COMUNE DI CONIOLO

Provincia di Alessandria

MANUALE DI GESTIONE DOCUMENTALE

Conforme alle Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici pubblicate il10 settembre 2020 ai sensi dell'art. 71 del CAD e modificate il 18/05/2021 con determinazione n. 371/2021

Adottato con Deliberazione di Giunta Comunale n.42 del 07/06/2025

Cod. **850365.d**
Grafiche E. Gaspari

Sommario

PARTE PRIMA – DISPOSIZIONI PRELIMINARI 5

1. Riferimenti normativi 5

2. Finalità, contenuti e metodologia del documento 6

3. Definizioni 6

PARTE SECONDA – ORGANIZZAZIONE 7

4. Area organizzativa omogenea e Unità Organizzative Responsabili (UOR) 7

5. Il Responsabile della gestione documentale 7

6. La governance della gestione documentale 8

7. Livelli di accesso al sistema di protocollo 8

PARTE TERZA – FORMAZIONE DEI DOCUMENTI 9

Modalità di formazione 9

8. Modalità di formazione dei documenti informatici 9

8.1. Creazione e redazione tramite software di documenti informatici 9

8.2. Acquisizione di documenti informatici 10

8.3. Copie per immagine su supporto informatico di documenti analogici 11

8.4. Duplicati, copie ed estratti informatici di documenti informatici 11

8.5. Acquisizione di istanze tramite moduli online 12

Sezione seconda – Disposizioni comuni a tutte le modalità di formazione 13

9. Dispositivi di firma elettronica 13

10. Identificazione univoca del documento informatico 13

11. Associazione degli allegati al documento principale 13

12. Metadati del documento informatico 14

13. Immodificabilità e integrità del documento informatico 14

PARTE QUARTA - GESTIONE DOCUMENTALE 15

Flussi documentali esterni 15

14. Ricezione telematica di documenti informatici in entrata 15

15. Canali di ricezione 15

16. Valutazione di interoperabilità 16

17. Trasmissione telematica di documenti informatici in uscita 16

Cod. **850365.d**
Grafiche E. Gaspari

18. Comunicazioni e trasmissione di documenti con altre Pubbliche Amministrazioni 17

19. Disposizioni sui documenti analogici 17

Protocollo informatico 18

20. Sistema di protocollo informatico 18

21. Funzioni del Responsabile della Gestione Documentale in materia diprotocollo informatico 18

22. Registro generale di protocollo 18

23. Documenti soggetti a registrazione di protocollo e documenti esclusi 19

24. Registrazione di protocollo 19

25. Annullamento e modifiche della registrazione di protocollo 20

26. Segnatura di protocollo 21

27. Documenti soggetti a registrazione particolare 21

28. Registro di emergenza 22

29. Disposizioni sulla protocollazione di documenti analogici 23

Classificazione e fascicolazione 24

30. Classificazione dei documenti 24

31. Fascicolazione informatica dei documenti 25

Flussi documentali interni 26

32. Assegnazione dei documenti in entrata agli uffici 26

33. Comunicazioni interne 26

34. Pubblicazioni nell'Albo pretorio 26

PARTE QUINTA – CONSERVAZIONE DEIDOCUMENTI 27

35. Piano di conservazione dell'archivio 27

36. Responsabile della conservazione 27

37. Oggetti e formati della conservazione 28

38. Archiviazione e conservazione digitale dei documenti informatici 29

39. Selezione e scarto archivistico 29

40. Misure di sicurezza e monitoraggio 29

PARTE SESTA – MISURE DI SICUREZZA E PROTEZIONE DEI DATI PERSONALI 31

41. Piano di sicurezza informatica 31

42. Credenziali di accesso al sistema documentale 32

43. Trattamento dei dati personali 33
44. Piano formativo del personale 33
45. Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza..... 34
PARTE SETTIMA - NORME TRANSITORIE E FINALI 35
46. Modalità di approvazione e aggiornamento del manuale..... 35
47. Pubblicità del manuale..... 35
48. Entrata in vigore..... 35

ALLEGATI

Allegato 1. Glossario e definizioni
Allegato 2. Organigramma con indicazione delle UOR
Allegato 3. Titolario
Allegato 4. Livelli di abilitazione
Allegato 5. Metadati
Allegato 6. Metadati documento fiscale e contabile
Allegato 7. Modulo misure minime di sicurezza

Cod. **850365.d**
Grafiche E. Gaspari

PARTE PRIMA – DISPOSIZIONI PRELIMINARI

1. Riferimenti normativi

Il presente Manuale di gestione documentale èadottato ai sensi delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* (d'ora in avanti "Linee guida"), emanate dall'Agenzia per l'Italia Digitale con determinazione del Direttore generale del 9 settembre 2020, n. 407 e pubblicate il 10 settembre 2020, come modificate dalla recente determinazione n. 371 del 17 maggio 2021.

Gli allegati alle Linee guida sono parte integrante delle stesse e contengono disposizioni relative a:

1) Glossario dei termini e degli acronimi;
2) Formati di file e riversamento;
3) Certificazione di processo;
4) Standard e specifiche tecniche;
5) Metadati;
6) Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

Ulteriori norme rilevanti ai fini della gestione documentale sono:

- le disposizioni in materia di formazione dei documenti informatici, anche di natura amministrativa, e di digitalizzazione dell'attività amministrativa di cui al d.lgs. 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale*" (di seguito "CAD")
- le disposizioni in materia di documentazione amministrativa di cui al d.P.R. 28 dicembre 2000, n. 445 *"Disposizioni legislative in materia di documentazione amministrativa"* (di seguito "TUDA");
- le norme sul procedimento amministrativo di cui alla l. 7 agosto 1990, n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";
- le disposizioni sulla trasparenza di cui al d.lgs. 14 marzo 2013, n. 33 "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*";
- le disposizioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno di cui al Regolamento

(UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014 (Regolamento “eIDAS”);

- le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 *“Regolamento generale sulla protezione dei dati”* (“GDPR”) e d.lgs. 30 giugno 2003 n. 196 “*Codice in materia di protezionedei dati personali*”;

- Circolare 18 aprile 2017, n. 2/2017 dell’Agenzia per l’Italia Digitale*, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni*.

2. Finalità, contenuti e metodologia del documento

Il Manuale della gestione documentale descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Con la pubblicazione nella sezione “Amministrazione Trasparente” del sito internet istituzionale, il Manuale è reso noto anche esternamente all’ente. In quest’ottica, il Manuale costituisce altresì un documento pubblico funzionale al perseguimento del principio di trasparenza dell’azione amministrativa.

3. Definizioni

Ai fini dell’utilizzo del presente manuale si applicano le definizioni del glossario di cui all’Allegato n. 2 “Glossario e definizioni” che ne costituisce parte integrante.

PARTE SECONDA – ORGANIZZAZIONE

4. Area organizzativa omogenea e Unità Organizzative Responsabili (UOR)

Il Comune di Coniolo si configura come un'unica Area Organizzativa Omogenea ("AOO") denominata "Area Omogenea Unica". L'AOO e gliindirizzi di posta elettronica a essa associati sono indicati nell'Indice PA.

5. Il Responsabile della gestione documentale

Il Comune di Coniolo nell'ottica di gestire modo integrato tutte le fasi del ciclo di vita dei documenti informatici, ha individuato un'unica figura dirigenziale, il "Responsabile della gestione documentale", dotata di competenze giuridiche, informatiche e archivistiche, a cui affidare le funzioni e i compiti del Responsabile per la gestione documentale e del Responsabile della conservazione.

Con riferimento all'unica AOO si prende atto che con deliberazione di Giunta Comunale n. 41 in data 07/06/2025 è stato individuato nel signor Arles Garelli che riveste la qualifica di Sindaco pro tempore il Responsabile della gestione documentale, che ha provveduto alla predisposizione del presente manuale, parimenti con il medesimo provvedimento è stato individuato il vicario nella dott.ssa Daria Patrucco che riveste la qualifica di istruttore amministrativo/contabile.

I compiti del Responsabile della gestione documentale (di seguito "Responsabile") sono definiti nell'atto di nomina. In particolare, il Responsabile:

- è preposto, ai sensi dell'art. 61 TUDA, al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi della AOO unica del Comune;
- provvede, d'intesa con il Responsabile per la Transizione Digitale (RTD), previo parere del Responsabile per la Protezione dei Dati personali (RPD), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;
- monitora i processi e le attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;
- valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;
- vigila sul rispetto delle norme e delle procedure durante le operazioni di registrazione di protocollo, di segnatura di protocollo, di produzione e conservazione del registro giornaliero di protocollo;
- assicura l'accesso al sistema di gestione documentale, provvedendo alla definizione delle abilitazioni di accesso, e vigila sul rispetto delle misure di sicurezza e di protezione dei dati;
- effettua un periodico censimento degli strumenti software di gestione documentale in uso presso il Comune e, di concerto con il RTD, ne verifica la

conformità alla normativa vigente.

6. La governance della gestione documentale

Il responsabile della gestione documentale è preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi e, d'intesa con il responsabile della conservazione (se soggetto diverso), il responsabile per la transizione digitale (RTD) e acquisito il parere del responsabile della protezione dei dati personali, predispone il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione.

7. Livelli di accesso al sistema di protocollo

Ciascun utente che abbia accesso al Sistema di protocollo è identificato da un profilo, al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

Di norma tutti gli utenti hanno un profilo standard di abilitazione alle funzioni di inserimento in partenza o interni, aggiornamento e consultazione di protocolli esclusivamente attinenti alla propria area di appartenenza.

Solo gli addetti al Servizio hanno una profilatura che permetta la registrazione, modifica ed accesso a tutte le registrazioni di protocollo e fascicolazioni, al fine di garantire un servizio di assistenza generale a tutti gli altri utenti.

Nei casi in cui sia necessario estendere l'abilitazione del profilo per particolari esigenze di servizio, il Responsabile dell'Area di appartenenza ne deve fare espressa e motivata richiesta al Responsabile della Gestione Documentale, che autorizzerà la modifica del Profilo. La profilatura degli accessi è costantemente monitorata dal Responsabile della Gestione Documentale.

I livelli di abilitazione sono riportati nell'allegato 4 al presente Manuale.

