme, standard, regolamenti e misure di sicurezza che l'Istituto abbia emanato - Verifica degli impatti ambientali, funzionali, organizzativi, prestazionali, e di sicurezza - Risultanze di eventuali test e verifiche effettuati ai ambienti diversi da quello di produzione, laddove questo si riveli essere necessario, economicamente percorribile e tecnicamente fattibile. L'inserimento di nuovi componenti, siano essi di tipo hardware o software, dovrà esplicitamente essere approvato per iscritto da soggetti o tipologie di soggetti che saranno individuate in seguito, tenuto conto di considerazioni di tipo organizzativo, procedurale, economico e di conformità con quanto prescritto dal GDPR – General Data Protection Regulation – Regolamento UE 2016/679 e da eventuali standard internazionali ai quali l'Istituto valuterà l'ipostesi di conformarsi, come ad esempio lo standard ISO/OSI 27001 e 27002. In una seconda fase si potranno utilizzare strumenti automatizzati per la scansione della rete ed il censimento delle risorse attive, ad esempio utilizzando utility del tipo "ipscan" oppure nmap o Zenmap, che permettono di effettuare scansioni con vari livelli di identificazione degli apparati in rete.

1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	In una fase iniziale, la gestione dell'inventario sarà fatta manualmente e saranno registrati gli indirizzi ip assegnati staticamente alle risorse maggiormente critiche, di cui al punto 1.1.1. In una seconda fase si potranno utilizzare strumenti automatizzati per la scansione della rete ed il censimento delle risorse attive, ad esempio utilizzando utility del tipo "ipscan".
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID	Livello	Descrizione	Modalità di implementazione

2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Sarà avviato un processo di ricognizione ed analisi dei trattamenti di dati effettivamente svolti da ciascun profilo di utenza, concentrandosi in primis sull'ambito maggiormente critico ed importante, cioè la segreteria e l'amministrazione. Sulla base delle risultanze del succitato processo di ricognizione, saranno ricavati i fabbisogni informativi in termini di software di sistema, applicativo e di produttività individuale. In primis il vincolo di non installare software non autorizzato sarà gestito in maniera procedurale, mediante comunicazioni, mansionari, lettere di nomina, atti di natura regolamentare, responsabilizzando l'utente finale ed effettuando dei controlli a campioni effettuati nell'ambito di audit periodici del sistema informativo. Laddove tecnicamente fattibile ed economicamente percorribile, considerati i costi e le disponibilità economiche dell'istituto, tenuto conto degli impatti a livello organizzativo e procedurale, se del caso, verrà valutata l'ipotesi di implementare dei meccanismi automatici.
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	

2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Considerato che l'utente medio necessita di un numero estremamente contenuto di software per effettuare i trattamenti di dati e svolgere i compiti affidati, e dovendo l'azione amministrativa essere sempre improntata ai criteri di efficienza, efficacia ed economicità, al momento attuale non si ritiene economicamente conveniente implementare meccanismi automatici per effettuare scansioni automatiche per la rilevazione della presenza di software non autorizzato, che sarebbe di gestione complessa e presenterebbe un notevole impatto a livello di costi. Quanto sopra premesso, la rilevazione di eventuali software non autorizzati verrà effettuata manualmente, nel corso di regolari audit di compliance e sicurezza che dovrebbero comunque venire effettuati, in ottemperanza a quanto previsto del GDPR – Regolamento UE 2016/679 e da consolidati standard e framework di gestione dei sistemi informativi (es. ISACA, COBIT, ISO/IEC 27001, ISO/IEC 27002).
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non	

				devono essere installate in ambienti direttamente collegati in rete.	

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Sarà avviato un processo volto ad individuare, per ciascuna tipologia di sistema operativo, con particolare riferimento ai sistemi operativi di tipo server ed al relativo software di base, configurazioni sicure standard finalizzate al raggiungimento dei seguenti obiettivi: - Eliminazione di account non necessari - Disattivazione od eliminazione di componenti, servizi, processi ed applicazioni non necessarie - Attivazione e configurazione di adeguati meccanismi di accounting e logging, che prevedano come minimo la tracciatura degli accessi e delle operazioni effettuate con profilo di administrator o equivalenti. Le registrazioni (access log) dovranno avere caratteristiche di completezza, inalterabilita' e possibilita' di verifica della loro integrita' adeguate al raggiungimento dello scopo di verifica per cui sono state istituite. Le registrazioni dovranno comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate - Conservazione in sicurezza dei file di log di cui sopra, per un congruo periodo, non inferiore ai sei mesi - Identificazione nominativa individuale univoca dei soggetti che accedono al sistema con profilo di administrator o equivalente, previa valutazione valutazione dell'esperienza, della capacità e dell'affidabilità dei soggetti designati, che

					devono fornite idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, compreso il profilo relativo alla sicurezza.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Tenuto conto che all'interno dell'Istituto operano tipologie di utenti con profili e necessità estremamente diverse (es. personale di segreteria, docenti, studenti, collaboratori esterni), non è possibile individuare un'unica configurazione standard. Lo stesso dicasi per i server ed i sistemi, che hanno caratteristiche, requisiti di sicurezza, architetture operative, funzionali e di esercizio completamente differenti ed eterogenee, per cui non è possibile individuare un'unica configurazione standard. Di volta in volta, sarà implementata la configurazione ritenuta più sicura ad adeguata allo specifico contesto operativo e di utilizzo, tenendo conto anche del progresso tecnologico e dell'evoluzione dell'offerta in termini di sistemi operativi ed architetture di virtualizzazione.

3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Le azioni da intraprendere a seguito di una compromissione di un sistema devono essere valutate con attenzione, tenendo conto almeno dei seguenti fattori: - Tipologia di compromissione - Tipologia, valore, importanza e criticità delle risorse compromesse - Se siano state compromesse risorse di tipo sistema operativo, software di base, middleware transazionale, software applicativo, software di comunicazione, pacchetti di produttività individuale - Se la compromissione sia stata effettuata mediante virus o codici maligni Ad esempio, nel caso la compromissione sia stata effettuata tramite virus o codici maligni, il ripristino potrebbe avvenire in maniera molto semplice mediante la scansione di un buon antivirus o di una utility di disinfezione ad hoc. Nel caso la compromissione abbia riguardato solo i dati, potrebbe essere sufficiente un semplice ripristino dei dati salvati. Tenuto conto di quanto sopra esposto, la gestione della compromissione dei sistemi verrà gestita valutando in primis le soluzioni più semplici, meno costose e meno onerose da mettere in atto, come quelle a titolo esemplificativo esposte in precedenza. La reinstallazione ex-novo di una configurazione standard, ammesso che questa sia stata definita e conservata, deve essere valutata come estrema ratio in quanto estremamente costosa ed onerosa da mettere in atto.

3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Tenuto conto di quanto premesso al punto 3.2.2, sono state date istruzioni organizzative e tecniche ai soggetti interessati, affinché le immagini di installazione siano custodite off-line.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Saranno state date istruzioni organizzative e tecniche ai soggetti interessati, specificando che le operazioni di amministrazione di sistema effettuate da remoto utilizzino connessioni che prevedano la cifratura dei dati trasmessi. In particolare sarà richiesto a tutti i fornitori che le operazioni di amministrazione e gestione di sistema svolte da remoto siano effettuate mediante vpn.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	

3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Il requisito di estendere la ricerca delle vulnerabilità a tutti i sistemi in rete è irragionevole e va contro i principi di efficienza, efficacia ed economicità ai quali l'azione amministrativa si deve sempre ispirare. Posto che talvolta vi possono essere centinaia di sistemi in rete, e che l'effettuazione di una scansione può comportare una spesa, ed ha comunque dei costi, quanto proposto viola palesemente i principi di efficienza, efficacia ed economicità ai quali l'azione amministrativa si deve sempre ispirare. Inoltre, non sempre la ricerca delle vulnerabilità richiede strumenti automatici: talvolta può essere più opportuno utilizzare utility manuali ad hoc, per la ricerca e il remediation di specifiche vulnerabilità (ad esempio su centralino Voip).
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common	

				Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Gli strumenti di scansione delle vulnerabilità che verranno utilizzati (a titolo esemplificativo ma non esaustivo: MBSA – Microsoft Baseline Security Analyzer e Qualys) sono regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Installare automaticamente le patch e gli aggiornamenti dei sistemi operativi è quanto di più pericoloso si possa fare, dal punto di vista della sicurezza, poiché spesso gli aggiornamenti possono causare disservizi, malfunzionamenti, interruzioni del servizio e introdurre essi stessi vulnerabilità o configurazioni poco sicure, per cui l'Istituto si guarderà bene del mettere in atto tale prassi pericolosa.

					Nei limiti del possibile, tenuto conto dei costi e degli impatti, gli aggiornamenti verranno prima testati in un ambiente di test, al fine di accertare il fatto che gli aggiornamenti stessi non introducano disservizi o malfunzionamenti o degradi funzionali o prestazionali. Solo dopo aver superato con esiti positivo il suddetto test, verrà valutata l'ipotesi di applicare gli aggiornamenti nell'ambiente di esercizio.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Concettualmente verrà adottato il medesimo approccio e la stessa metodologia di cui al precedente è punto 4.5.1
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	La metodologia di gestione delle vulnerabilità che sarà adottata prevederà esplicitamente che per ciascuna vulnerabilità emersa sia individuato il soggetto (o i soggetti) incaricato della sua gestione, qualsiasi sia lo strumento di remediation utilizzato. Laddove possibile ed economicamente percorribile sarà implementato un sistema automatizzato di workflow management, che talvolta è compreso nello strumento di vulnerability management. Ad esempio la piattaforma Qualys è dotata di un ottimo strumento di workflow management per assegnare, gestire e tracciare le operazioni di remediation.