PARTE TERZA – FORMAZIONE DEI DOCUMENTI

Modalità di formazione

8. Modalità di formazione dei documenti informatici

Tutti i documenti sono formati in originale come documenti informatici mediante una delle seguenti modalità:

a) creazione e redazione tramite l'utilizzo di strumenti di 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 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 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.

Di seguito sono fornite indicazioni specifiche per ciascuna delle modalità sopra descritte

8.1. Creazione e redazione tramite software di documenti informatici

Gli uffici del Comune dispongono dei seguenti strumenti software per la creazione dei documenti informatici mediante redazione:

- programmi della suite *Microsoft Office: Word, Excel, Access, Powerpoint, ecc.;*
- programmi del gestionale Siscom.

Elementi essenziali del documento amministrativo informatico

Ogni documento amministrativo informatico creato e redatto dal Comune deve recare obbligatoriamente i seguenti elementi:

1. denominazione dell'Amministrazione;
2. autore e ufficio responsabile;
3. numero e data di protocollo o di registrazione (se soggetto a registrazione particolare);
4. oggetto del documento;
5. riferimenti a procedimento o fascicolo;
6. sottoscrizione;

7. data e luogo;
8. numeri di pagina;
9. indicazione degli allegati (se presenti);
10. identificazione e dati dei destinatari (se si tratta di documento in uscita);
11. dati dell'Amministrazione (compresi indirizzo e recapiti, se si tratta di documento in uscita);
12. mezzo di spedizione (se documento in uscita).

Scelta del formato e modalità di sottoscrizione

Il formato del documento informatico deve essere individuato tra quelli previsti nell'Allegato 2 alle Linee guida dell'AgID.

Le versioni del documento precedenti alla versione definitiva (bozze, minute, ecc.), possono essere salvate in un formato che ne consente la modificabilità (ad esempio, .docx o .odt). La versione definitiva del documento, invece, è sempre preferibile sia in formato PDF.

Una volta giunto alla sua versione definitiva, prima della sottoscrizione, il documento informatico in formato PDF. I documenti di maggiore rilevanza giuridico-amministrativa (ad esempio, gli atti del Sindaco e degli organi collegiali, i contratti, le determine a contenuto provvedimentale, ecc.), prima della firma, devono essere convertiti in formato PDF/A (PDF non modificabile). I documenti in formato PDF e PDF/A sono sottoscritti con firma PADES.

Nel caso il documento definitivo assuma un formato diverso dal PDF, la sottoscrizione avviene con firma CADES (P7M).

8.2. Acquisizione di documenti informatici

La formazione di documenti informatici per acquisizione può avvenire secondo una delle seguenti modalità:

a) acquisizione di un documento informatico per via telematica o su supporto informatico;

b) acquisizione della copia per immagine su supporto informatico di un documento analogico;

c) acquisizione della copia informatica di un documento analogico.

In caso di acquisizione di copia informatica del documento originale (analogico o informatico), al fine di assicurarne l'efficacia giuridico-probatoria, occorre attestare la conformità della copia all'originale da cui è estratta (con le modalità indicate nelle disposizioni successive).

In caso di acquisizione di un duplicato informatico, ai sensi dell'art. 23-*bis* del CAD, esso ha la stessa efficacia giuridico-probatoria del documento informatico originale; pertanto, non è richiesta l'attestazione di conformità.

8.3. Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 delle Linee Guida "Certificazione di Processo".

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD, nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico 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.

La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'art. 22, commi 4 e 5 del CAD.

8.4. Duplicati, copie ed estratti informatici di documenti informatici

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".doc" in un documento ".pdf". L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;

- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 delle Linee Guida "Certificazione di Processo".

Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

Fatto salvo quanto previsto dall'art. 23bis comma 2 del CAD, nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

8.5. Acquisizione di istanze tramite moduli online

Le istanze provenienti dagli utenti possono essere formate anche tramite la compilazione di moduli e *form* messi a disposizione sul sito web del Comune e resi accessibili previa identificazione dell'utente con gli strumenti di identificazione SPID, CIE e CNS. I dati immessi dall'istante sono acquisiti e memorizzati su supporto informatico. Le istanze così formate sono acquisite dal Sistema di protocollo informatico del Comune e costituiscono a tutti gli effetti documenti amministrativi informatici e sono trattati come documenti in entrata soggetti a registrazione di protocollo. Il file di log relativi agli accessi e alle attività svolte dagli utenti sono conservati secondo le stesse modalità di conservazione delle istanze ricevute tramite PEC.

Sezione seconda – Disposizioni comuni a tutte le modalità di formazione

9. Dispositivi di firma elettronica

Il Comune garantisce che tutti i dipendenti e i titolari di cariche che firmano documenti a valenza esterna siano dotati di dispositivi di firma elettronica. A tal fine, il Comune è dotato di sistemi di gestione documentale che consentono ai dipendenti in possesso di profilo utente l'apposizione della firma digitale.

L'utilizzo del dispositivo di firma è strettamente personale e riconducibile al suo titolare. Pertanto, il dispositivo non deve essere ceduto, né devono essere diffuse le chiavi dei certificati.

Ogni titolare di dispositivo di firma verifica periodicamente la validità e la data di scadenza del certificato di firma, al fine di provvedere tempestivamente al rinnovo.

Quando la firma è apposta utilizzando un certificato prossimo alla scadenza, il titolare ne dà avviso al Responsabile, affinché provveda a costituire un riferimento temporale giuridicamente valido tale da attestare che la firma sia stata apposta in un momento in cui il certificato era valido. In particolare, costituiscono riferimento temporale giuridicamente valido le seguenti attività sul documento firmato:

- apposizione di marca temporale;
- apposizione della segnatura di protocollo;
- versamento in conservazione.

Documenti, dati e altre informazioni trasmesse in cooperazione applicativa non richiedono la sottoscrizione digitale o l'apposizione della marca temporale.

10. Identificazione univoca del documento informatico

Ogni documento informatico deve essere identificato in modo univoco e persistente.

L'identificazione univoca dei documenti è effettuata con l'associazione al documento dell'impronta crittografica *hash*. Per i documenti soggetti a registrazione di protocollo, l'associazione è effettuata tramite le apposite funzioni del Sistema di protocollo informatico del Comune. Per i documenti non protocollati, l'associazione è effettuata tramite le apposite funzioni degli strumenti software in uso per la formazione degli atti. In ogni caso l'impronta crittografica deve essere basata su una funzione di hash conforme alle tipologie di algoritmi previste nell'allegato 6 alle Linee guida.

11. Associazione degli allegati al documento principale

Gli allegati sono congiunti in modo univoco al documento informatico principale tramite l'associazione delle impronte hash dei documenti allegati al documento principale.

Al documento principale, inoltre, devono essere associati i seguenti metadati:

- numero allegati;
- indice allegati;

- identificativo del documento allegato (IdDoc);
- titolo dell'allegato (Descrizione).

A ciascun allegato, invece, deve essere associato il metadato identificativo del documento principale (IdDoc).

Le operazioni di associazione degli allegati, quando possibile, sono effettuate in modo automatizzato dal sistema di gestione documentale adoperato per la formazione del documento principale.

In alternativa, è possibile associare gli allegati al documento principale manualmente, riportando in calce al documento stesso l'elenco degli allegati, indicando per ciascuno l'oggetto e la relativa impronta hash. L'associazione sarà assicurata una volta che il documento informatico principale sia divenuto immodificabile.

12. Metadati del documento informatico

Al documento informatico e al documento amministrativo informatico devono essere associati i metadati obbligatori previsti dall'Allegato 5 alle Linee guida dell'AgID e riportati nell'Allegato 5 del presente manuale assieme ai metadati relativi al documento contabile e fiscale (Allegato 6).

I metadati devono essere associati prima che il documento informatico acquisisca le caratteristiche di immodificabilità e integrità, dunque prima della sottoscrizione, della memorizzazione nel sistema o del versamento in conservazione.

13. Immodificabilità e integrità del documento informatico

Affinché sia garantito il valore giuridico-probatorio del documento informatico, ne deve essere assicurata l'immodificabilità e l'integrità.

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nelle fasi di accesso, gestionee conservazione.

L'immodificabilità e l'integrità dei documenti informatici dell'ente possono sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza;
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento ad un sistema di conservazione.

PARTE QUARTA - GESTIONE DOCUMENTALE

Flussi documentali esterni

14. Ricezione telematica di documenti informatici in entrata

I documenti informatici in entrata, pervenuti tramite i canali di ricezione previsti, sono oggetto di registrazione di protocollo secondo quanto previsto nella sezione successiva. Una volta che ne sia accertata la provenienza, i documenti sono validi ai fini del procedimento amministrativo.

Le istanze, le dichiarazioni e le comunicazioni trasmesse per via telematica, in ogni caso, devono ritenersi valide a tutti gli effetti di legge quando:

a) sono contenute in documenti sottoscritti con firma digitale o firma elettronica qualificata;

b) sono trasmesse a mezzo posta elettronica certificata da un indirizzo PEC iscritto in uno degli elenchi di domicili digitali previsti dalla normativa vigente;

c) sono trasmesse attraverso un sistema informatico che consente la previa identificazione dell'utente con i sistemi SPID, CIE o CNS;

d) sono trasmesse da un domicilio digitale PEC ai sensi dell'art. 3-bis, comma4-quinquies del CAD ed è possibile accertare la provenienza della trasmissione. Tale modalità di trasmissione costituisce elezione di domiciliodigitale speciale per quel singolo procedimento o affare;

e) sono contenute in copie digitali di documenti originali cartacei sottoscritti e presentati unitamente a copia del documento d'identità dell'autore;

f) è comunque possibile accertarne la provenienza secondo la normativa vigente o, comunque, in base a criteri di attendibilità e riconducibilità al mittente dichiarato.

15. Canali di ricezione

La ricezione di comunicazioni e documenti informatici è assicurata tramite i seguenti canali:

- casella PEC;
- acquisizione di istanze, redatte anche tramite *form*;
- acquisizione tramite servizio online, accessibile previa identificazione dell'utente, delle istanze e dei documenti informatici relativi alle pratiche degli sportelli SUE e SUAP;
- cooperazione applicativa tra pubbliche amministrazioni;
- altri canali di trasmissione, anche di posta elettronica ordinaria, indicati per specifici procedimenti.

L'indirizzo di posta elettronica certificata è riportato nell'Indice delle Pubbliche

Amministrazioni e pubblicizzato sul sito web istituzionale.

Nel caso in cui un soggetto tenuto a effettuare comunicazioni esclusivamente in via telematica (imprese, professionisti, altre PP.AA., salvi i casi di cui all'art. 2, comma 6, CAD) faccia pervenire agli uffici del Comune comunicazioni e documenti in modalità analogica, questi non saranno ritenuti validamente trasmessi. In tali casi, la circostanza è segnalata in nota alla registrazione di protocollo. Il responsabile dell'UO assegnataria della comunicazione, o comunque il soggetto individuato quale responsabile del procedimento, ai sensi dell'art. 5, comma 3, l. n. 241/1990, provvede a comunicare al mittente il motivo della mancata accettazione dei documenti e a indicare modalità di trasmissione valide. La comunicazione, quando possibile, è trasmessa al domicilio digitale del mittente estratto dagli indici di cui agli articoli 6-*bis* e 6-*ter* del CAD.

16. Valutazione di interoperabilità

Sono accettati, e conseguentemente registrati al protocollo, documenti informatici esclusivamente nei formati previsti dall'allegato 2 alle Linee guida "Formati di file e riversamento".

Nello scegliere i formati di file di cui sopra, da utilizzare per i propri documenti informatici, i soggetti preposti possono effettuare una valutazione di interoperabilità che tenga conto dei seguenti fattori: formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo.

È possibile utilizzare formati diversi da quelli elencati nell'Allegato 2, effettuando una valutazione di interoperabilità in base alle indicazioni previste nell'Allegato stesso. 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.

A seguito della valutazione di interoperabilità, il responsabile della gestione documentale valuta l'esigenza o l'opportunità di effettuare o pianificare il riversamento dei file da un formato di file ad un altro formato, sempre tenendo in considerazione quanto previsto nel punto precedente. Il riversamento è effettuato in base alle indicazioni previste nell'Allegato 2.

17. Trasmissione telematica di documenti informatici in uscita

La trasmissione di comunicazioni e documenti avviene sempre per via telematica, salvo il caso trasmissione a soggetti privati privi di domicilio digitale ai sensi degli artt.6 e ss. del CAD.

Per la trasmissione telematica di documenti a imprese e professionisti tenuti obbligatoriamente all'iscrizione in albi o elenchi, il domicilio digitale è estratto dall'indice INI-PEC (www.inipec.gov.it).

I documenti informatici in uscita sono trasmessi a mezzo PEC solo dopo essere stati

classificati, fascicolati e protocollati secondo le disposizioni della presente Parte del Manuale.

La trasmissione di dati e altre informazioni in cooperazione applicativa è soggetta a protocollazione o a registrazione particolare secondo le medesime regole per la registrazione di protocollo dei documenti.

18. Comunicazioni e trasmissione di documenti con altre Pubbliche Amministrazioni

La trasmissione di comunicazioni e documenti verso altre pubbliche amministrazioni avviene sempre per via telematica, agli indirizzi di posta elettronica, anche ordinaria, dei singoli uffici. Gli indirizzi di spedizione sono rilevati tramite la consultazione dell'Indice delle Pubbliche Amministrazioni (indicepa.gov.it) di cui all'art. 6-*ter* del CAD.

I documenti che devono essere prodotti entro un determinato termine sono sempre trasmessi a mezzo PEC.

19. Disposizioni sui documenti analogici

I documenti su supporto analogico possono pervenire al Comune attraverso:

- il servizio postale;
- la consegna diretta agli uffici agli addetti alle attività di sportello;
- il fax, nei soli casi di esclusione dell'applicazione della normativa previsti dall'art. 2,comma 6, D.lgs. n. 82/2005.

Gli orari definiti per la presentazione della documentazione analogica sono indicati sul sito web istituzionale del Comune.

Le buste delle comunicazioni cartacee sono conservate insieme ai documenti in esse contenuti.

Protocollo informatico

20. Sistema di protocollo informatico

Per la gestione dei documenti è adottato un modello organizzativo che prevede la partecipazione attiva di più soggetti ed uffici utente, ognuno dei quali è abilitato a svolgere soltanto le operazioni di propria competenza.

Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica dei documenti, l'identificazione degli uffici utente e del personale abilitati allo svolgimento delle operazioni di registrazione di protocollo, l'organizzazione ed archiviazione dei documenti dell'AOO, sono individuate dal Responsabile del servizio di protocollo informatico (se diverso dal Responsabile della gestione documentale) che tiene conto delle richieste e delle esigenze dei responsabili delle UOR.

Il servizio informatico esegue la funzione di aggiornamento dei profili di abilitazione alla protocollazione, solo su indicazione del Responsabile del servizio di Protocollo.

21. Funzioni del Responsabile della Gestione Documentale in materia diprotocollo informatico

La corretta tenuta del protocollo informatico è garantita dal Responsabile della gestione documentale. In particolare, il Responsabile, nella veste di responsabile del protocollo informatico:

a. coordina la gestione del Sistema di protocollo informatico;
b. assegna al personale addetto alla protocollazione l'abilitazione all'utilizzo delle funzioni di protocollo del Sistema;
c. esercita il controllo generale sui flussi documentali esterni e interni;
d. assicura la corretta esecuzione delle attività di protocollazione;
e. autorizza l'attivazione del protocollo di emergenza;
f. autorizza con comunicazione formale le operazioni di annullamento delle registrazioni di protocollo;
g. vigila sull'osservanza della normativa e delle disposizioni del presente Manuale da parte del personale addetto.

Le attività di protocollazione sono eseguite dagli utenti delegati dal Responsabile.

22. Registro generale di protocollo

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

Nell'ambito della AOO il Registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo.

Il numero di protocollo è costituito da almeno sette cifre numeriche. La numerazione è

progressiva, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo è associato in modo univoco e immodificabile al documento; pertanto, esso individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo, anche se i documenti sono strettamente correlati tra loro. Non è pertanto consentita in nessun caso la cosiddetta registrazione “a fronte”, cioè l’utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione che non è stata registrata sul protocollo viene considerata giuridicamente inesistente presso l’amministrazione. Non è consentita la protocollazione di un documento già protocollato. Qualora ciò avvenisse per errore, la seconda protocollazione va annullata.

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso è prodotto automaticamente dal Sistema di protocollo informatico, che provvede altresì al versamento automatico al Sistema di conservazione.

23. Documenti soggetti a registrazione di protocollo e documenti esclusi

Tutti i documenti prodotti e ricevuti dall’Ente, indipendentemente dal supporto sul quale sono formati, sono registrati al protocollo, ad eccezione di quelli indicati successivamente.

Ai sensi dell’articolo 53 del TUDA sono esclusi dalla registrazione di protocollo:

- Gazzette Ufficiali, Bollettini Ufficiali, notiziari della Pubblica Amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, stampe varie, plichi di libri;
- biglietti augurali, inviti a manifestazioni e documenti di occasione vari che non attivino procedimenti amministrativi;
- bolle accompagnatorie;
- richiesta/invio comunicazioni informali.

Le ricevute di accettazione e di consegna di un messaggio inviato tramite PEC non devono essere protocollate, ma devono essere associate alla registrazione di protocollo del documento trasmesso/ricevuto a cui la ricevuta stessa si riferisce.

24. Registrazione di protocollo

La registrazione di protocollo è l’insieme dei metadati che il registro di protocollo deve memorizzare in forma non modificabile al fine di garantirne l'identificazione univoca e certa. Ai sensi dell’art. 53, comma 1, TUDA, metadati di registrazione di protocollo sono:

a) numero di protocollo del documento, generato automaticamente dal sistema;
b) data di registrazione di protocollo, assegnata automaticamente dal sistema;
c) il mittente, per i documenti ricevuti, e il destinatario (o i destinatari), per i documenti spediti;
d) oggetto del documento;
e) data e protocollo del documento ricevuto, se disponibili;
f) l'impronta del documento informatico.

A suddetti metadati registrati in forma non modificabile, inoltre, possono essere aggiunti (a seconda dei casi) i seguenti ulteriori metadati:

a) tipologia di documento;
b) classificazione (titolo e classe) sulla base del Titolario e del Prontuario di Classificazione;
c) fascicolo di appartenenza;
d) assegnazione interna (per competenza o per conoscenza);
e) data e ora di arrivo;
f) allegati;
g) livello di riservatezza;
h) mezzo di ricezione o invio;
i) annotazioni;
j) (eventualmente) estremi del provvedimento di differimento della registrazione;
k) (se necessario) elementi identificativi del procedimento amministrativo.

25. Annullamento e modifiche della registrazione di protocollo

La registrazione degli elementi obbligatori del protocollo non può essere modificata né integrata, né cancellata, ma soltanto annullata attraverso l'apposita procedura conforme all'art. 54 del TUDA. In particolare, i metadati non sono modificabili, ma eventualmente annullabili.

Ogni annullamento della registrazione deve:

- essere autorizzato con comunicazione formale del Responsabile;
- comportare la memorizzazione di data, ora e estremi della comunicazione formale di annullamento;
- consentire sempre la memorizzazione e la visibilità delle informazioni oggetto di annullamento.

Le richieste di annullamento rivolte al Responsabile devono essere motivate. Le richieste sono accolte, di norma, in casi di mero errore materiale (quali ad es. la doppia registrazione, la registrazione di documenti che non diano seguito a procedimenti o ad attività amministrative proprie dell'ente, la registrazione errata che necessiterebbe di modifiche sostanziali dei campi obbligatori). Solo il Responsabile ha il potere di autorizzare l'annullamento delle registrazioni di protocollo, ovvero di dare disposizioni in tal senso. Il Responsabile può delegare il personale addetto al Servizio di Protocollo ad autorizzare le operazioni di annullamento, che deve risultare in modo esplicito nel provvedimento di delega. In tal caso, la comunicazione formale di autorizzazione resa

dal delegato deve indicare gli estremi del provvedimento di delega.

Come previsto dal par. 3.1.5. delle Linee Guida AgID, le uniche informazioni modificabili di una registrazione di protocollo sono quelle relative a:

- classificazione (titolo e classe);
- assegnazione interna all'amministrazione (per competenza o per conoscenza).

Le operazioni di modifica posso essere svolte dal personale addetto alla protocollazione, anche senza previa autorizzazione del Responsabile.

L'annullamento e le modifiche avvengono in modo da consentire di mantenere traccia di ogni operazione, così come richiesto dalla normativa.