4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	La metodologia strutturata di risk assessment e risk management che l'Istituto applicherà, terrà conto, secondo consolidate best practice, di quanto segue: - Minacce - Vulnerabilità - Probabilità di verificarsi dell'evento avverso - Conseguenze all'atto del verificarsi dell'evento avverso - Livello di rischio - Tipologia e valore delle risorse potenzialmente impattate.
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	La metodologia di remediation delle vulnerabilità attribuirà un livello di priorità nell'applicazione delle contromisure che terrà conto di una complessa combinazione di fattori, tra cui tutti quelli citati nel precedente punto 4.8.1
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	E' prevista l'identificazione nominativa individuale univoca dei soggetti che accedono al sistema con profilo di administrator o equivalente, sia interni che esterni all'Ente, previa valutazione valutazione dell'esperienza, della capacità e dell'affidabilità dei soggetti designati, che devono fornite idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, compreso il profilo relativo alla sicurezza.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Sarà avviato un processo volto ad individuare, per ciascuna tipologia di sistema operativo, con particolare riferimento ai E' prevista l'attivazione e configurazione di adeguati meccanismi di accounting e logging, che prevedano come minimo la tracciatura degli accessi e delle operazioni effettuate con profilo di administrator o equivalenti. Le registrazioni (access log) dovranno avere caratteristiche di completezza, inalterabilita' e possibilita' di verifica della loro integrita' adeguate al raggiungimento dello scopo di verifica per cui sono state istituite. Le registrazioni dovranno comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate. Le registrazioni saranno conservate in sicurezza, per un congruo periodo, non inferiore ai sei mesi, e3 l'analisi dei suddetti file di log al fine di individuare eventuali accessi abusivi o indizi di condotte illecite o fraudolente.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	

5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	E' stato avviato un processo strutturato e tracciabile di ricognizione ed inventariazione delle utenze amministrative, con identificazione nominativa individuale dei soggetti che le possono utilizzare. Le prassi messe in atto dall'Istituto prevedono che ciascun soggetto di cui al punto precedente debba essere debitamente e formalmente autorizzato.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	La nomenclatura degli account di administrator o equivalenti sarà tale da permettere l'identificazione nominativa personale univoca dei soggetti che accedono con qualifica di administrator. In caso di dimissioni, licenziamenti, variazioni di ruolo o responsabilità, si procederà a tenere traccia di tali eventi fondamentali e laddove tecnicamente fattibile si procederà alla disattivazione dell'account ed in ogni caso a disattivare la possibilità di accesso remoto al sistema, nel caso gli interventi di amministrazione e gestione di sistema fossero possibili da remoto. In ogni caso, la revisione della sussistenza o meno della qualifica e della titolarità, nonché della necessità e liceità, di utilizzare account di administrator sarà effettuata con frequenza almeno trimestrale e sarà documentata per iscritto.

5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Saranno date istruzioni organizzative e tecniche ai soggetti che agiscono con profilo di administrator o equivalente, di utilizzare per le utenze amministrative password lunghe almeno 14 caratteri. Laddove tecnicamente fattibile, tale vincolo sarà implementato a livello di sistema (accesso al dominio) e di software applicativi installati.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Saranno date istruzioni organizzative e tecniche ai soggetti che agiscono con profilo di administrator o equivalente, di effettuare la modifica delle password con frequenza almeno semestrale. Laddove tecnicamente fattibile, tale vincolo sarà implementato a livello di sistema operativo (accesso al dominio) e di software applicativi.

5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Saranno date istruzioni organizzative e tecniche ai soggetti che agiscono con profilo di administrator o equivalente, di non riutilizzare le password precedenti. Laddove tecnicamente fattibile, tale vincolo sarà implementato a livello di sistema operativo e di software applicativi.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Eventuali casistiche di utilizzo di credenziali privilegiate per l'esecuzione di compiti che richiedono invece utenze non privilegiate, saranno individuate e "bonificate" mediante la creazione e l'assegnazione di credenziali diverse, di profilo diverso da quello di administrator.

5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	E' stato avviato un processo strutturato e tracciabile di ricognizione ed inventariazione delle utenze amministrative, con identificazione nominativa individuale dei soggetti che le possono utilizzare. Le prassi messe in atto dall'Istituto prevedono che ciascun soggetto di cui al punto precedente debba essere debitamente e formalmente autorizzato.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Saranno date istruzioni organizzative e tecniche ai soggetti che accedono con profilo di administrator o equivalente, finalizzate a evidenziare che le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, devono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	E' stato formalmente definito ed assegnato per il ruolo di "custode delle password di sistema" , che dovrà custodire in sicurezza le credenziali amministrative in modo da garantirne disponibilità e riservatezza. Tenuto conto dell'importanza e della delicatezza di tale compito, è stata allo scopo predisposta una apposita procedura operativa.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Nel caso in cui per l'autenticazione vengano utilizzati certificati digitali, saranno impartite istruzioni organizzative e tecniche che prevedono la diligente custodia in sicurezza delle chiavi private.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Su tutti i sistemi connessi alla rete sono installati antivirus aggiornati automaticamente.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Prima di mettere in atto tale misura di sicurezza ne sarà valutata la reale necessità ed efficacia, nonché i costi e gli impatti derivanti.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'uso di dispositivi esterni deve essere formalmente autorizzato per iscritto e l'autorizzazione viene rilasciata solo nel caso di reale necessità per lo svolgimento di funzioni istituzionali.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	

8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Tale vincolo sarà implementato in modalità centralizzata agendo a livello di Group Policy, oppure agendo a livello di singola macchina laddove si tratti di macchine stand-alone o non in dominio.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Tale vincolo sarà implementato in modalità centralizzata agendo a livello di Group Policy, oppure agendo a livello di singola macchina laddove si tratti di macchine stand-alone o non in dominio.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Tale vincolo sarà implementato in modalità centralizzata agendo a livello di Group Policy, oppure agendo a livello di singola macchina laddove si tratti di macchine stand-alone o non in dominio.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Tale vincolo sarà implementato in modalità centralizzata agendo a livello di Group Policy, oppure agendo a livello di singola macchina laddove si tratti di macchine stand-alone o non in dominio.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Tale vincolo sarà implementato in modalità centralizzata agendo a livello di Group Policy, oppure agendo a livello di singola macchina laddove si tratti di macchine stand-alone o non in dominio.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Sarà valutata l'ipotesi di utilizzare pacchetti antispam, tenuto conto dei costi e degli impatti a livello organizzativo e procedurale.

8	9	2	M	Filtrare il contenuto del traffico web.	Sarà predisposto un atto di natura regolamentare volto a disciplinare finalità, modalità e strumenti di web content filtering.
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Tale vincolo sarà implementato a livello centralizzato laddove possibile (es. antivirus o antispam centralizzato) , oppure a livello locale .
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Tutti i dati centralizzati sono salvati con frequenza almeno settimanale. Sarà formalmente individuato un soggetto incaricato dell'esecuzione delle copie di backup, della verifica dell'esito delle stesse, della gestione di eventuali errori od anomalie, nonché della custodia in sicurezza di eventuali supporti rimovibili di memorizzazione .
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima	In primis la riservatezza delle informazioni sarà assicurata mediante adeguata protezione fisica dei supporti, che dovranno essere custoditi in cassaforte, oppure in una cassetta di sicurezza presso

				della trasmissione consente la remotizzazione del backup anche nel cloud.	una banca, oppure in locali ad accesso controllato. Per quanto riguarda il backup in cloud, già attualmente i dati sono cifrati.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Saranno date istruzioni organizzative e tecniche al fine di assicurare che almeno una copia di backup sia memorizzata e permanentemente custodita off-line.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Ai sensi ed in ottemperanza a quanto previsto dall'art. 32 del GDPR, la cifratura dei dati è una (tra le tante) delle possibili misure di sicurezza che possono essere applicate, "tenendo conto dello stato dell'arte e dei costi di attuazione…., se del caso", per cui la cifratura dei dati non è una misura obbligatoria. Va inoltre tenuto in conto il costo e la complessità organizzativa indotta dall'adozione di procedure di cifratura (es. creazione, comunicazione, custodia e disponibilità) delle chiave o dei dispositivi di cifratura. Per cui di volta in volta verrà fatta un'analisi costi/benefici e si valuterà la misura di sicurezza più adeguata per assicurare la riservatezza dei dati.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	

13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	L'utilizzo di blacklist per filtrare il traffico web è una tecnica estremamente grezza e poco efficace, di fatto completamente in disuso, anche tenuto conto del fatto che le blacklist si possono applicare solo laddove vi sia un limitatissimo numero di siti web da autorizzare o da negare. Inoltre, la gestione e l'aggiornamento delle blacklist può rivelarsi talvolta estremamente oneroso da mettere in atto. Verranno valutate tecniche di filtraggio e di web content filtering basate su categorie, tenuto conto dei costi e delle reali necessità. In ogni caso, l'adozione di meccanismi di filtraggio degli url, in quanto tecnicamente potrebbero costituire "interruzione o impedimento di comunicazioni elettroniche", che è un reato penale, dovrà previamente essere autorizzata con atto scritto del Dirigente

					Scolastico o del Consiglio di Istituto e dovrà essere disciplinata da apposito regolamento.
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

<< Nome Istituto>>

<< Dati Istituto>>

6.4. OTTEMPERANZA AL PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI RELATIVO AL CONTROLLO DELL'OPERATO DEGLI AMMINISTRATORI DI SISTEMA

Per garantire l'ottemperanza a quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 27-11-2008 relativo al controllo dell'operato degli amministratori di sistema, deve essere messo in atto quanto segue:

- a livello di software per la gestione del protocollo e dei flussi documentali, deve essere attivato (ed eventualmente configurato) un meccanismo di logging (tracciatura) delle operazioni di amministrazione e gestione di sistema effettuate con profilo di administrator;
- il suddetto file di log non deve essere sovrascritto per un periodo minimo di 12 mesi;
- il suddetto file di log non dovrà essere per nessun motivo modificato o alterato;
- con frequenza al massimo semestrale, si dovrà procedere all'estrazione (copia) del suddetto file di log; sono ammesse modalità di estrazione "continua" dei file di log, ad esempio ogni 5 minuti od ogni 20 minuti;
- la copia estratta del file di log dovrà essere generata in un formato non modificabile (pdf, tiff o altri formati non modificabili) e firmata digitalmente con certificato digitale emesso da una certification authority trusted di primo livello;
- la copia del file di log firmata digitalmente dovrà essere custodita in un luogo sicuro per un periodo di almeno 12 mesi;
- con frequenza semestrale si dovrà controllare l'operato degli amministratori di sistema, mediante analisi dei file di log e del registro delle operazioni di amministrazione e gestione di sistema effettuate sul sistema di videosorveglianza; alla conclusione delle operazioni di controllo / verifica dovrà essere redatto apposito verbale e relazione.

7. DIRITTO DI ACCESSO AGLI ATTI

7.1. ACCESSO DOCUMENTALE

Per diritto di accesso si intende, ai sensi dell'art. 22, comma 1, lett. a), della L. 241/1990, "*il diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi*".

Gli istanti devono essere portatori di un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento amministrativo e ai documenti connessi.

Gli interessati devono effettuare una richiesta di accesso motivata, essendo necessaria una valutazione oggettiva circa la posizione dell'istante per verificare l'esistenza di un nesso di strumentalità rispetto ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso.

Il diritto di accesso è escluso per[61]:

- i documenti coperti dal segreto di Stato;
- i procedimenti tributari;
- l'attività della Pubblica Amministrazione diretta all'emanazione di atti normativi o amministrativi generali;
- i procedimenti selettivi contenenti informazioni di carattere psicoattitudinale.

Il diritto all'accesso ai documenti amministrativi è prioritario rispetto al diritto alla riservatezza in tutti quei casi in cui l'istanza ostensiva sia preordinata alla tutela e alla difesa dei propri interessi giuridici.

L'Istituzione scolastica deve effettuare una valutazione oggettiva circa la posizione dell'istante per verificare l'esistenza di un nesso di strumentalità rispetto ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso, tenendo conto altresì di quanto previsto eventualmente nello specifico regolamento per l'accesso documentale, adottato dalla scuola, in conformità alle previsioni contenute nella delibera ANAC 1309/2016.