26. Segnatura di protocollo

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa, come indicate all'art. 53, comma 1, TUDA.

Le operazioni di segnatura sono effettuate contemporaneamente alla registrazione di protocollo o ad altra registrazione cui il documento è soggetto.

I requisiti necessari di ciascuna segnatura di protocollo sono:

a. indicazione della Amministrazione mittente;
b. codice identificativo dell'AOO mittente;
c. codice identificativo del registro;
d. numero progressivo di protocollo;
e. data di registrazione;
f. oggetto del messaggio di protocollo;
g. classificazione del messaggio di protocollo;
h. indicazione del fascicolo in cui è inserito il messaggio di protocollo.

Per i documenti informatici trasmessi ad altre Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file XML conforme alle indicazioni previste dall'Allegato 6 alle Linee guida dell'AgID.

27. Documenti soggetti a registrazione particolare

- CORRISPONDENZA RISERVATA

La corrispondenza personale indirizzata al dipendente va evidenziata con l'apposizione della dicitura "personale" o "riservata" sulla busta chiusa. Conseguentemente la busta va consegnata integra direttamente al destinatario, il quale valuterà l'opportunità di sottoporre il documento alla registrazione.

- FAX

I documenti ricevuti tramite fax sono giuridicamente validi ai sensi dell'art. 45 del D.

Lgs 82/2005 e s.m.i. e vanno quindi protocollati e la segnatura viene effettuata sulla prima pagina del documento; sull'eventuale originale cartaceo ricevuto per posta ordinaria deve essere apposto lo stesso numero e data di protocollo del corrispondente documento anticipato via fax.

- DOCUMENTI INFORMATICI E POSTA ELETTRONICA CERTIFICATA

I documenti informatici inviati con posta elettronica certificata, quelli sottoscritti con firma elettronica, quelli inviati alla casella istituzionale dell'ente, del settore o del responsabile del procedimento, sono soggetti a registrazione di protocollo utilizzando le funzioni del sistema che prevedono l'indicazione del mezzo di trasmissione e l'esplicitazione che si tratta di un documento originale digitale, come specificato nei manuali tecnici del sistema di protocollo.

Il Responsabile di Settore o il responsabile del procedimento amministrativo valuta comunque l'opportunità di registrare il documento in funzione della rilevanza dello stesso per l'attività amministrativa dell'Ente.

- DOCUMENTI INERENTI A GARE D'APPALTO

La corrispondenza riportante l'indicazione "*offerta*", "*gara d'appalto*", "*concorso*" o simili o comunque dalla cui confezione si evinca la partecipazione ad una gara, non viene aperta, ma viene protocollata in arrivo con l'apposizione del numero di protocollo, della data e dell'ora di arrivo direttamente sulla busta (plico o simili).

28. Registro di emergenza

Il responsabile del servizio di protocollo informatico autorizza lo svolgimento delle operazioni di registrazione di protocollo sull'apposito registro di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema.

Il registro di emergenza è unico ed è gestito dall'Ufficio Protocollo. Tutti i servizi comunali, in caso di necessità, fanno quindi riferimento a questo ufficio per ottenere l'assegnazione di un numero di protocollo di emergenza, in entrata o in uscita.

Il registro di emergenza si rinnova ogni anno solare, pertanto inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Si applicano le seguenti modalità di registrazione e di recupero dei dati:

- sul registro di emergenza sono riportate le cause, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;
- per ogni giornata di registrazione in emergenza è riportato sul registro il numero totale di operazioni registrate;
- la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO;
- le informazioni relative ai documenti protocollati in emergenza sono inserite immediatamente nel sistema di protocollo informatico ripristinato;
- durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, annotando nella

scheda di protocollo gli elementi necessari a mantenere stabilmente la correlazione univoca con il numero attribuito in emergenza.

29. Disposizioni sulla protocollazione di documenti analogici

Il personale addetto a effettuare la registrazione di protocollo informatica in entrata è competente anche per la protocollazione dei documenti analogici in entrata (consegnati a mano o pervenuti tramite servizio postale). Di tale documentazione è effettuata una copia per immagine su supporto informatico (scansione in formato pdf/A) prima della registrazione.

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è cura del personale del Servizio di Protocollo rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal protocollo informatico. La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo riporta i seguenti dati:

- il numero e la data di protocollo;
- l'indicazione dell'AOO;
- il mittente;
- l'oggetto;
- numero e descrizione degli allegati se presenti;
- l'indicazione del Responsabile dell' UO e Responsabile del Procedimento Amministrativo cui è assegnato il documento per competenza;
- l'operatore di protocollo che ha effettuato la registrazione.

Qualora per ragioni organizzative o tecniche non sia possibile protocollare immediatamente il documento, l'addetto al protocollo comunica al mittente o ad altra persona incaricata il termine entro il quale il documento verrà protocollato, impegnandosi – se richiesto – a far pervenire la ricevuta all'indirizzo o recapito indicato dal mittente stesso (anche tramite e-mail). La ricevuta può essere altresì ritirata dall'interessato o da persona espressamente delegata nei giorni successivi.

Classificazione e fascicolazione

30. Classificazione dei documenti

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (Titolario – Allegato 3).

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.

Il Titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza di leggi o regolamenti.

Le modifiche al Titolario sono apportate con provvedimento esplicito della funzione di governo dell'amministrazione.

La revisione anche parziale del Titolario viene proposta dal RSP quando necessaria e opportuna.

Dopo ogni modifica del Titolario, il Responsabile del protocollo provvede a informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a fornire loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Viene garantita la storicizzazione delle variazioni di Titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli digitali e dei documenti con la struttura del Titolario vigente al momento della produzione degli stessi.

Per ogni modifica di una voce, viene riportata la data di introduzione e la data di variazione. Le variazioni sono di norma introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo Titolario, e valgono almeno per l'intero anno.

Il titolario adottato dall'amministrazione è composto da 2 livelli. Le voci di primo e secondo livello (titoli e classi) individuano le funzioni primarie e di organizzazione dell'ente.

I titoli e le classi sono già forniti nel sistema informatico di protocollo e gestione documentale.

I successivi livelli di classificazione (macro-fascicoli, fascicoli, sotto-fascicoli…) corrispondono a specifiche competenze che rientrano concettualmente nelle macrofunzioni descritte dai primi livelli.

Le operazioni di classificazione vengono generalmente svolte in momenti diversi e da personale differente.

I primi due livelli di classificazione (titolo-classe) vengono attribuiti nella fase di protocollazione; l'individuazione dei successivi livelli (macro-fascicolo, fascicolo, sotto-fascicolo digitale...) è invece generalmente demandata al Responsabile del

procedimento o suo incaricato.

Tutti i documenti ricevuti e prodotti dall'Ente, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario.

31. Fascicolazione informatica dei documenti

I documenti ricevuti e prodotti dall'Ente sono raccolti in fascicoli costituiti in modo che ciascuno rappresenti l'insieme ordinato dei documenti riferiti ad uno stesso procedimento amministrativo o, comunque, ad una stessa pratica.

I fascicoli sono informatici e sono costituiti con le regole espresse come sopra, contengono pertanto tutta la documentazione originale della pratica prodotta in formato elettronico e le copie per immagine dei documenti cartacei.

I Responsabili dei singoli uffici interni dell'AOO forniscono le indicazioni operative per la gestione dei fascicoli e assicurano che la costituzione dei fascicoli avvenga secondo modalità uniformi, sia per quanto riguarda i criteri da adottare per la denominazione della pratica al fine di identificare il fascicolo in modo univoco che di quelli adottati per la descrizione del fascicolo.

I fascicoli informatici devono recare i metadati obbligatori delle aggregazioni documentali previsti nell'allegato 5 alle Linee guida AgID.

Il fascicolo informatico deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo;
3. codice IPA Amministrazione titolare (campo "Ruolo");
4. codice IPA Amministrazioni partecipanti (campo "Ruolo");
5. dati identificativi del RUP (nome, cognome, codice IPA dell'Amministrazione di appartenenza, domicilio digitale).

Flussi documentali interni

32. Assegnazione dei documenti in entrata agli uffici

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate. In particolare, sono automaticamente assegnati alle UO Responsabili preventivamente individuate i documenti provenienti dai portali dei servizi online (SUAP, SUE, ecc.) e le fatture provenienti dal Sistema Di Interscambio (SDI). Ulteriori criteri di assegnazione automatica sono definiti dal Responsabile, sentite le UOR interessate.

I documenti non assegnati automaticamente sono assegnati alle UO Responsabili dal personale addetto alla protocollazione in base all'oggetto del documento e alla classificazione. Quando un documento è di interesse anche per più UOR, si provvede a più assegnazioni, sia "per competenza" che "per conoscenza".

Lo scambio di documenti tra il Servizio di Gestione Documentale e le diverse UOR del Comune è effettuato per mezzo di posta elettronica. Lo scambio di documenti tra le UOR del Comune non richiede la protocollazione del messaggio. Scambi di documenti tra gli uffici possono essere effettuati anche attraverso rete intranet e cartelle condivise. In ogni caso, nelle attività di trasmissione e scambio dei documenti tutto il personale deve utilizzare esclusivamente gli strumenti di comunicazione messi a disposizione dal Comune.

33. Comunicazioni interne

Tutte le comunicazioni interne sono effettuate esclusivamente in modalità telematiche, ivi compresa la pubblicazione di avvisi e comunicazioni a carattere informativo.

Le comunicazioni personali sono trasmesse a mezzo posta elettronica ordinaria. Quando la comunicazione indirizzata a più destinatari, in ragione del contenuto e degli invii multipli, potrebbe comportare la divulgazione di dati personali, il mittente provvedea invii individuali o in copia conoscenza nascosta (ccn).

34. Pubblicazioni nell'Albo pretorio

Tutti gli atti prodotti dal Comune che, ai sensi della normativa vigente, sono soggetti a pubblicazione nell'Albo pretorio online dell'ente, sono trasmessi per la pubblicazione in modo automatizzato solo dopo che il documento sia divenuto immodificabile. Gli atti oggetto di notificazione tramite pubblicazione ai sensi del codice di procedura civile, una volta ricevuti e scansionati, sono inseriti manualmente dal personale abilitato.

PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI

35. Piano di conservazione dell'archivio

Il Comune di Coniolo, per la conservazione dei documenti informatici e degli altri oggetti della conservazione, si avvale del sistema di conservazione di un conservatore esterno ai sensi dell'art. 44, comma 1-quater, CAD.

Le attività affidate al Conservatore sono puntualmente indicate nella convenzione per l'affidamento del servizio.

Per la descrizione delle attività del processo di conservazione non definite nel presente Manuale, così come consentito dal par. 4.6 delle Linee Guida, è fatto rinvio alle disposizioni contenute nel CAD nonché agli ulteriori documenti tecnici concernenti l'affidamento del serviziodi conservazione.

36. Responsabile della conservazione

È compito del Responsabile assicurare il rispetto della normativa vigente da parte del Conservatore e degli obblighi contrattuali dallo stesso assunti, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile agisce d'intesa conil RPD dell'ente.

Il Responsabile, sotto la propria responsabilità, può delegare in tutto o in parte una o più attività di propria competenza relative alla conservazione, affidandole a soggetti interni all'ente dotati di adeguate competenze. Gli atti di delega devono individuare le specifiche attività e funzioni delegate.

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, 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;

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 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;

m) predispone il manuale di conservazione in collaborazione con il Conservatore e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

37. Oggetti e formati della conservazione

Gli oggetti della conservazione sono:

- i documenti informatici formati dal Comune e i rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- i fascicoli informatici e rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- il registro del protocollo informatico generale e giornaliero;
- gli altri registri e repertori tenuti dall'ente.

Gli oggetti della conservazione sono trattati dal sistema di conservazione del Conservatore in pacchetti informativi che si distinguono in:

a) pacchetti di versamento;
b) pacchetti di archiviazione;
c) pacchetti di distribuzione.

Il Responsabile provvede ad associare a ogni pacchetto di versamento almeno i seguenti metadati:

1. identificativo univoco e persistente del pacchetto di versamento;
2. riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
3. denominazione del soggetto responsabile della produzione del pacchetto;
4. impronta del pacchetto di versamento;
5. numero dei documenti compresi nel pacchetto.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie di documentarie oggetto del servizio di conservazione sono dettagliatamente descritte nel Manuale del Conservatore.

I dati e i documenti informatici sono memorizzati nel Sistema di gestione documentale, che provvede all'archiviazione su server cloud qualificato dall'AgID ai sensi della normativa vigente.

I formati ammessi per la conservazione sono individuati nell'allegato 2 alle Linee guida dell'AgID.

All'inizio di ogni anno i responsabili del procedimento individuano i fascicoli che sono da versare nell'archivio di deposito in quanto relativi ad affari o procedimenti conclusi o comunque non più necessari allo svolgimento delle attività correnti.

38. Archiviazione e conservazione digitale dei documenti informatici

Per la conservazione dei propri documenti informatici e delle loro aggregazioni documentali con i metadati a essi associati, il comune si attiene a quanto disposto dal conservatore accreditato esterno che cura la gestione, l'accessibilità e le operazioni di scarto dell'archivio digitale dell'ente, secondo le normative di legge e le modalità indicate dal Manuale della conservazione.

39. Selezione e scarto archivistico

In base al piano di conservazione adottato, sarà cura del Responsabile produrre periodicamente l'elenco dei documenti e dei fascicoli sui quali, trascorso il periodo obbligatorio di conservazione, previa comunicazione al Responsabile della gestione documentale, è possibile operare lo scarto.

L'elenco di scarto è prodotto secondo il modulo predisposto dalla Soprintendenza archivistica e a questa inviato per la necessaria autorizzazione, ai sensi dell'art. 21, comma 5 del D.Lgs 490/1999.

40. Misure di sicurezza e monitoraggio

Il Manuale di conservazione e il piano della sicurezza descrivono le modalità con cui il Conservatore assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello

sviluppo) e le procedure adottate per garantire i *backup* degli archivi e il *Disaster recovery*.

Il Conservatore provvede altresì al periodico monitoraggio al fine di verificare lo stato delle componenti infrastrutturali del sistema e l'integrità degli archivi.

Il Responsabile vigila affinché il Conservatore provveda alla conservazione integrata dei documenti, dei fascicoli e dei metadati associati nelle fasi di gestione e di conservazione. A tal fine, con cadenza almeno annuale, richiede al Conservatore l'esibizione di un campione di documenti o fascicoli.

Nel caso siano riscontrate irregolarità, provvede a sollecitare il Conservatore affinché vi ponga rimedio, anche attraverso gli strumenti previsti nell'atto di affidamento del servizio.

PARTE SESTA – MISURE DI SICUREZZA E PROTEZIONE DEI DATI PERSONALI

41. Piano di sicurezza informatica

La sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici archiviati sono garantiti dall'applicazione informatica adottata dall'Ente.

Il piano di sicurezza informatica del sistema informativo dell'amministrazione è definito dall'organizzazione dell'Ente che gestisce il sistema informatico generale.

A tale fine l'Ente definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui alla Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale*, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni* (di cui all'Allegato 7 "Modulo misure minime di sicurezza" al presente Manuale);
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il Responsabile della gestione documentale ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza prestabilita durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo in caso di disastro;
- conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;

- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal Responsabile della gestione documentale e dal titolare dei dati e, ove previsto, dalle forze dell'ordine.

42. Credenziali di accesso al sistema documentale

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di gestione documentale e protocollo informatico nel rispetto di modalità prestabilite.

Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).

Gli utenti del programma di gestione documentale e protocollo, in base alle rispettive competenze, dispongono di autorizzazioni di accesso differenziate.

Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente pubblica che permette l'identificazione dell'utente da parte del sistema (userID), e da una componente privata o riservata di autenticazione (password);
- una autorizzazione di accesso (profilo) che limita le operazioni di protocollo, gestione documentale e workflow effettuabili alle sole funzioni necessarie.

La visibilità normalmente attribuita ad un utente si limita alla documentazione relativa ai servizi di competenza. La visibilità su altri documenti può essere attribuita dal responsabile della pratica o del procedimento.

L’accesso diretto alla banca dati, l’inserimento di nuovi utenti, la modifica dei diritti e le impostazioni sui documenti sono consentiti esclusivamente agli amministratori del sistema.

I diversi livelli di autorizzazione sono assegnati agli utenti dal RSP, in base alle indicazioni fornite dai Responsabili dei servizi di appartenenza.

Gli accessi esterni a documenti, dati e informazioni non divulgabili sono subordinati alla registrazione sul sistema e al possesso di apposite credenziali, rilasciate previa identificazione diretta da parte di un dipendente abilitato.

Gli accessi esterni a documenti, dati e informazioni divulgabili sono consentiti anche senza autenticazione all'accesso, garantendo comunque il diritto alla riservatezza e all'oblio, e la tutela dei dati personali in conformità alle disposizioni vigenti.

Gli accessi esterni vengono di norma gestiti attraverso il sito web dell'Ente. I dati in libera consultazione vengono esposti in formato aperto (con dovute eccezioni, indotte anche da considerazioni di carattere tecnico, organizzativo o gestionale) che ne consentano il riutilizzo.

43. Trattamento dei dati personali

Ai fini dell’applicazione della normativa sul trattamento dei dati personali, in relazione al ruolo funzionale svolto, gli addetti all’ufficio protocollo sono nominati incaricati dal designato al Trattamento dei dati per il trattamento dei dati personali in ambito di Banche dati informatizzate e cartacee inerenti alla gestione del flusso documentale della corrispondenza in arrivo e in partenza.

È disponibile un’area di sistema interna e condivisa tra tutti i Responsabili designati al trattamento dei dati personali, come previsto dal Regolamento Europeo n. 679/2016 e decreti attuativi, aggiornata in tempo reale contenente sia i registri di trattamento che dell’accesso agli atti e dell’attività, anche in linea con le direttive del Segretario Generale, nonché secondo appositi modelli predisposti ai sensi di legge.

Al seguente link del sito istituzionale è disponibile l’informativa in ordine al trattamento dei dati personali: “Informativa email ai sensi e per gli effetti di cui all’articolo 13 ed all’articolo 14 del Regolamento (UE) 2016/679 (GDPR)” https://www.comune.coniolo.al.it

44. Piano formativo del personale

In conformità a quanto disposto dall’art. 13 del D.lgs. 82/2005, ai fini di una corretta gestione dell’intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, l’Ente predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del Sistema di Gestione Informatica dei Documenti;
- fascicolazione dei documenti informatici;

- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione in materia di protezione dei dati personali;
- aggiornamento sui temi suddetti.

Periodicamente è cura del Responsabile rilevare necessità formative in accordo con i vari responsabili di settore, ed effettuare dei controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della catena documentale e sull'utilizzo di un unico registro informatico, verificando, attraverso controlli nei vari uffici, la classificazione e la fascicolazione archivistica nonché le modalità di gestione dei documenti informatici.

45. Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

Il fornitore del software di gestione documentale controlla giornalmente i log di sistema e li mantiene per 6 mesi, al fine di verificare eventuali violazioni del Sistema.

Il Responsabile della gestione documentale dell'ente effettua periodiche verifiche sul corretto funzionamento del sistema di gestione informatica dei documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti alla gestione documentale.

PARTE SETTIMA - NORME TRANSITORIE E FINALI

46. Modalità di approvazione e aggiornamento del manuale

Il Manuale sarà aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevata nello svolgimento delle attività correnti;
- modifiche apportate negli allegati dal Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi.

Il Manuale viene approvato con deliberazione della Giunta comunale su proposta del Responsabile della gestione documentale.

47. Pubblicità del manuale

Il presente Manuale, ai sensi della normativa vigente, è reso disponibile alla consultazione del pubblico mediante pubblicazione nel sito internet dell'Amministrazione, all'indirizzo http://www.comune.coniolo.al.it nell'Area "Amministrazione trasparente" sezione Regolamenti Area Amministrativa.

Inoltre, copia del presente Manuale:

a) è resa disponibile a tutto il personale dell'Amministrazione mediante la rete intranet ed internet;

b) è inviata, per opportuna conoscenza, alla Soprintendenza Archivistica.

48. Entrata in vigore

Il presente documento diviene efficace al conseguimento dell'eseguibilità della deliberazione di approvazione.