Per quanto afferisce ai profili *privacy*, il D.Lgs. 196/2003 all'art. 59, rubricato "*Accesso a documenti amministrativi e accesso civico*" prevede che "*1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.".*

In breve, si rileva che rispetto ai[62]*:*

- *Dati personali:* il diritto all'accesso ai documenti amministrativi può prevalere sull'interesse alla riservatezza, nel rispetto del principio di minimizzazione;
- *Dati cc.dd. sensibili e giudiziari:* il diritto all'accesso prevale solo laddove sia strettamente indispensabile;
- *Dati cc.dd. sensibilissimi (dati genetici e/o idonei a rivelare lo stato di salute e la vita sessuale):* il diritto di accesso prevale esclusivamente se la situazione giuridicamente rilevante che si

[61] Art. 24, L. 241/1990.
62 Art. 24, comma 7, D. Lgs. 241/1990; Art. 59 e 60, D. Lgs. 196/2003.

intende tutelare con la richiesta di accesso ai documenti amministrativi consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

A tal proposito, nella gestione degli accessi e consultazione dei documenti detenuti dall'Istituzione scolastica, da parte di terzi, il Responsabile della gestione è tenuto ad informare in modo costante ed aggiornato il Responsabile della protezione dei dati personali.

In ogni caso, nell'ipotesi di accesso diretto ai propri archivi, l'Amministrazione titolare dei dati, rilascia all'Amministrazione procedente apposita autorizzazione in cui vengono indicati eventuali limiti e condizioni di accesso, volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente anche mediante la stipula di apposite convenzioni di servizio.

Allo stesso modo, nel caso in cui sia effettuata una protocollazione riservata (come indicato nel paragrafo 5.8.), la visibilità completa del documento è possibile solo all'utente assegnatario per competenza e agli operatori di protocollo che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo). Tutti gli altri utenti (seppure inclusi nella giusta lista di competenza) possono accedere solo ai dati di registrazione (ad esempio, progressivo di protocollo, data di protocollazione), mentre sono oscurati i dati relativi al profilo del protocollo (ad esempio, classificazione).

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca *full text*.

7.2. ACCESSO CIVICO GENERALIZZATO (FOIA)

Il diritto all'accesso civico generalizzato (FOIA) riguarda la possibilità di accedere a dati, documenti e informazioni detenuti dalle Pubbliche Amministrazioni ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria previsti dal D.Lgs. 33/2013[63].

Le istanze possono essere presentate da chiunque, a prescindere da particolari requisiti di qualificazione, e senza necessità di motivazione.

L'accesso civico generalizzato è volto a:

- assicurare a chiunque l'accesso indipendentemente dalla titolarità di situazioni giuridiche soggettive;
- promuovere la partecipazione al dibattito pubblico;
- favorire forme diffuse di controllo sul perseguimento delle finalità istituzionali e sull'utilizzo delle risorse pubbliche.

Le Istituzioni scolastiche, al fine di esaminare le istanze, dovrebbero adottare anche adeguate soluzioni organizzative, quali, ad esempio, *"la concentrazione della competenza a decidere sulle richieste di accesso in un unico ufficio (dotato di risorse professionali adeguate, che si specializzano nel tempo, accumulando know how ed esperienza), che, ai fini istruttori, dialoga con gli uffici che detengono i dati richiesti*", come indicato nella Deliberazione ANAC 1309/2016[64].

[63] L'accesso civico generalizzato è previsto dall'art. 5, comma 2, del D.Lgs. 33/2013 e si differenzia dall'accesso civico semplice di cui al comma 1 del medesimo articolo, il quale stabilisce che "*L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione*". Come precedentemente evidenziato, l'istanza di accesso civico, qualora abbia a oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013, è presentata al Responsabile per la prevenzione della corruzione e della trasparenza.

[64] La Deliberazione ANAC n. 1309 del 28 dicembre 2016, recante "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 c. 2 del D.Lgs. 33/2013*" è stata adottata ai sensi dell'art. 5-*bis*, comma 6, del D.Lgs. 33/2013 il quale stabilisce che "*Ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui al presente articolo, l'Autorità nazionale anticorruzione, d'intesa con il Garante per la protezione dei*

Fatto salvo quanto sopra, le scuole destinatarie dell'istanza, devono emettere un provvedimento espresso e motivato nei successivi trenta giorni.

Si rappresenta che l'accesso civico generalizzato è limitato qualora sia pregiudicato un interesse pubblico, ovvero:

- la sicurezza pubblica e l'ordine pubblico;
- la sicurezza nazionale;
- la difesa e le questioni militari;
- le relazioni internazionali;
- la politica e la stabilità finanziaria ed economica dello Stato;
- la conduzione di indagini sui reati e il loro perseguimento;
- il regolare svolgimento di attività ispettive.

L'Istituzione scolastica deve, altresì, effettuare un'attività valutativa con la tecnica del bilanciamento, caso per caso, tra l'interesse pubblico alla *disclosure* generalizzata e la tutela di interessi considerati validi dall'ordinamento. Il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:

- protezione dei dati personali;
- libertà e segretezza della corrispondenza;
- interessi economici e commerciali, inclusi la proprietà intellettuale, il diritto d'autore e i segreti commerciali[65].

Sulle richieste di riesame presentate dai richiedenti ai quali sia stato negato totalmente o parzialmente l'accesso o che non abbiano avuto risposta entro il termine stabilito, il Responsabile per la prevenzione della corruzione e della trasparenza decide con provvedimento motivato, entro il termine di venti giorni.

Qualora l'accesso sia stato negato o differito per esigenze di tutela della protezione dei dati personali, il Responsabile della prevenzione della corruzione e della trasparenza, fatto salvo il confronto con il RPD, deve provvedere, sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta.

Il termine per l'adozione del provvedimento da parte del RPCT è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni[66].

Nei casi di risposta negativa o parzialmente negativa sopra elencati, l'Istituzione scolastica è tenuta, ad ogni modo, a una congrua e completa motivazione.

Specifiche indicazioni e raccomandazioni operative sul FOIA sono contenute nella Circolare del Ministro per la Semplificazione e la Pubblica Amministrazione n. 2/2017 avente ad oggetto "*Attuazione delle norme sull'accesso civico generalizzato (c.d. FOIA)*", in particolare:

- uffici competenti;
- tempi di decisione;
- controinteressati;
- rifiuti non consentiti;
- dialogo con i richiedenti;

dati personali e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta linee guida recanti indicazioni operative".

[65] Si vedano, sul punto, l'art. 5-*bis* del D.Lgs. 33/2013 e la Deliberazione ANAC 1309/2016.

[66] Art. 5, comma 7, del D.Lgs. 33/2013.

- Registro degli accessi.

Il 28 giugno 2019 il Ministero della Pubblica Amministrazione ha adottato, inoltre, la circolare n. 1/2019 allo scopo di fornire alle Pubbliche Amministrazioni "*indirizzi e chiarimenti*" ulteriori rispetto alle "*raccomandazioni operative*" di cui alla circolare n. 2/2017 ed alle Linee Guida dell'ANAC adottate d'intesa con il Garante per la protezione dei dati personali nel 2016. I profili trattati riguardano:

- criteri applicativi di carattere generale;
- regime dei costi;
- notifica ai controinteressati;
- partecipazione dei controinteressati alla fase di riesame;
- termine per proporre l'istanza di riesame;
- strumenti tecnologici di supporto.

7.3. REGISTRO DEGLI ACCESSI

Il registro delle richieste di accesso presentate per tutte le tipologie di accesso è istituito presso l'Istituzione scolastica, in conformità a quanto stabilito dai già citati documenti, ovvero, la Deliberazione ANAC n. 1309/2016, nonché dalla Circolare del Ministro per la Pubblica Amministrazione n. 2/2017, e dalla successiva Circolare del Ministro per la Pubblica Amministrazione n. 1/2019.

Il registro è costituito attraverso la raccolta organizzata delle richieste con l'indicazione dell'oggetto, della data e del relativo esito (con data della decisione), il quale sarà pubblicato sul sito istituzionale dell'Istituzione scolastica con cadenza trimestrale. L'implementazione del registro avviene mediante l'utilizzo del sistema di protocollo informatico e dei flussi documentali di cui è dotata l'Istituzione scolastica ai sensi del D.P.R. n. 445 del 2000, del CAD e delle relative regole tecniche.

ALLEGATI

Allegato 1 – UOR

Alla data di ultimo aggiornamento del presente documento non sono definite UOR.

Allegato 2 – Titolario

Allegato 3 – Massimario di Conservazione e di Scarto per le Istituzioni Scolastiche

Allegato 4 - Metadati

TITOLARIO UNICO DI CLASSIFICAZIONE PER LE ISTITUZIONI SCOLASTICHE

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

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

AGID | Agenzia per l'Italia Digitale

I metadati

Allegato 5 al documento "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

Questo allegato è parte integrante al testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

---

1. Introduzione

Il presente allegato illustra i metadati relativi al documento informatico, al documento amministrativo informatico e all'aggregazione documentale informatica, intendendo, con quest'ultima, sia il fascicolo informatico, che la serie documentale.

Le implementazioni effettuate rispetto all'allegato alla precedente versione delle Linee guida si sono rese necessarie per ottemperare sempre più ai principi di interoperabilità, trasparenza e conoscenza approfondita del contesto documentale.

Il lessico utilizzato permette di astrarsi dal particolare dominio di appartenenza al fine di permettere una piena circolarità degli oggetti digitali e una semplificazione del loro recupero nel tempo.

L'elaborazione degli schemi è stata effettuata tenendo conto anche delle informazioni necessarie in vista della conservazione a lungo termine.

Gli schemi sotto riportati sono organizzati in modo da indicare per ogni metadato:

- **Informazione**: il nome;
- **Sottocampi**: l'eventuale sottostruttura del metadato complesso;
- **Valori ammessi**: valori accettati all'interno del campo;
- **Tipo dato**: numerici o alfanumerici;
- **Obbligatorietà**: l'indicazione di obbligatorietà, eventualmente condizionata;
- **Nuova definizione**: metadati nuovi o ridefiniti rispetto all'allegato alla normativa precedente;
- **Definizione**: indicazione sulla modalità di utilizzo del metadato.

Gli schemi di metadati relativi al documento informatico e al documento amministrativo informatico - se si esclude, per quest'ultimo caso, l'identificativo legato alla segnatura del protocollo - presentano sostanziali analogie strutturali, alle quali, però, corrispondono particolari e determinati controlli di obbligatorietà e codifica.

Sono stati definiti metadati complessi volti a garantire la massima flessibilità in termini di utilizzo.

Esemplificativo di tale intervento, il metadato "*Soggetti*", che consente di tipizzare gli attori che a vario titolo - "*Ruolo*" - concorrono alla definizione del documento informatico, del documento amministrativo informatico o della stessa aggregazione documentale, garantendo la possibilità di indicare molteplici tipologie di soggetti, dalle persone fisiche alle AOO delle Amministrazioni Pubbliche.

L'attività di **indicizzazione, individuazione e ricerca** è significativamente agevolata dalla definizione di metadati legati:

- alla tipologia – "*Tipologia documentale*" o "*Tipologia fascicolo*";
- alla registrazione – "*Dati registrazione*";
- all'Oggetto – "*Chiave descrittiva*";
- alla Classificazione – "*Classificazione*";

Particolarmente rilevante è il metadato complesso "*Assegnazione*" dell'aggregazione documentale informatica. Tale metadato, strutturato in vari sottocampi opportunamente valorizzati, consente di tracciare ogni passaggio dell'aggregazione per competenza o per conoscenza, al fine di garantire la massima trasparenza nell'ambito di qualsiasi procedimento amministrativo della PA.

2. METADATI DEL DOCUMENTO INFORMATICO

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
IdDoc					NO, ma ridefinito
	Impronta	Rappresenta l'hash del documento	Binary	SI	
	Algoritmo	Rappresenta l'algoritmo applicato Default = SHA-256	Alfanumerico	SI	
	Identificativo	Come da sistema di identificazione formalmente definito	Alfanumerico	SI	

Definizione

Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione.
Inoltre, rappresenta le informazioni necessarie per verificare l'integrità del documento.
L'impronta è generata impiegando la funzione di hash, come da definizione nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento".
Il metadato è costituito dai sottocampi:

- *Impronta: sottocampo in cui viene memorizzato l'hash del documento*
- *Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"*
- *Identificativo: come da sistema di identificazione formalmente definito*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Modalità di formazione		Indicare: • *creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;* • *acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;* • *memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;*	Alfanumerico	SI	SI

		• *generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.*			

Definizione

Indica la modalità di generazione del documento informatico.

Sono previste le seguenti modalità secondo quanto riportato nelle Linee guida:

a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipologia documentale		• Fatture • Determine • Delibere	Alfanumerico	SI	SI
Definizione					
Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Dati di registrazione					
	Tipologia di flusso	• In uscita • In entrata • Interno	Alfanumerico	SI	SI
	Tipo registro	• Nessuno, • Protocollo Ordinario/ Protocollo Emergenza • Repertorio/Registro	Alfanumerico	SI	SI
	Data registrazione	nel caso di documento non protocollato: • Data di registrazione del documento nel caso di documento protocollato: • Data di registrazione di protocollo	Datatime	SI	NO, ma ridefinito

	Numero Documento	nel caso di documento non protocollato: • Numero di registrazione del documento nel caso di documento protocollato: • Numero di protocollo	Alfanumerico	SI	SI
	IdRegistro	Codice identificativo del registro in cui il documento viene registrato.	Alfanumerico	SI, nel caso di documento registrato	SI
Definizione					
Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato. Si intende per registrazione l'operazione che, in senso lato, associa ad un documento una data e un numero. In tale ottica quindi potrebbe non essere identificabile uno specifico registro, ma sono sempre identificabili una data di registrazione e un numero di registrazione del documento. *Sono previsti i seguenti sottocampi:* • *Tipologia di flusso: indica se si tratta di un documento in uscita, in entrata o interno.* • *Tipo registro: indica il sistema di registrazione adottato: protocollo ordinario/ protocollo emergenza, o Repertorio/Registro.* • *Data: è la data associata al documento all'atto della registrazione* • *Numero documento: Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato.* • *IdRegistro: Identificativo del registro in cui il documento viene registrato.*				

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Chiave descrittiva					
	Oggetto	Testo libero	Alfanumerico	SI	SI

	Parole chiave	Testo libero	Alfanumerico	NO	SI

Definizione

Metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura. È costituito da seguenti sottocampi:

- *Oggetto: testo libero;*
- *Parole Chiave: da compilare facoltativamente attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca del documento. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Soggetti					
	Ruolo	• Autore • Mittente • Destinatario • Assegnatario • Operatore • Altro	Alfanumerico	SI, e nel caso di documento protocollato è obbligatorio indicare almeno il Mittente e il Destinatario	NO, ma ridefinita
	Tipo soggetto	• PF per Persona Fisica • PG per Organizzazione • PA per le Amministrazioni Pubbliche	Alfanumerico	SI	SI

	Nominativo	Nominativo: se Tipo soggetto = PF: ✓ cognome e nome; se Tipo soggetto = PG: ✓ denominazione se Tipo soggetto = PA: ✓ denominazione Amministrazione \ denominazioneAOO;	Alfanumerico	SI	SI
	Codice	Codice identificativo: se Tipo soggetto = PF ✓ codice fiscale se Tipo soggetto = PG: ✓ codice fiscale; se Tipo soggetto = PA: ✓ Codice IPA dell'Amministrazione \ Codice AOO	Alfanumerico	SI	SI
	UOR	Unità Organizzativa di riferimento	Alfanumerico	NO	SI
Definizione					

Indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo. Sono definiti quindi i seguenti attributi:

- *Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Obbligatorio indicare almeno l'autore o il mittente. In particolare, per "Operatore" si intende il soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato "Verifica modifica documento"*
- *Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche*
- *Nominativo: valorizzato a seconda del tipo soggetto.*
- *Codice: valorizzato a seconda del tipo soggetto.*
- *UOR: Unità Organizzativa di riferimento. Non obbligatorio Il metadato ha una struttura ricorsiva.*

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Allegati						
	Numero allegati		0:n	Number	SI	SI
	Indice allegati		Da indicare per ogni allegato se Numero allegati > 0			
		IdDoc	Identificativo del documento relativo all'allegato		SI, se numero allegati > 0	SI
		Descrizione	Testo libero	Alfanumerico	SI, se numero allegati > 0	SI

Definizione

Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- *IdDoc: Identificativo del documento relativo all'allegato*
- *Descrizione: Titolo dell'Allegato*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Classificazione		*sia nel caso di documento protocollato che nel caso di documento non protocollato*			
	Indice di classificazione	Codifica del documento secondo il Piano di classificazione utilizzato	Alfanumerico	NO	SI
	Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico	NO	SI
	Piano di classificazione	URI del Piano di classificazione pubblicato	Alfanumerico	NO	SI
Definizione					
Classificazione del documento secondo il Piano di classificazione utilizzato: • *Indice di classificazione:* *Codifica del documento secondo il Piano di classificazione utilizzato* • *Descrizione:* *Descrizione per esteso dell'Indice di classificazione indicato.* • *Piano di classificazione:* *se presente, riportare eventualmente l'URI di pubblicazione del Piano di classificazione*					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Riservato		• Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato	Boolean	SI	SI
Definizione					
Rappresenta il livello di sicurezza di accesso al documento: • *Vero: se il documento è considerato riservato* • *Falso: se il documento non è considerato riservato.* *Consente di gestire gli accessi al documento al solo personale autorizzato.*					

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Identificativo del formato						
	Formato		Previsti dall'Allegato 2 delle Linee Guida	Alfanumerico	SI	SI
	Prodotto software		Prodotto software utilizzato per la creazione del documento e relativa versione	Alfanumerico	SI, quando rilevabile	SI
		Nome prodotto		Alfanumerico		SI
		Versione prodotto		Alfanumerico		SI
		Produttore		Alfanumerico		SI

Definizione

Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso. É costituito dai seguenti sottocampi:

- *Formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida.*
- *Prodotto software: Prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:*
  - *Nome prodotto*
  - *Versione prodotto*
  - *Produttore*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione

Verifica					
	Firmato Digitalmente	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Sigillato Elettronicamente	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Marcatura Temporale	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Conformità copie immagine su supporto informatico	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = b	SI
Definizione					
Check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
IdAgg		Identificativo del fascicolo o della serie *come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE.*	Alfanumerico	NO	SI

Definizione
Identificativo univoco dell'Aggregazione come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE. Metadato ricorsivo.

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
IdIdentificativoDocumentoPrincipale		IdDoc del documento principale		SI, nel caso in cui sia presente un documento principale	SI

Definizione
Identificativo univoco e persistente del Documento principale

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Versione del documento		1,2,3….	Alfanumerico	SI	SI

Definizione
Versione del documento.

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tracciature modifiche documento					
	Tipo modifica	• Annullamento • Rettifica • Integrazione • Annotazione	Alfanumerico	Si, nel caso di versione > 1 o in caso di annullamento	SI
	Codice fiscale dell'autore della modifica	Codice fiscale del soggetto definito con ruolo Operatore nel metadato "Soggetti"	Alfanumerico	Si, nel caso di versione > 1 o in caso di annullamento	SI
	Data Modifica		Datatime	Si, nel caso di versione > 1 o in caso di annullamento	SI
	IdDoc versione precedente	Identificativo documento versione precedente		Si, nel caso di versione > 1 o in caso di annullamento	SI
Definizione					
Metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore"					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tempo di conservazione		• 9999 • 5 anni • 10 anni • ……..	Numerico	NO	SI

Definizione
Tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente".

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Note		Testo Libero	Alfanumerico	NO	SI
Definizione					
Eventuali indicazioni aggiuntive					

2.1 XSD METADATI DEL DOCUMENTO INFORMATICO

Schema xsd:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

	<xs:element name="DocumentoInformatico">
		<xs:complexType>
			<xs:sequence>
				<xs:element name="IdDoc">
					<xs:complexType>
						<xs:sequence>
							<xs:element name="Impronta" Type="xs:base64Binary" />
							<xs:element name="Algoritmo" Type="xs:string" default="SHA-256"/>
							<xs:element name="Identificativo" Type="xs:string" />
						</xs:sequence>
					</xs:complexType>
				</xs:element>
				<xs:element name="ModalitaDiFormazione">
					<xs:simpleType>
						<xs:restriction base="xs:string">
							<xs:enumeration value="creazione tramite utilizzo di strumenti software che assicurino la
produzione di documenti nei formati previsti in allegato 2"/>
							<xs:enumeration value="acquisizione di un documento informatico per via telematica o su
supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico"/>
							<xs:enumeration value="memorizzazione su supporto informatico in formato digitale delle
informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili ad utente"/>
							<xs:enumeration value="generazione o raggruppamento anche in via automatica di un insieme di
dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma
statica"/>
						</xs:restriction>
					</xs:simpleType>
				</xs:element>
				<xs:element name="TipologiaDocumentale" Type="xs:string" />
```

```
                    <xs:element name="DatiDiRegistrazione">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="TipologiaDiFlusso">
                                    <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                            <xs:enumeration value="In entrata"/>
                                            <xs:enumeration value="In uscita"/>
                                            <xs:enumeration value="Interno"/>
                                        </xs:restriction>
                                    </xs:simpleType>
                                </xs:element>
                                <xs:element name="TipoRegistro">
                                    <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                            <xs:enumeration value="Nessuno"/>
                                            <xs:enumeration value="Protocollo Ordinario/Protocollo
Emergenza"/>
                                            <xs:enumeration value="Repertorio/Registro"/>
                                        </xs:restriction>
                                    </xs:simpleType>
                                </xs:element>
                                <xs:element name="DataRegistrazione" Type="xs:dateTime"/>
                                <xs:element name="NumeroDocumento" Type="xs:string" />
                                <xs:element name="IdRegistro" Type="xs:string" minOccurs="0" />
                            </xs:sequence>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="ChiaveDescrittiva">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="Oggetto" Type="xs:string" />
                                <xs:element name="ParoleChiave" Type="xs:string" minOccurs="0" maxOccurs="5" />
                            </xs:sequence>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="Soggetti" minOccurs="1" maxOccurs="unbounded"  >
                        <xs:complexType>
                            <xs:sequence>
```