Cod. 850365.d
Grafiche E. Gaspari

Allegato 1

Area organizzativa omogenea del Comune di Coniolo

Responsabile della gestione documentale: Arles Garelli

Vicario: Daria Patrucco

Glossario dei termini e degli acronimi

Glossario dei termini

TERMINE	DEFINIZIONE
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.

TERMINE	DEFINIZIONE
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un *wrapper* (codifica), così come di estrarli da esso (decodifica).
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo

TERMINE	DEFINIZIONE
	adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato.
Digest	Vedi Impronta crittografica.
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
eSeal	Vedi sigillo elettronico.
Esibizione	operazione che consente di visualizzare un documento conservato
eSignature	Vedi firma elettronica.
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.

TERMINE	DEFINIZIONE
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di *bit* che può essere elaborata da una procedura informatica.
Fascicolo informatico	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.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
File container	Vedi Formato contenitore.
File wrapper	Vedi Formato contenitore.
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS.
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS.
Flusso (binario)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o *wrapping*), in uno stesso file, di una o più

TERMINE	DEFINIZIONE
	evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
Funzione di *hash* crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.

TERMINE	DEFINIZIONE
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Naming convention	Vedi Convenzioni di denominazione
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.

TERMINE	DEFINIZIONE
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di file (*file package*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
Path	Percorso (*vedi*).
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano della sicurezza del sistema di gestione Informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.

TERMINE	DEFINIZIONE
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
qSeal	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
qSignature	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

TERMINE	DEFINIZIONE
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Responsabile del servizio di conservazione	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della funzione archivistica di conservazione	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.

TERMINE	DEFINIZIONE
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
***Sidecar* (file)**	File-manifesto (*vedi*).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito

TERMINE	DEFINIZIONE
	della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazionedei documenti informatici, al fine di fruire delle informazioni di interesse.
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Glossario degli Acronimi

ACRONIMO	DEFINIZIONE
AGID	Agenzia per l'Italia digitale

ACRONIMO	DEFINIZIONE
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
eIDAS	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
FEA	Vedi firma elettronica avanzata.
FEQ	Vedi firma elettronica qualifica.
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("*General Data Protection Regulation*"), 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.
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
UOR	Unità Organizzativa Responsabile

Allegato 3
Titolario

Il Comune di Coniolo adotta la classificazione esplicitata nel titolario allegato al presente manuale, comunicato alla Soprintendenza Archivistica competente per territorio.

Allegato 4
Livelli di abilitazione

Nome Daria

Cognome Patrucco

Area Amministrativa/Ragioneria

Livello di abilitazione: Consultazione – Gestione – Amministrazione

Modalità di accesso alle procedure: Firma semplice – PIN – SPID/CNS/CIE

-

Nome Luigi

Cognome Birocco

Area Tecnica/Tributi

Livello di abilitazione: Consultazione – Gestione – Amministrazione

Modalità di accesso alle procedure: Firma semplice – PIN – SPID/CNS/CIE

-

Nome Arles

Cognome Garelli

Area Amministrativa

Livello di abilitazione: Consultazione – Gestione – Amministrazione

Modalità di accesso alle procedure: Firma semplice – PIN – SPID/CNS/CIE

-

Nome Sante

Cognome Palmieri

Area Segreteria/Personale/Affari generali

Livello di abilitazione: Consultazione – Gestione – Amministrazione

Modalità di accesso alle procedure: Firma semplice – PIN – SPID/CNS/CIE

-

Nome Samantha

Cognome Mutti

Area Amministrativa/Ragioneria

Livello di abilitazione: Consultazione – Gestione – Amministrazione

Modalità di accesso alle procedure: Firma semplice – PIN – SPID/CNS/CIE

1. METADATI DEL DOCUMENTO INFORMATICO

Definizione del metadato IdDoc (element xsd: IdDoc)

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 da:

- 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

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Impronta crittografica del documento					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	NO, ma ridefinito

Definizione del metadato Modalità di formazione (element xsd: ModalitaDiFormazione)

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare: 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.	Alfanumerico	SI	SI

Definizione del metadato Tipologia documentale (element xsd: TipologiaDocumentale)

Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Metadato testuale libero per indicare le tipologie documentali trattate (ad esempio, fatture, delibere, determine, etc)	Alfanumerico	SI	SI

Definizione del metadato Dati di registrazione (element xsd: DatiDiRegistrazione)

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 campi:

- 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.
- Codice Registro: Identificativo del registro nel caso in cui il tipo registro sia protocollo ordinario/ protocollo emergenza, o Repertorio/Registro.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipologia di flusso	• "U" = In uscita • "E" = In entrata • "I" = Interno	Alfanumerico	SI	SI
Tipo registro	• Nessuno, • Protocollo Ordinario/Protocollo Emergenza • Repertorio/Registro	Alfanumerico	SI	SI

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Data registrazione	nel caso di documento non protocollato: • Data di registrazione del Documento/Ora di registrazione del Documento nel caso di documento protocollato: • Data di registrazione di protocollo/Ora di protocollazione del Documento	Date/Time	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
Codice Registro	Codice identificativo del registro in cui il documento viene registrato.	Alfanumerico	SI, nel caso in cui il tipo registro sia protocollo ordinario/protocollo emergenza, o Repertorio/Registro	SI

Definizione del metadato Soggetti (element xsd: Soggetti)

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. Al fine di renderei dati di registrazione univoci deve essere sempre indicato il Soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla). Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.
- 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 "Tracciature modifiche documento".
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento.

Il metadato ha una struttura ricorsiva.

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Ruolo		• Assegnatario • Autore • Destinatario • Mittente • Operatore • Produttore • RGD (Responsabile della Gestione Documentale) • RSP (Responsabile del Servizio di Protocollo) • Soggetto che effettua la registrazione • Altro	Alfanumerico	SI, al fine di rendere i dati di registrazione univoci deve essere sempre indicato il soggetto che effettua la registrazione del documento. Obbligatorio indicare inoltre almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente. Per "Operatore" si intende il soggetto autorizzato ad	NO, ma ridefinito

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
				apportare modifiche/ integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato “Tracciature modifiche documento”.	
Tipo soggetto		Se Ruolo = Assegnatario ✓ AS Se Ruolo = Soggetto che effettua la registrazione ✓ PF per Persona Fisica ✓ PG per Organizzazione Se Ruolo = Mittente o Destinatario o Altro ✓ PF per Persona Fisica ✓ PG per Organizzazione ✓ PAI per le Amministrazioni Pubbliche italiane (valido solo come mittente nei flussi in entrata, come destinatario nei flussi in uscita) ✓ PAE per le Amministrazioni Pubbliche estere (valido solo come mittente nei flussi in entrata, come destinatario nei flussi in uscita) Se Ruolo = Autore ✓ PF per Persona Fisica ✓ PG per Organizzazione ✓ PAI per le Amministrazioni Pubbliche italiane (valido solo nei flussi in entrata)	Alfanumerico	SI	SI

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		✓ PAE per le Amministrazioni Pubbliche estere (valido solo nei flussi in entrata) Se Ruolo = Operatore o Responsabile della Gestione Documentale o Responsabile del Servizio Protocollo ✓ PF per Persona Fisica Se Ruolo = Produttore ✓ SW per i documenti prodotti automaticamente			
	PF	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	
		Codice Fiscale	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PG	Denominazione Organizzazione	Alfanumerico	SI	SI
		Codice fiscale\Partita Iva	Alfanumerico	NO	
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PAI	Denominazione Amministrazione \ Codice IPA	Alfanumerico	SI	SI
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	NO	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PAE	Denominazione Amministrazione	Alfanumerico	SI	SI

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	AS	Cognome	Alfanumerico	NO	SI
		Nome	Alfanumerico	NO	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Organizzazione	Alfanumerico	SI	
		Denominazione Ufficio	Alfanumerico	SI	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	SW	Denominazione Sistema	Alfanumerico	SI	SI

Definizione del metadato Chiave descrittiva (element xsd: ChiaveDescrittiva)

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

- 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.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Oggetto	Testo libero	Alfanumerico	SI	SI
Parole chiave	Testo libero	Alfanumerico	NO	SI

Definizione del metadato Allegati (element xsd: Allegati)

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

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Numero allegati		Inserire un numero intero compreso tra 0 e 9999	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 del metadato Classificazione (element xsd: Classificazione)

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
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 del metadato Riservato (element xsd: Riservato)

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.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	• Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato	Boolean	SI	SI

Definizione del metadato Identificativo del formato (element xsd: IdentificativoDelFormato)

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

- 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

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

Definizione del metadato Verifica (element xsd: Verifica)

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

Campi	Valori Ammessi\	Tipo dato	Obbligatorietà	Nuova definizione
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 del metadato Identificativo dell'Aggregazione documentale (element xsd: Agg)

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

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

Definizione del metadato Identificativo del Documento Primario (element xsd: IdIdentificativoDocumentoPrimario)

Identificativo univoco e persistente del Documento primario.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	IdDoc del documento primario		SI, nel caso in cui sia presente un documento primario	SI

Definizione del metadato Nome del documento\file (element xsd: NomeDelDocumento)

Nome del documento\file così come riconosciuto all’esterno.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile		Alfanumerico	SI	SI

Definizione del metadato Versione del documento (element xsd: VersionedelDocumento)

Versione del documento.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare la versione del documento	Alfanumerico	SI	SI

Definizione del metadato Tracciature modifiche documento (element xsd: TracciatureModificheDocumento)

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".