```
                                        <xs:element name="Ruolo">
                                                <xs:simpleType>
                                                        <xs:restriction base="xs:string">
                                                                <xs:enumeration value="Autore"/>
                                                                <xs:enumeration value="Mittente"/>
                                                                <xs:enumeration value="Destinatario"/>
                                                                <xs:enumeration value="Assegnatario"/>
                                                                <xs:enumeration value="Operatore"/>
                                                                <xs:enumeration value="Altro"/>
                                                        </xs:restriction>
                                                </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="TipoSoggetto">
                                                <xs:simpleType>
                                                        <xs:restriction base="xs:string">
                                                                <xs:enumeration value="PF"/>
                                                                <xs:enumeration value="PG"/>
                                                                <xs:enumeration value="PA"/>
                                                        </xs:restriction>
                                                </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="Nominativo" Type="xs:string" />
                                        <xs:element name="Codice" Type="xs:string" />
                                        <xs:element name="UOR" Type="xs:string" minOccurs="0" />
                                </xs:sequence>
                        </xs:complexType>
                </xs:element>
                <xs:element name="Allegati">
                        <xs:complexType>
                                <xs:sequence>
                                        <xs:element name="NumeroAllegati" >
                                                <xs:simpleType>
                                                        <xs:restriction base="xs:integer">
                                                                <xs:minInclusive value="0"/>
                                                                <xs:maxInclusive value="999"/>
                                                        </xs:restriction>
                                                </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="IndiceAllegati" minOccurs="0" maxOccurs="unbounded">
```

```
                                                                                <xs:complexType>
                                                                                        <xs:sequence>
                                                                                                <xs:element name="IdDoc">
                                                                                                        <xs:complexType>
                                                                                                                <xs:sequence>
                                                                                                                        <xs:element
name="Impronta" Type="xs:base64Binary" />
                                                                                                                        <xs:element
name="Algoritmo" Type="xs:string" default="SHA-256"/>
                                                                                                                        <xs:element
name="Identificativo" Type="xs:string" />
                                                                                                                </xs:sequence>
                                                                                                        </xs:complexType>
                                                                                                </xs:element>
                                                                                                <xs:element name="Descrizione" Type="xs:string" />
                                                                                        </xs:sequence>
                                                                                </xs:complexType>
                                                                        </xs:element>
                                                                </xs:sequence>
                                                        </xs:complexType>
                                                </xs:element>
                                                <xs:element name="Classificazione" minOccurs="0">
                                                        <xs:complexType>
                                                                <xs:sequence>
                                                                        <xs:element name="IndiceDiClassificazione" Type="xs:string" />
                                                                        <xs:element name="Descrizione" Type="xs:string" />
                                                                        <xs:element name="PianoDiClassificazione" Type="xs:string" minOccurs="0" />
                                                                </xs:sequence>
                                                        </xs:complexType>
                                                </xs:element>
                                                <xs:element name="Riservato" Type="xs:boolean" />
                                                <xs:element name="IdentificativoDelFormato">
                                                        <xs:complexType>
                                                                <xs:sequence>
                                                                        <xs:element name="Formato" Type="xs:string" />
                                                                        <xs:element name="ProdottoSoftware" minOccurs="0">
                                                                                <xs:complexType>
                                                                                        <xs:sequence>
```

```
                                                                        <xs:element name="NomeProdotto" Type="xs:string"
minOccurs="0" />
                                                                        <xs:element name="VersioneProdotto" Type="xs:string"
minOccurs="0" />
                                                                        <xs:element name="Produttore" Type="xs:string"
minOccurs="0" />
                                                                                </xs:sequence>
                                                                        </xs:complexType>
                                                                </xs:element>
                                                        </xs:sequence>
                                                </xs:complexType>
                                        </xs:element>
                                        <xs:element name="Verifica" minOccurs="0">
                                                <xs:complexType>
                                                        <xs:sequence>
                                                                <xs:element name="FirmatoDigitalmente" Type="xs:boolean" />
                                                                <xs:element name="SigillatoElettronicamente" Type="xs:boolean" />
                                                                <xs:element name="MarcaturaTemporale" Type="xs:boolean" />
                                                                <xs:element name="ConformitaCopieImmagineSuSupportoInformatico" Type="xs:boolean" />
                                                        </xs:sequence>
                                                </xs:complexType>
                                        </xs:element>
                                        <xs:element name="IdAgg" minOccurs="0" maxOccurs="unbounded">
                                                <xs:complexType>
                                                        <xs:sequence>
                                                                <xs:element name="TipoAggregazione">
                                                                        <xs:simpleType>
                                                                                <xs:restriction base="xs:string">
                                                                                        <xs:enumeration value="Fascicolo"/>
                                                                                        <xs:enumeration value="Serie Documentale"/>
                                                                                        <xs:enumeration value="Serie Di Fascicoli"/>
                                                                                </xs:restriction>
                                                                        </xs:simpleType>
                                                                </xs:element>
                                                                <xs:element name="IdAggregazione" Type="xs:string" />
                                                        </xs:sequence>
                                                </xs:complexType>
                                        </xs:element>
                                        <xs:element name="IdIdentificativoDocumentoPrincipale" minOccurs="0">
```

```
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element name="Impronta" Type="xs:base64Binary" />
                                                        <xs:element name="Algoritmo" Type="xs:string" default="SHA-256"/>
                                                        <xs:element name="Identificativo" Type="xs:string" />
                                                </xs:sequence>
                                        </xs:complexType>
                                </xs:element>
                                <xs:element name="VersioneDelDocumento" Type="xs:string" />
                                <xs:element name="TracciatureModificheDocumento" minOccurs="0" >
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element name="TipoModifica">
                                                                <xs:simpleType>
                                                                        <xs:restriction base="xs:string">
                                                                                <xs:enumeration value="Annullamento"/>
                                                                                <xs:enumeration value="Rettifica"/>
                                                                                <xs:enumeration value="Integrazione"/>
                                                                                <xs:enumeration value="Annotazione"/>
                                                                        </xs:restriction>
                                                                </xs:simpleType>
                                                        </xs:element>
                                                        <xs:element name="CodiceFiscaleAutoreDellaModifica">
                                                                <xs:simpleType>
                                                                        <xs:restriction base="xs:string" >
                                                                                <xs:pattern value="[A-Z]{6}[0-
9LMNPQRSTUV]{2}[ABCDEHLMPRST][0-9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{3}[A-Z]"/>
                                                                        </xs:restriction>
                                                                </xs:simpleType>
                                                        </xs:element>
                                                        <xs:element name="DataModifica" Type="xs:dateTime"/>
                                                        <xs:element name="IdDocVersionePrecedente">
                                                                <xs:complexType>
                                                                        <xs:sequence>
                                                                                <xs:element name="Impronta" Type="xs:base64Binary" />
                                                                                <xs:element name="Algoritmo" Type="xs:string"
default="SHA-256"/>
                                                                                <xs:element name="Identificativo" Type="xs:string" />
                                                                        </xs:sequence>
```