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipo modifica	• Annullamento • Rettifica • Integrazione • Annotazione	Alfanumerico	SI, nel caso di versione > 1 o in caso di annullamento	SI
Soggetto autore della modifica	Come da ruolo = Operatore definito nel metadato Soggetti	Alfanumerico	SI, nel caso di versione > 1 o in caso di annullamento	SI
Data modifica/Ora modifica		Date/Time	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 del metadato Tempo di conservazione (element xsd: TempoDiConservazione)

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”.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare il numero di anni come da Piano di classificazione; Indicare 9999 per un tempo di conservazione perenne	Numerico	NO	SI

Definizione del metadato Note (element xsd: Note)

Eventuali indicazioni aggiuntive utili ad indicare situazioni particolari.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Testo Libero	Alfanumerico	NO	SI

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" type="DocumentoInformaticoType"/>
                  <xs:complexType name="DocumentoInformaticoType">
                        <xs:sequence>
                              <xs:element name="IdDoc" type="IdDocType"/>
                              <xs:element name="ModalitaDiFormazione" type="ModalitaDiFormazioneType"/>
                              <xs:element name="TipologiaDocumentale" type="xs:string" />
                              <xs:element name="DatiDiRegistrazione" type="DatiDiRegistrazioneType"/>
                              <xs:element name="Soggetti" type="SoggettiType"/>
                              <xs:element name="ChiaveDescrittiva" type="ChiaveDescrittivaType"/>
                              <xs:element name="Allegati" type="AllegatiType"/>
                              <xs:element name="Classificazione" type="ClassificazioneType" minOccurs="0"/>
                              <xs:element name="Riservato" type="xs:boolean" />
                              <xs:element name="IdentificativoDelFormato" type="IdentificativoDelFormatoType"/>
                              <xs:element name="Verifica" type="VerificaType"/>
                              <xs:element name="Agg" type="AggType"/>
                              <xs:element name="IdIdentificativoDocumentoPrimario" type="IdDocType" minOccurs="0"/>
                              <xs:element name="NomeDelDocumento" type="xs:string" />
                              <xs:element name="VersioneDelDocumento" type="xs:string" />
                              <xs:element     name="TracciatureModificheDocumento"     type="TracciatureModificheDocumentoType"
minOccurs="0" />
                              <xs:element name="TempoDiConservazione" type="TempoDiConservazioneType" minOccurs="0"/>
                              <xs:element name="Note" type="xs:string" minOccurs="0" />
                        </xs:sequence>
                  </xs:complexType>
```

```
        <xs:complexType name="IdDocType">
                        <xs:sequence>
                                <xs:element                                                     name="ImprontaCrittograficaDelDocumento"
type="ImprontaCrittograficaDelDocumentoType" />
                                <xs:element name="Identificativo" type="xs:string" />
                        </xs:sequence>
        </xs:complexType>
                                        <xs:complexType name="ImprontaCrittograficaDelDocumentoType">
                                                <xs:sequence>
                                                        <xs:element name="Impronta" type="xs:base64Binary" />
                                                        <xs:element name="Algoritmo" type="xs:string" default="SHA-256"/>
                                                </xs:sequence>
                                        </xs:complexType>

                <xs:simpleType name="ModalitaDiFormazioneType">
                        <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:complexType name="DatiDiRegistrazioneType">
```

```
                        <xs:sequence>
                                <xs:element name="TipologiaDiFlusso" type="TipologiaDiFlussoType"/>
                                <xs:element name="TipoRegistro" type="TipoRegistroType"/>
                        </xs:sequence>
                </xs:complexType>

                        <xs:simpleType name="TipologiaDiFlussoType">
                                <xs:restriction base="xs:string">
                                        <xs:enumeration value="E"/>
                                        <xs:enumeration value="U"/>
                                        <xs:enumeration value="I"/>
                                </xs:restriction>
                        </xs:simpleType>

                        <xs:complexType name="TipoRegistroType">
                                <xs:sequence>
                                        <xs:choice>
                                                <xs:element name="Nessuno" type="NoRegistroType"/>
                                                <xs:element                             name="ProtocolloOrdinario_ProtocolloEmergenza"
type="ProtocolloType"/>
                                                <xs:element name="Repertorio_Registro" type="NoProtocolloType"/>
                                        </xs:choice>
                                </xs:sequence>
                        </xs:complexType>

                                        <xs:complexType name="NoRegistroType">
                                                <xs:sequence>
                                                  <xs:element name="TipoRegistro" type="xs:string" fixed = 'Nessuno'/>
                                                        <xs:element name="DataDocumento" type="xs:date"/>
                                                        <xs:element name="OraDocumento" type="xs:time" minOccurs="0"/>
```

```
                                        <xs:element name="NumeroDocumento" type="xs:string" />
                                    </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="ProtocolloType">
                                    <xs:sequence>
                                    <xs:element name="TipoRegistro" type="xs:string" fixed =
'ProtocolloOrdinario\ProtocolloEmergenza'/>
                                        <xs:element name="DataProtocollazioneDocumento" type="xs:date"/>
                                        <xs:element name="OraProtocollazioneDocumento" type="xs:time"
minOccurs="0"/>
                                        <xs:element name="NumeroProtocolloDocumento" type="NumProtType"/>
                                        <xs:element name="CodiceRegistro" type="CodiceRegistroType"/>
                                    </xs:sequence>
                                </xs:complexType>

        <xs:complexType name="NoProtocolloType">
                                        <xs:sequence>
                <xs:element name="TipoRegistro" type="xs:string" fixed = 'Repertorio\Registro'/>
                                        <xs:element name="DataRegistrazioneDocumento" type="xs:date"/>
                                        <xs:element name="OraRegistrazioneDocumento" type="xs:time"
minOccurs="0"/>
                                        <xs:element name="NumeroRegistrazioneDocumento" type="xs:string"/>
                                        <xs:element name="CodiceRegistro" type="CodiceRegistroType"/>
                                    </xs:sequence>
                                </xs:complexType>

                                  <xs:simpleType name="NumProtType">
                                        <xs:restriction base="xs:string">
                                                                <xs:pattern value="[0-9]{7,}"/>
```

```
                                        </xs:restriction>
                                    </xs:simpleType>

        <xs:simpleType name="CodiceRegistroType">
                <xs:restriction base="xs:string">
                        <xs:pattern value="[A-Za-z0-9_\.\-]{1,16}"/>
                </xs:restriction>
        </xs:simpleType>

<xs:complexType name="SoggettiType">
                <xs:sequence>
                        <xs:element name="Ruolo" type="RuoloType" minOccurs="1" maxOccurs="unbounded"/>
                </xs:sequence>
</xs:complexType>

                  <xs:complexType name="RuoloType">
                        <xs:choice>
          <xs:element name="SoggettoCheEffettuaLaRegistrazione" type="TipoSoggetto21Type"/>
          <xs:element name="Assegnatario" type="TipoSoggetto22Type"/>
          <xs:element name="Destinatario" type="TipoSoggetto11Type"/>
          <xs:element name="Mittente"     type="TipoSoggetto12Type"/>
          <xs:element name="Autore" type="TipoSoggetto31Type"/>
          <xs:element name="Operatore" type="TipoSoggetto32Type"/>
          <xs:element name="ResponsabileGestioneDocumentale" type="TipoSoggetto33Type"/>
          <xs:element name="ResponsabileServizioProtocollo" type="TipoSoggetto34Type"/>
          <xs:element name="Produttore" type="TipoSoggetto4Type"/>
          <xs:element name="Altro" type="TipoSoggetto13Type"/>
                                </xs:choice>
                  </xs:complexType>
```

```
                    <xs:complexType name="TipoSoggetto11Type">
                        <xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Destinatario'/>
                            <xs:choice>
                                <xs:element name="PF" type="PFType"/>
                                <xs:element name="PG" type="PGType"/>
                                <xs:element name="PAI" type="PAIType"/>
                                <xs:element name="PAE" type="PAEType"/>
                            </xs:choice>
                        </xs:sequence>
                    </xs:complexType>

                    <xs:complexType name="TipoSoggetto12Type">
                        <xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Mittente'/>
                            <xs:choice>
                                <xs:element name="PF" type="PFType"/>
                                <xs:element name="PG" type="PGType"/>
                                <xs:element name="PAI" type="PAIType"/>
                                <xs:element name="PAE" type="PAEType"/>
                            </xs:choice>
                        </xs:sequence>
                    </xs:complexType>

                <xs:complexType name="TipoSoggetto13Type">
                        <xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Altro'/>
                            <xs:choice>
                                <xs:element name="PF" type="PFType"/>
                                <xs:element name="PG" type="PGType"/>
```

```
                                                <xs:element name="PAI" type="PAIType"/>
                                                <xs:element name="PAE" type="PAEType"/>
                                        </xs:choice>
                                </xs:sequence>
                        </xs:complexType>

                        <xs:complexType name="TipoSoggetto21Type">
                                <xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Soggetto Che Effettua La Registrazione'/>
                                        <xs:choice>
                                                <xs:element name="PF" type="PFType"/>
                                                <xs:element name="PG" type="PGType"/>
                                        </xs:choice>
                                </xs:sequence>
                        </xs:complexType>

                <xs:complexType name="TipoSoggetto22Type">
                                <xs:sequence>
                                <xs:element name="TipoRuolo" type="xs:string" fixed = 'Assegnatario'/>
                                <xs:element name="AS" type="ASType"/>
                                </xs:sequence>
                        </xs:complexType>

                        <xs:complexType name="ASType" >
                                        <xs:sequence>
         <xs:element name="Cognome" type="xs:string" minOccurs="0"/>
         <xs:element name="Nome" type="xs:string" minOccurs="0" />
         <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
        <xs:element name="DenominazioneOrganizzazione" type="xs:string" />
                                        <xs:element name="DenominazioneUfficio" type="xs:string" />
```

```
                                                    <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
                                        </xs:complexType>


      <xs:complexType name="TipoSoggetto31Type">
                                            <xs:sequence>
         <xs:element name="TipoRuolo" type="xs:string" fixed = 'Autore'/>
                                                <xs:choice>
                                                    <xs:element name="PF" type="PFType"/>
                                                    <xs:element name="PG" type="PGType"/>
                                                    <xs:element name="PAI" type="PAIType"/>
                                                    <xs:element name="PAE" type="PAEType"/>
                                                </xs:choice>
                                            </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="TipoSoggetto32Type">
                                            <xs:sequence>
               <xs:element name="TipoRuolo" type="xs:string" fixed = 'Operatore'/>
                                                                    <xs:element name="PF" type="PFType"/>
                                            </xs:sequence>
                                        </xs:complexType>

                                            <xs:complexType name="TipoSoggetto33Type">
                                            <xs:sequence>
               <xs:element name="TipoRuolo" type="xs:string" fixed = 'Responsabile della Gestione Documentale'/>
                                                                    <xs:element name="PF" type="PFType"/>
                                            </xs:sequence>
```

```
</xs:complexType>
```

```
                                        <xs:complexType name="TipoSoggetto34Type">
                                        <xs:sequence>
            <xs:element name="TipoRuolo" type="xs:string" fixed = 'Responsabile del Servizio di Protocollo'/>
                                                                        <xs:element name="PF" type="PFType"/>
                                        </xs:sequence>
                                    </xs:complexType>