```
                                                                    </xs:complexType>
                                                                </xs:element>
                                                            </xs:sequence>
                                                        </xs:complexType>
                                                    </xs:element>
                                                    <xs:element name="TempoDiConservazione" minOccurs="0">
                                                        <xs:simpleType>
                                                            <xs:restriction base="xs:integer">
                                                                <xs:minInclusive value="1"/>
                                                                <xs:maxInclusive value="9999"/>
                                                            </xs:restriction>
                                                        </xs:simpleType>
                                                    </xs:element>
                                                    <xs:element name="Note" Type="xs:string" minOccurs="0" />
                                                </xs:sequence>
                                            </xs:complexType>
                                        </xs:element>
</xs:schema>
```

3. METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
IdDoc						
	Impronta crittografica del documento					
		Impronta	Rappresenta l'hash del documento	Binary	SI	NO, ridefinito.
		Algoritmo	Rappresenta l'algoritmo applicato Default = SHA-256	Alfanumerico	SI	SI
	Segnatura		Segnatura del protocollo	Alfanumerico	SI, nel caso di documento protocollato	
	Identificativo		Come da sistema di identificazione formalmente definito	Alfanumerico	SI	
Definizione						

Identificativo univoco e persistente associato in modo univoco e permanente al documento amministrativo informatico in modo da consentirne l'identificazione.
Inoltre, rappresenta le informazioni necessarie per verificare l'integrità del documento. Il metadato è costituito dai sottocampi:

- *Impronta crittografica del documento: a sua volta suddiviso in:*
  - *Impronta: sottocampo in cui viene memorizzato l'hash del documento*
  - *Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato secondo quanto riportato nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"*
- *Segnatura: segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida*
- *Identificativo: come da sistema di identificazione formalmente definito*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Modalità di formazione		Indicare • *creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee;* • *acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione*	Alfanumerico	SI	SI

		della copia informatica di un documento analogico; • *memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;* • *generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica*			
Definizione					

Indica la modalità di generazione del documento informatico.
Sono previste le seguenti modalità, secondo quanto riportato nelle Linee guida:

- *a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;*
- *b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;*
- *c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;*
- *d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipologia documentale		• Fatture • Determine • Delibere …	Alfanumerico	SI	SI
Definizione					
Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Dati di registrazione					

	Tipologia di flusso	• In uscita • In entrata • Interno Per documenti interni si intende i documenti scambiati all'interno della medesima AOO	Alfanumerico	SI	SI
	Tipo registro	• Protocollo Ordinario/ Protocollo Emergenza, • Repertorio/Registro	Alfanumerico	SI	SI
	Data registrazione	nel caso di documento non protocollato: • Data di registrazione del documento nel caso di documento protocollato: • Data di registrazione di protocollo.	Datatime	SI	NO, ma ridefinito

	Numero Documento		nel caso di documento non protocollato: • Numero di registrazione del documento nel caso di documento protocollato: • Numero di protocollo	Alfanumerico	SI	NO, ma ridefinito
	IdRegistro		Codice identificativo del registro in cui il documento viene registrato.	Alfanumerico	SI	SI
	Amministrazione che effettua la registrazione					
		Codice IPA Amministrazione		Alfanumerico	SI	NO, ma ridefinito
		Codice IPA AOO		Alfanumerico	SI	NO, ma ridefinito
Definizione						

Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato.

Sono previsti i seguenti sottocampi:

- *Tipologia di flusso: indica se si tratta di un documento in uscita, in entrata o interno. Per documento interno si intende un documento scambiato tra le diverse UOR afferenti alla stessa AOO*
- *Tipo registro: indica il sistema di registrazione adottato: protocollo ordinario/ protocollo emergenza, o Repertorio/Registro.*
- *Data: è la data associata al documento all'atto della registrazione*
- *Numero documento: Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato.*
- *IdRegistro: Identificativo del registro in cui il documento viene registrato.*
- *Amministrazione che effettua la registrazione: codice IPA dell'Amministrazione e dell'AOO che sta effettuando la registrazione*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Chiave descrittiva					
	Oggetto	Testo libero	Alfanumerico	SI	SI
	Parole chiave	Testo libero	Alfanumerico	NO	SI

Definizione

Metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura. È costituito da seguenti sottocampi:

- *Oggetto: testo libero;*
- *Parole Chiave: da compilare facoltativamente attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca del documento. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione

Soggetti					
	Ruolo	• Autore • Mittente • Destinatario • Assegnatario • Operatore • RUP	Alfanumerico	SI, e nel caso di documento protocollato è obbligatorio indicare almeno il Mittente e il Destinatario	SI
	Tipo soggetto	• PF per Persona Fisica • PG per Organizzazione • PA per le Amministrazioni Pubbliche	Alfanumerico	SI	SI
	Nominativo	Nominativo: se Tipo soggetto = PF: ✓ cognome e nome; se Tipo soggetto = PG: ✓ denominazione se Tipo soggetto = PA: ✓ denominazione Amministrazione \ denominazioneAOO;	Alfanumerico	SI	SI

	Codice	Codice identificativo: se Tipo soggetto = PF: ✓ codice fiscale se Tipo soggetto = PG: ✓ codice fiscale se Tipo soggetto = PA: ✓ Codice IPA dell'Amministrazione \ Codice AOO	Alfanumerico	SI	SI
	UOR	Unità Organizzativa di riferimento	Alfanumerico	Obbligatorio nel caso si stia indicando Ruolo = RUP	SI
	Indirizzi digitali di riferimento	Posta elettronica certificata – domicilio digitale	Alfanumerico	SI	SI
Definizione					

Indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo.
Sono definiti quindi i seguenti attributi:

- *Ruolo: consente di indicare, a seconda delle necessità, il l'autore del documento, il mittente, il destinatario e assegnatario. In particolare, per "Operatore" si intende il soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato "Verifica modifica documento"*
- *Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche o responsabile unico del procedimento.*
- *Nominativo: valorizzato a seconda del tipo soggetto*
- *Codice: valorizzato a seconda del tipo soggetto.*
- *UOR: Unità Organizzativa di riferimento. Obbligatorio nel caso si stia indicando il RUP*
- *Indirizzi digitali di riferimento: valorizzato con il recapito associato al soggetto. Il metadato ha una struttura ricorsiva.*

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Allegati						
	Numero allegati		0:n	Numerico	SI	SI
	Indice allegati		Da indicare per ogni allegato se Numero allegati > 0			
		IdDoc	Identificativo del documento relativo all'allegato		SI, se numero allegati > 0	SI
		Descrizione	Testo libero	Alfanumerico	SI, se numero allegati > 0	SI
Definizione						
Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati: • *IdDoc: Identificativo del documento relativo all'allegato* • *Descrizione: Titolo dell'allegato*						

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Classificazione		*sia nel caso di documento protocollato che nel caso di documento non protocollato*			
	Indice di classificazione	Codifica del documento secondo il Piano di classificazione utilizzato	Alfanumerico	SI	SI
	Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico	SI	SI
	Piano di classificazione	URI del Piano di classificazione pubblicato	Alfanumerico	SI	SI

Definizione

Classificazione del documento secondo il Titolario utilizzato:

- *Indice di classificazione: Codifica del documento secondo il Piano di classificazione utilizzato*
- *Descrizione: Descrizione per esteso dell'Indice di classificazione indicato.*
- *Piano di classificazione: riportare l'URI di pubblicazione del Piano di classificazione*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Riservato		• Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato	Boolean	SI	SI

Definizione

Rappresenta il livello di sicurezza di accesso al documento:

- *Vero: se il documento è considerato riservato*
- *Falso: se il documento non è considerato riservato*

Consente di gestire gli accessi al documento al solo personale autorizzato.

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Identificativo del formato						
	Formato		Previsti dall'Allegato 2 delle Linee guida	Alfanumerico	SI	SI
	Prodotto software		Prodotto software utilizzato per la creazione del documento e relativa versione	Alfanumerico	SI, quando rilevabile	SI
		Nome prodotto		Alfanumerico		SI
		Versione prodotto		Alfanumerico		SI
		Produttore		Alfanumerico		SI

Definizione

Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso. É costituito dai seguenti sottocampi:

- *Formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida.*
- *Prodotto software: Prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:*
  - *Nome prodotto*
  - *Versione prodotto*
  - *Produttore*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Verifica					

	Firmato Digitalmente	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Sigillato Elettronicamente	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Marcatura Temporale	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Conformità copie immagine su supporto informatico	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = b	SI

Definizione
Check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione

IdAgg		Identificativo del fascicolo o della serie *come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE.*	Alfanumerico	SI	SI
Definizione					
Identificativo univoco dell'Aggregazione come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE. Metadato ricorsivo.					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
IdIdentificativoDocumentoPrincipale		IdDoc del documento principale		SI, nel caso in cui sia presente un documento principale	SI
Definizione					
Identificativo univoco e persistente del Documento principale					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Versione del documento		1,2,3….	Alfanumerico	SI	SI
Definizione					
Versione del documento					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tracciature modifiche documento					
	Tipo modifica	• Annullamento • Rettifica • Integrazione • Annotazione	Alfanumerico	Si, nel caso di versione > 1 o in caso di annullamento	SI
	Codice fiscale dell'autore della modifica	Codice fiscale del soggetto definito con ruolo Operatore nel metadato "Soggetti"	Alfanumerico	Si, nel caso di versione > 1 o in caso di annullamento	Si
	Data modifica		Datatime	Si, nel caso di versione > 1 o in caso di annullamento	SI
	IdDoc versione precedente	Identificativo documento versione precedente		Si, nel caso di versione > 1 o in caso di annullamento	SI
Definizione					
Metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore"					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tempo di conservazione		• 9999 • 5 anni • 10 anni • …….	Numerico	NO	SI

Definizione
Tempo di conservazione del documento desunto dal Piano di conservazione formalmente integrato al Piano di classificazione o prescritto dalla normativa salvo contenzioso. In generale il *tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente".*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Note		Testo Libero	Alfanumerico	NO	SI
Definizione					
Eventuali indicazioni aggiuntive utili ad indicare situazioni particolari.					

3.1 XSD METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO

Schema xsd:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
	<xs:element name="DocumentoAmministrativoInformatico">
		<xs:complexType>
			<xs:sequence>
				<xs:element name="IdDoc">
					<xs:complexType>
						<xs:sequence>
							<xs:element name="ImprontaCrittograficaDelDocumento">
								<xs:complexType>
```

```
                                                                                <xs:sequence>
                                                                                        <xs:element name="Impronta" Type="xs:base64Binary" />
                                                                                        <xs:element name="Algoritmo" Type="xs:string"
default="SHA-256"/>
                                                                                </xs:sequence>
                                                                        </xs:complexType>
                                                                </xs:element>
                                                                <xs:element name="Segnatura" Type="xs:string" minOccurs="0" />
                                                                <xs:element name="Identificativo" Type="xs:string" />
                                                        </xs:sequence>
                                                </xs:complexType>
                                        </xs:element>
                                        <xs:element name="ModalitaDiFormazione">
                                                <xs:simpleType>
                                                        <xs:restriction base="xs:string">
                                                                <xs:enumeration value="creazione tramite utilizzo di strumenti software che assicurino la
produzione di documenti nei formati previsti in allegato 2"/>
                                                                <xs:enumeration value="acquisizione di un documento informatico per via telematica o su
supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico"/>
                                                                <xs:enumeration value="memorizzazione su supporto informatico in formato digitale delle
informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili ad utente"/>
                                                                <xs:enumeration value="generazione o raggruppamento anche in via automatica di un insieme di
dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma
statica"/>
                                                        </xs:restriction>
                                                </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="TipologiaDocumentale" Type="xs:string" />
                                        <xs:element name="DatiDiRegistrazione">
                                                <xs:complexType>
                                                        <xs:sequence>
                                                                <xs:element name="TipologiaDiFlusso">
                                                                        <xs:simpleType>
                                                                                <xs:restriction base="xs:string">
                                                                                        <xs:enumeration value="In entrata"/>
                                                                                        <xs:enumeration value="In uscita"/>
                                                                                        <xs:enumeration value="Interno"/>
                                                                                </xs:restriction>
                                                                        </xs:simpleType>
```

```
                                                </xs:element>
                                                <xs:element name="TipoRegistro">
                                                        <xs:simpleType>
                                                                <xs:restriction base="xs:string">
                                                                        <xs:enumeration value="Protocollo Ordinario/Protocollo
Emergenza"/>
                                                                        <xs:enumeration value="Repertorio/Registro"/>
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                                <xs:element name="DataRegistrazione" Type="xs:dateTime"/>
                                                <xs:element name="NumeroDocumento" Type="xs:string" />
                                                <xs:element name="IdRegistro" Type="xs:string" />
                                                <xs:element name="AmministrazioneCheEffettuaRegistrazione">
                                                        <xs:complexType>
                                                                <xs:sequence>
                                                                        <xs:element name="CodiceIPAAmministrazione"
Type="xs:string" />
                                                                        <xs:element name="CodiceIPAAOO" Type="xs:string" />
                                                                </xs:sequence>
                                                        </xs:complexType>
                                                </xs:element>
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="ChiaveDescrittiva">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="Oggetto" Type="xs:string" />
                                                <xs:element name="ParoleChiave" Type="xs:string" minOccurs="0" maxOccurs="5" />
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="Soggetti" minOccurs="1" maxOccurs="unbounded"  >
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="Ruolo">
                                                        <xs:simpleType>
                                                                <xs:restriction base="xs:string">
```

```
                                                                <xs:enumeration value="Autore"/>
                                                                <xs:enumeration value="Mittente"/>
                                                                <xs:enumeration value="Destinatario"/>
                                                                <xs:enumeration value="Assegnatario"/>
                                                                <xs:enumeration value="Operatore"/>
                                                                <xs:enumeration value="RUP"/>
                                                        </xs:restriction>
                                                </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="TipoSoggetto">
                                                <xs:simpleType>
                                                        <xs:restriction base="xs:string">
                                                                <xs:enumeration value="PF"/>
                                                                <xs:enumeration value="PG"/>
                                                                <xs:enumeration value="PA"/>
                                                        </xs:restriction>
                                                </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="Nominativo" Type="xs:string" />
                                        <xs:element name="Codice" Type="xs:string" />
                                        <xs:element name="UOR" Type="xs:string" minOccurs="0" />
                                        <xs:element name="IndirizziDigitaliDiRiferimento" Type="xs:string" minOccurs="1"
maxOccurs="unbounded"/>
                                </xs:sequence>
                        </xs:complexType>
                </xs:element>
                <xs:element name="Allegati">
                        <xs:complexType>
                                <xs:sequence>
                                        <xs:element name="NumeroAllegati">
                                                <xs:simpleType>
                                                        <xs:restriction base="xs:integer">
                                                                <xs:minInclusive value="0"/>
                                                                <xs:maxInclusive value="999"/>
                                                        </xs:restriction>
                                                </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="IndiceAllegati" minOccurs="0" maxOccurs="unbounded">
                                                <xs:complexType>
```

```
<xs:sequence>
<xs:element name="IdDoc">
<xs:complexType>
<xs:sequence>
<xs:element
name="ImprontaCrittograficaDelDocumento">
<xs:complexType>
<xs:sequence>
<xs:element name="Impronta" Type="xs:base64Binary" />
<xs:element name="Algoritmo" Type="xs:string" default="SHA-256"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element
name="Segnatura" Type="xs:string" minOccurs="0" />
<xs:element
name="Identificativo" Type="xs:string" />
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Descrizione" Type="xs:string" />
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Classificazione" >
<xs:complexType>
<xs:sequence>
<xs:element name="IndiceDiClassificazione" Type="xs:string"  />
<xs:element name="Descrizione" Type="xs:string" />
<xs:element name="PianoDiClassificazione" Type="xs:string" />
```

```
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="Riservato" Type="xs:boolean" />
                        <xs:element name="IdentificativoDelFormato">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="Formato" Type="xs:string" />
                                                <xs:element name="ProdottoSoftware" minOccurs="0">
                                                        <xs:complexType>
                                                                <xs:sequence>
                                                                        <xs:element name="NomeProdotto" Type="xs:string"
minOccurs="0" />
                                                                        <xs:element name="VersioneProdotto" Type="xs:string"
minOccurs="0" />
                                                                        <xs:element name="Produttore" Type="xs:string"
minOccurs="0" />
                                                                </xs:sequence>
                                                        </xs:complexType>
                                                </xs:element>
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="Verifica" minOccurs="0">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="FirmatoDigitalmente" Type="xs:boolean" />
                                                <xs:element name="SigillatoElettronicamente" Type="xs:boolean" />
                                                <xs:element name="MarcaturaTemporale" Type="xs:boolean" />
                                                <xs:element name="ConformitaCopieImmagineSuSupportoInformatico" Type="xs:boolean" />
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="IdAgg" minOccurs="1" maxOccurs="unbounded">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="TipoAggregazione">
                                                        <xs:simpleType>
                                                                <xs:restriction base="xs:string">
```

```
                                                                        <xs:enumeration value="Fascicolo"/>
                                                                        <xs:enumeration value="Serie Documentale"/>
                                                                        <xs:enumeration value="Serie Di Fascicoli"/>
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                                <xs:element name="IdAggregazione" Type="xs:string" />
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="IdIdentificativoDocumentoPrincipale" minOccurs="0">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="ImprontaCrittograficaDelDocumento">
                                                        <xs:complexType>
                                                                <xs:sequence>
                                                                        <xs:element name="Impronta" Type="xs:base64Binary" />
                                                                        <xs:element name="Algoritmo" Type="xs:string"
default="SHA-256"/>
                                                                </xs:sequence>
                                                        </xs:complexType>
                                                </xs:element>
                                                <xs:element name="Segnatura" Type="xs:string" minOccurs="0" />
                                                <xs:element name="Identificativo" Type="xs:string" />
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="VersioneDelDocumento" Type="xs:string"/>
                        <xs:element name="TracciatureModificheDocumento" minOccurs="0" >
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="TipoModifica">
                                                        <xs:simpleType>
                                                                <xs:restriction base="xs:string">
                                                                        <xs:enumeration value="Annullamento"/>
                                                                        <xs:enumeration value="Rettifica"/>
                                                                        <xs:enumeration value="Integrazione"/>
                                                                        <xs:enumeration value="Annotazione"/>
                                                                </xs:restriction>
```

```
                                                                        </xs:simpleType>
                                                                </xs:element>
                                                                <xs:element name="CodiceFiscaleAutoreDellaModifica">
                                                                        <xs:simpleType>
                                                                                <xs:restriction base="xs:string" >
                                                                                        <xs:pattern value="[A-Z]{6}[0-
9LMNPQRSTUV]{2}[ABCDEHLMPRST][0-9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{3}[A-Z]"/>
                                                                                </xs:restriction>
                                                                        </xs:simpleType>
                                                                </xs:element>
                                                                <xs:element name="DataModifica" Type="xs:dateTime"/>
                                                                <xs:element name="IdDocVersionePrecedente">
                                                                        <xs:complexType>
                                                                                <xs:sequence>
                                                                                        <xs:element name="ImprontaCrittograficaDelDocumento">
                                                                                                <xs:complexType>
                                                                                                        <xs:sequence>
                                                                                                                <xs:element
name="Impronta" Type="xs:base64Binary" />
                                                                                                                <xs:element
name="Algoritmo" Type="xs:string" default="SHA-256"/>
                                                                                                        </xs:sequence>
                                                                                                </xs:complexType>
                                                                                        </xs:element>
                                                                                        <xs:element name="Segnatura" Type="xs:string"
minOccurs="0" />
                                                                                        <xs:element name="Identificativo" Type="xs:string" />
                                                                                </xs:sequence>
                                                                        </xs:complexType>
                                                                </xs:element>
                                                        </xs:sequence>
                                                </xs:complexType>
                                        </xs:element>
                                        <xs:element name="TempoDiConservazione" minOccurs="0">
                                                <xs:simpleType>
                                                        <xs:restriction base="xs:integer">
                                                                <xs:minInclusive value="1"/>
                                                                <xs:maxInclusive value="9999"/>
                                                        </xs:restriction>
```

```
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element name="Note" Type="xs:string" minOccurs="0" />
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
</xs:schema>
```

4. METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
IdAgg					
	TipoAggregazione	Indicare: • Fascicolo • Serie Documentale • Serie di fascicoli	Alfanumerico	SI	SI
	IdAggregazione	Come da sistema di identificazione formalmente definito.	Alfanumerico	SI	NO, ma ridefinito
Definizione					
L'idAgg è una sequenza di caratteri alfanumerici associata in modo univoco all'aggregazione documentale informatica in modo da consentirne l'identificazione, indica se si tratta di un Fascicolo o di una Serie Documentale o di una serie fascicoli. *Il fascicolo è una aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.* *Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.* *Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.*					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione

Tipologia fascicolo		Solo in caso di TipoAggregazione = 'Fascicolo' Tipologia del fascicolo: • affare • attività • persona fisica • persona giuridica • procedimento amministrativo	Alfanumerico	SI, solo in caso di TipoAggregazione = 'Fascicolo'	SI
Definizione					
I fascicoli sono organizzati per tipo: • *Tipo 1 - fascicolo per affare: conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta.* • *Tipo 2 - fascicolo per persona fisica o giuridica: comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona (fisica o giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.* • *Tipo 3 - fascicolo per attività: comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.* • *Tipo 4 - fascicolo per procedimento amministrativo: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.*					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Soggetti					
	Ruolo	• Amministrazione titolare • Amministrazioni partecipanti • Soggetto intestatario persona fisica • Soggetto intestatario persona giuridica • RUP (Solo in caso di • TipoAggregazione = 'Fascicolo')	Alfanumerico	SI	SI

	Tipo soggetto	• PF per Persona Fisica • PG per Organizzazione • PA per le Amministrazioni Pubbliche	Alfanumerico	SI	SI
	Nominativo	Nominativo: se Tipo Soggetto = PF: ✓ cognome e nome; se Tipo Soggetto = PG: ✓ denominazione se Tipo Soggetto = PA: ✓ denominazione Amministrazione \ denominazioneAOO;	Alfanumerico	SI	SI
	Codice	Codice identificativo: se Tipo Soggetto = PF ✓ codice fiscale se Tipo Soggetto = PG: ✓ codice fiscale se Tipo Soggetto = PA: ✓ Codice IPA dell'Amministrazione \ Codice AOO	Alfanumerico	SI	SI
	UOR	Unità Organizzativa di riferimento	Alfanumerico	Obbligatorio nel caso si stia indicando Ruolo = RUP	SI

Definizione

Indica il metadato che consente di individuare le informazioni relative a tutti i Soggetti che, a vario titolo, sono coinvolti nella costituzione dell'aggregazione. Sono definiti quindi i seguenti attributi:
• *Ruolo:*
  ○ *Amministrazione titolare*
  ○ *Amministrazioni partecipanti*
  ○ *Soggetto intestatario persona fisica*
  ○ *Soggetto intestatario persona giuridica*
  ○ *RUP (Solo in caso di TipoAggregazione = 'Fascicolo')*
• *Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche*
• *Nominativo: valorizzato a seconda del tipo soggetto.*
• *Codice: valorizzato a seconda del tipo soggetto.*
• *UOR: Nel caso in cui sia stato definito un Ruolo=RUP è obbligatorio indicare anche l'UOR corrispondente.*
Il metadato ha una struttura ricorsiva

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Assegnazione					
	Tipo assegnazione	• Per competenza • Per conoscenza	Alfanumerico	SI, in caso di fascicolo	SI
	Ruolo	Definito come da *Ruolo* del metadato Soggetti.	Alfanumerico	SI, in caso di fascicolo	SI
	Tipo soggetto	Definito come da *Tipo soggetto* del metadato Soggetti.	Alfanumerico	SI, in caso di fascicolo	SI
	Codice	Definito come da *Codice* del metadato Soggetti.	Alfanumerico	SI, in caso di fascicolo	SI
	Data inizio assegnazione	Data inizio assegnazione	Datatime	SI, in caso di fascicolo	SI

	Data fine assegnazione	Data fine assegnazione	Datatime	NO	SI
Definizione					
Indica il metadato che consente di individuare le informazioni relative all'assegnazione per conoscenza o per competenza. *I Soggetti indicati in questo metadato devono essere stati dichiarati nel metadato Soggetti. Sono definiti quindi i seguenti attributi:* • *Tipo assegnazione* • *Ruolo* • *Tipo soggetto* • *Codice* • *Data inizio assegnazione* • *Data fine assegnazione* *Il metadato ha una struttura ricorsiva.*					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
DataApertura		Data	Date	SI	SI
Definizione					
Data di apertura dell'aggregazione documentale.					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione

Classificazione					
	Indice di classificazione	Codifica secondo il Piano di classificazione utilizzato	Alfanumerico	SI	SI
	Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico	SI	SI
	Piano di classificazione	URI del Piano di classificazione pubblicato	Alfanumerico	SI	SI

Definizione

Classificazione dell'aggregazione:

- *Indice di classificazione:* *Codifica del documento secondo il Piano di classificazione utilizzato*
- *Descrizione:* *Descrizione per esteso dell'Indice di classificazione indicato.*
- *Piano di classificazione:* *se presente, riportare eventualmente l'URI di pubblicazione del Piano di classificazione*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
Progressivo			Numerico	SI	SI

Definizione

Progressivo numerico calcolato nell'ambito della chiave della classificazione o in ordine cronologico nell'ambito dell'anno

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione

Chiave descrittiva					
	Oggetto	Testo libero	Alfanumerico	SI	SI
	Parole chiave	Testo libero	Alfanumerico	NO	SI

Definizione

Metadato funzionale volto a chiarirne la natura del fascicolo o della serie. È costituito da seguenti sottocampi:

- *Oggetto: testo libero;*
- *Parole Chiave: da compilare facoltativamente con l'ausilio di attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
DataChiusura		Data	Date	SI, quando l'aggregazione viene chiusa	SI

Definizione

Data di chiusura dell'aggregazione documentale.

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Procedimento Amministrativo					

	Materia\Argomento\Struttura		Indicare la materia o l'argomento o la struttura per la quale sono stati catalogati i procedimenti amministrativi	Alfanumerico	SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
	Procedimento		Denominazione del Procedimento	Alfanumerico	SI, nel caso Tipologia fascicolo = procedimento amministrativo.	SI
	Catalogo procedimenti		Uri di pubblicazione del catalogo	Alfanumerico	SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
	Fasi		A sua volta suddiviso, in una struttura ricorsiva:		SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
		Tipo Fase	• Preparatoria • Istruttoria • Consultiva • Decisoria o deliberativa • Integrazione dell'efficacia	Alfanumerico	SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
		Data inizio fase		Date	SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
		Data fine fase		Date	NO	SI
Definizione						

Metadato funzionale volto ad indicare il procedimento a cui il fascicolo afferisce, nonché lo stato di avanzamento e le relative fasi.
Il sottocampo "Fase", a sua volta costituito da "Tipo Fase":

- *Preparatoria*
- *Istruttoria*
- *Consultiva*
- *Decisoria o deliberativa*
- *Integrazione dell'efficacia*

"Data inizio fase" e "Data fine fase" deve considerarsi dinamico, destinato ad essere aggiornato con lo stato di avanzamento dell'iter del procedimento\processo.

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
Indice documenti		IdDoc		SI	NO, ma ridefinito
Definizione					
Elenco degli identificativi dei documenti contenuti nell'aggregazione. Metadato ricorsivo					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
Posizione fisica Aggregazione Documentale		Testo libero	Alfanumerico	SI, solo nel caso di fascicoli cartacei digitalizzati o di fascicoli ibridi	SI
Definizione					
Posizione fisica dell'aggregazione. Nel caso di fascicoli ibridi indica la posizione della componente cartacea del fascicolo.					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
IdAggPrincipale		Come da sistema di identificazione formalmente definito	Alfanumerico	NO	SI
Definizione					
Identificativo univoco e persistente del livello superiore di fascicolazione nel caso in cui si stia definendo un sottofascicolo o una sottoserie					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tempo di conservazione		• 9999 • 5 anni • 10 anni • …….	Numerico	NO	SI
Definizione					
Tempo di conservazione dell'aggregazione desunto dal Piano di conservazione formalmente integrato al Piano di classificazione. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente".					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
Note		Testo Libero	Alfanumerico	NO	SI
Definizione					
Eventuali indicazioni aggiuntive					

4.1 XSD METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE

Schema xsd:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

	<xs:element name="AggregazioneDocumentaliInformatiche">
		<xs:complexType>
			<xs:sequence>
				<xs:element name="IdAgg" >
					<xs:complexType>
						<xs:sequence>
							<xs:element name="TipoAggregazione">
								<xs:simpleType>
									<xs:restriction base="xs:string">
										<xs:enumeration value="Fascicolo"/>
										<xs:enumeration value="Serie
Documentale"/>
										<xs:enumeration value="Serie Di
Fascicoli"/>
									</xs:restriction>
								</xs:simpleType>
							</xs:element>
							<xs:element name="IdAggregazione" Type="xs:string" />
						</xs:sequence>
					</xs:complexType>
				</xs:element>
				<xs:element name="Tipologia" minOccurs="0">
					<xs:simpleType>
						<xs:restriction base="xs:string">
							<xs:enumeration value="affare"/>
							<xs:enumeration value="attivita"/>
							<xs:enumeration value="persona fisica"/>
							<xs:enumeration value="persona giuridica"/>
							<xs:enumeration value="procedimento amministrativo"/>
						</xs:restriction>
```

```
                                        </xs:simpleType>
                                </xs:element>
                                <xs:element name="Soggetti" minOccurs="1" maxOccurs="unbounded">
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element name="Ruolo">
                                                                <xs:simpleType>
                                                                        <xs:restriction base="xs:string">
                                                                                <xs:enumeration value="Amministrazione
titolare"/>
                                                                                <xs:enumeration value="Amministrazioni
partecipanti"/>
                                                                                <xs:enumeration value="Soggetto
intestatario persona fisica"/>
                                                                                <xs:enumeration value="Soggetto
intestatario persona giuridica"/>
                                                                                <xs:enumeration value="RUP" />
                                                                        </xs:restriction>
                                                                </xs:simpleType>
                                                        </xs:element>
                                                        <xs:element name="TipoSoggetto">
                                                                <xs:simpleType>
                                                                        <xs:restriction base="xs:string">
                                                                                <xs:enumeration value="PF"/>
                                                                                <xs:enumeration value="PG"/>
                                                                                <xs:enumeration value="PA"/>
                                                                        </xs:restriction>
                                                                </xs:simpleType>
                                                        </xs:element>
                                                        <xs:element name="Nominativo" Type="xs:string" />
                                                        <xs:element name="Codice" Type="xs:string" />
                                                        <xs:element name="UOR" Type="xs:string" minOccurs="0" />
                                                </xs:sequence>
                                        </xs:complexType>
                                </xs:element>
                                <xs:element name="Assegnazione" minOccurs="0" maxOccurs="unbounded">
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element name="TipoAssegnazione">
```

```
                                                        <xs:simpleType>
                                                                <xs:restriction base="xs:string">
                                                                        <xs:enumeration value="Per competenza"/>
                                                                        <xs:enumeration value="Per conoscenza"/>
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                                <xs:element name="Ruolo">
                                                        <xs:simpleType>
                                                                <xs:restriction base="xs:string">
                                                                        <xs:enumeration value="Amministrazione
titolare"/>
                                                                        <xs:enumeration value="Amministrazioni
partecipanti"/>
                                                                        <xs:enumeration value="Soggetto
intestatario persona fisica"/>
                                                                        <xs:enumeration value="Soggetto
intestatario persona giuridica"/>
                                                                        <xs:enumeration value="RUP" />
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                                <xs:element name="TipoSoggetto">
                                                        <xs:simpleType>
                                                                <xs:restriction base="xs:string">
                                                                        <xs:enumeration value="PF"/>
                                                                        <xs:enumeration value="PG"/>
                                                                        <xs:enumeration value="PA"/>
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                                <xs:element name="Codice" Type="xs:string" />
                                                <xs:element name="DataInizioAssegnazione" Type="xs:dateTime"/>
                                                <xs:element name="DataFineAssegnazione" Type="xs:dateTime"
minOccurs="0"/>
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="DataApertura" Type="xs:date"/>
```

```
                        <xs:element name="Classificazione" >
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="IndiceDiClassificazione" Type="xs:string" />
                                                <xs:element name="Descrizione" Type="xs:string" />
                                                <xs:element name="PianoDiClassificazione" Type="xs:string"/>
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="Progressivo">
                                <xs:simpleType>
                                        <xs:restriction base="Integer">
                                                <xs:minInclusive value="1"/>
                                                <xs:maxInclusive value="999999999"/>
                                        </xs:restriction>
                                </xs:simpleType>
                        </xs:element>
                        <xs:element name="ChiaveDescrittiva">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="Oggetto" Type="xs:string" />
                                                <xs:element name="ParoleChiave" Type="xs:string" minOccurs="0"
maxOccurs="5" />
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="DataChiusura" type="xs:date" minOccurs="0"/>
                        <xs:element name="ProcedimentoAmministrativo" minOccurs="0" >
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element name="MateriaArgomentoStruttura" Type="xs:string" />
                                                <xs:element name="Procedimento" Type="xs:string" />
                                                <xs:element name="CatalogoProcedimenti"  Type="xs:string" />
                                                <xs:element name="Fase" minOccurs="1" maxOccurs="unbounded">
                                                        <xs:complexType>
                                                                <xs:sequence>
                                                                        <xs:element name="TipoFase" >
                                                                                <xs:simpleType>
```

```
                                                                                    <xs:restriction
base="xs:string">
                                                                                            <xs:enumeration
value="Preparatoria"/>
                                                                                            <xs:enumeration
value="Istruttoria"/>
                                                                                            <xs:enumeration
value="Consultiva"/>
                                                                                            <xs:enumeration
value="Decisoria o deliberativa"/>
                                                                                            <xs:enumeration
value="Integrazione dell’efficacia"/>
                                                                                    </xs:restriction>
                                                                            </xs:simpleType>
                                                                    </xs:element>
                                                                    <xs:element name="DataInizioFase"
type="xs:date"/>
                                                                    <xs:element name="DataFineFase"
type="xs:date" minOccurs="0"/>
                                                            </xs:sequence>
                                                    </xs:complexType>
                                            </xs:element>
                                    </xs:sequence>
                            </xs:complexType>
                    </xs:element>
                    <xs:element name="IndiceDocumenti" minOccurs="1" maxOccurs="unbounded">
                            <xs:complexType>
                                    <xs:sequence>
                                            <xs:element name="IdDoc">
                                                    <xs:complexType>
                                                            <xs:sequence>
                                                                    <xs:element
name="ImprontaCrittograficaDelDocumento">
                                                                            <xs:complexType>
                                                                                    <xs:sequence>
                                                                                            <xs:element
name="Impronta" Type="xs:base64Binary" />
                                                                                            <xs:element
name="Algoritmo" Type="xs:string" default="SHA-256"/>
```

```
                                                                                                </xs:sequence>
                                                                                        </xs:complexType>
                                                                                </xs:element>
                                                                                <xs:element name="Segnatura"
Type="xs:string" minOccurs="0" />
                                                                                <xs:element name="Identificativo"
Type="xs:string" />
                                                                        </xs:sequence>
                                                                </xs:complexType>
                                                        </xs:element>
                                                </xs:sequence>
                                        </xs:complexType>
                                </xs:element>
                                <xs:element name="PosizioneFisicaAggregazioneDocumentale" Type="xs:string"
minOccurs="0" />
                                <xs:element name="IdAggPrincipale" minOccurs="0">
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element name="TipoAggregazione">
                                                                <xs:simpleType>
                                                                        <xs:restriction base="xs:string">
                                                                                <xs:enumeration value="Fascicolo"/>
                                                                                <xs:enumeration value="Serie
Documentale"/>
                                                                                <xs:enumeration value="Serie Di
Fascicoli"/>
                                                                        </xs:restriction>
                                                                </xs:simpleType>
                                                        </xs:element>
                                                        <xs:element name="IdAggregazione" Type="xs:string" />
                                                </xs:sequence>
                                        </xs:complexType>
                                </xs:element>
                                <xs:element name="TempoDiConservazione" minOccurs="0">
                                        <xs:simpleType>
                                                <xs:restriction base="xs:Integer">
                                                        <xs:minInclusive value="1"/>
                                                        <xs:maxInclusive value="9999"/>
                                                </xs:restriction>
```

```
                                    </xs:simpleType>
                                </xs:element>
                                <xs:element name="Note" Type="xs:string" minOccurs="0" />
                            </xs:sequence>
                        </xs:complexType>
                </xs:element>

</xs:schema>
```