                                    <xs:complexType name="TipoSoggetto4Type">
                                        <xs:sequence>
          <xs:element name="TipoRuolo" type="xs:string" fixed = 'Produttore'/>
                                                        <xs:element name="SW" type="SWType"/>
                                        </xs:sequence>
                                    </xs:complexType>

                                        <xs:complexType name="PFType">
                                            <xs:sequence>
                                                <xs:element name="Cognome" type="xs:string" />
                                                <xs:element name="Nome" type="xs:string" />
                                                <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
                                                <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                            </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="PGType">
                                            <xs:sequence>
                                                <xs:element                  name="DenominazioneOrganizzazione"
type="xs:string" />
```

```
                                                <xs:element      name="CodiceFiscale_PartitaIva"      type="PIType"
minOccurs="0"/>
                                                <xs:element      name="DenominazioneUfficio"      type="xs:string"
minOccurs="0" />
                                                <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                        </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="PAIType" >
                                        <xs:sequence>
                                                <xs:element name="IPAAmm" type="CodiceIPAType" />
                                                <xs:element name="IPAAOO" type="CodiceIPAType" minOccurs="0"
/>
                                                <xs:element          name="IPAUOR"          type="CodiceIPAType"
minOccurs="0"/>
                                                <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                                </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="PAEType" >
                                 <xs:sequence>
                                                <xs:element                  name="DenominazioneAmministrazione"
type="xs:string"/>
                                                <xs:element      name="DenominazioneUfficio"      type="xs:string"
minOccurs="0"/>
                                                <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                        </xs:sequence>
        </xs:complexType>
```

```
                                        <xs:complexType name="CodiceIPAType" >
                                                <xs:sequence>
                                                        <xs:element name="Denominazione" type="xs:string" />
                                                        <xs:element name="CodiceIPA" type="xs:string" />
                                                </xs:sequence>
                                        </xs:complexType>

                                <xs:complexType name="SWType">
                                        <xs:sequence>
                                                <xs:element name="DenominazioneSistema" type="xs:string" />
                                        </xs:sequence>
                                </xs:complexType>

<xs:complexType name="ChiaveDescrittivaType">
        <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:complexType name="AllegatiType">
        <xs:sequence>
                <xs:element name="NumeroAllegati" type="NumeroAllegatiType" />
                <xs:element name="IndiceAllegati" type="IndiceAllegatiType" minOccurs="0" maxOccurs="9999" />
        </xs:sequence>
</xs:complexType>

        <xs:simpleType name="NumeroAllegatiType">
                <xs:restriction base="xs:integer">
```

```
                        <xs:minInclusive value="0"/>
                        <xs:maxInclusive value="9999"/>
                    </xs:restriction>
                </xs:simpleType>

                <xs:complexType name="IndiceAllegatiType">
                    <xs:sequence>
                        <xs:element name="IdDoc" type="IdDocType" />
                        <xs:element name="Descrizione" type="xs:string" />
                    </xs:sequence>
                </xs:complexType>

        <xs:complexType name="ClassificazioneType">
                <xs:sequence>
                        <xs:element name="IndiceDiClassificazione" type="xs:string"  minOccurs="0" />
                        <xs:element name="Descrizione" type="xs:string"  minOccurs="0" />
                        <xs:element name="PianoDiClassificazione" type="xs:string" minOccurs="0" />
                </xs:sequence>
        </xs:complexType>

        <xs:complexType name="IdentificativoDelFormatoType">
                <xs:sequence>
                        <xs:element name="Formato" type="xs:string" />
                        <xs:element name="ProdottoSoftware" type="ProdottoSoftwareType" minOccurs="0"/>
                </xs:sequence>
        </xs:complexType>

                <xs:complexType name="ProdottoSoftwareType">
                    <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:complexType name="VerificaType">
        <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:complexType name="AggType">
                <xs:sequence>
                        <xs:element name="TipoAgg" type="IdAggType" minOccurs="0" maxOccurs="unbounded"/>
                </xs:sequence>
</xs:complexType>

<xs:complexType name="IdAggType">
        <xs:sequence>
                <xs:element name="TipoAggregazione" type="TipoAggregazioneType"/>
                <xs:element name="IdAggregazione" type="xs:string" />
        </xs:sequence>
</xs:complexType>

        <xs:simpleType name="TipoAggregazioneType">
                <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:complexType name="TracciatureModificheDocumentoType">
                        <xs:sequence>
                                <xs:element name="TipoModifica" type="TipoModificaType"/>
                                <xs:element name="SoggettoAutoreDellaModifica" type="PFType" />
                                <xs:element name="DataModifica" type="xs:date"/>
                                <xs:element name="OraModifica" type="xs:time" minOccurs="0"/>
                                <xs:element name="IdDocVersionePrecedente" type="IdDocType"/>
                        </xs:sequence>
                </xs:complexType>

                        <xs:simpleType name="TipoModificaType">
                                <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:simpleType name="CFType">
                                        <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:simpleType name="PIType">
                                <xs:restriction base="xs:string">
                                        <xs:pattern value="\d{11}"/>
                                </xs:restriction>
                        </xs:simpleType>

        <xs:simpleType name="TempoDiConservazioneType">
                <xs:restriction base="xs:integer">
                        <xs:minInclusive value="1"/>
                        <xs:maxInclusive value="9999"/>
                </xs:restriction>
        </xs:simpleType>
</xs:schema>
```

2. METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO

Definizione del metadato IdDoc (element xsd: IdDoc)

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 campi:

- 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"
- Identificativo: come da sistema di identificazione formalmente definito
- Segnatura: segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida.

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
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
Identificativo		Come da sistema di identificazione formalmente definito	Alfanumerico	SI	
Segnatura		Segnatura del protocollo	Alfanumerico	SI, nel caso di documento protocollato	

Definizione del metadato Modalità di formazione (element xsd: ModalitaDiFormazione)

Indica la modalità di generazione del documento amministrativo 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.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee; 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	Alfanumerico	SI	SI

Definizione del metadato Tipologia documentale (element xsd: TipologiaDocumentale)

Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Metadato testuale libero per indicare le tipologie documentali trattate (ad esempio, fatture, delibere, determine, etc)	Alfanumerico	SI	SI

Definizione del metadato Dati di registrazione (element xsd: DatiDiRegistrazione)

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

Sono previsti i seguenti campi:

- 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.
- Codice Registro: Identificativo del registro in cui il documento viene registrato.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipologia di flusso	• "U" = In uscita • "E" = In entrata • "I" = 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/Ora di registrazione del Documento nel caso di documento protocollato: • Data di registrazione di protocollo/Ora di protocollazione del Documento	Date/Time	SI	NO, ma ridefinito

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
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
Codice Registro	Codice identificativo del registro in cui il documento viene registrato.	Alfanumerico	SI	SI

Definizione del metadato Soggetti (element xsd: Soggetti)

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. Al fine di renderei dati di registrazione univoci deve essere sempre indicata l'Amministrazione che effettua la registrazione del documento. Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente. 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 "Tracciature modifiche documento". Nel caso di ruolo Assegnatario si prevede l'indicazione della UOR di riferimento con l'indicazione, a completamento, della persona fisica. Nel caso di ruolo RUP le informazioni relative alla persona fisica e alla UOR di appartenenza diventano obbligatorie.
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento.

Il metadato ha una struttura ricorsiva.

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Ruolo		• Amministrazione che effettua la registrazione • Assegnatario • Autore • Destinatario • Mittente • Operatore • Produttore • RGD (Responsabile della Gestione Documentale) • RSP (Responsabile del Servizio di Protocollo) • RUP	Alfanumerico	SI, al fine di rendere i dati di registrazione univoci deve essere sempre indicata l'Amministrazione che effettua la registrazione del documento. Obbligatorio indicare inoltre almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente. Per "Operatore" si intende il	NO ma ridefinito

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
				soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato “Tracciature modifiche documento”. Nel caso di ruolo Assegnatario si prevede l’indicazione sia della persona fisica che, a complemento o in alternativa, della relativa UOR di riferimento. Nel caso di ruolo = RUP le informazioni relative alla persona fisica e alla UOR di appartenenza diventano obbligatorie.	
Tipo soggetto		Se Ruolo = Assegnatario ✓ AS Se Ruolo = Amministrazione che effettua la registrazione ✓ PAI per le Amministrazioni Pubbliche italiane Se Ruolo = Mittente o Destinatario ✓ PF per Persona Fisica ✓ PG per Organizzazione ✓ PAI per le Amministrazioni Pubbliche Italiane	Alfanumerico	SI	SI

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		✓ PAE per le Amministrazioni Pubbliche Estere Se Ruolo = Autore ✓ PF per Persona Fisica ✓ PG per Organizzazione (valido solo nei flussi in entrata) ✓ PAI per le Amministrazioni Pubbliche italiane ✓ PAE per le Amministrazioni Pubbliche Estere (valido solo nei flussi in entrata) Se Operatore o Responsabile della Gestione Documentale o Responsabile del Servizio Protocollo ✓ PF per Persona Fisica Se Ruolo = RUP ✓ RUP Se Ruolo = Produttore ✓ SW per i documenti prodotti automaticamente			
	PF	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	Obbligatorio solo se si è indicato l'AOO o l'UOR	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	Obbligatorio solo se si è indicato l'Amministrazione o l'UOR	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	NO	

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PG	Denominazione Organizzazione	Alfanumerico	SI	SI
		Codice fiscale\Partita Iva	Alfanumerico	NO	
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PAI	Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	SI
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	PAE	Denominazione Amministrazione	Alfanumerico	SI	SI
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	AS	Cognome	Alfanumerico	NO	SI
		Nome	Alfanumerico	NO	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	SI	

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	RUP	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	SI	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	SW	Denominazione Sistema	Alfanumerico	SI	SI

Definizione del metadato Chiave descrittiva (element xsd: ChiaveDescrittiva)

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

- 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.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Oggetto	Testo libero	Alfanumerico	SI	SI
Parole chiave	Testo libero	Alfanumerico	NO	SI

Definizione del metadato Allegati (element xsd: Allegati)

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

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Numero allegati		Inserire un numero intero compreso tra 0 e 9999	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 del metadato Classificazione (element xsd: Classificazione)

Classificazione del documento secondo il Piano di classificazione utilizzato, da indicare 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
- Descrizione: Descrizione per esteso dell'Indice di classificazione indicato.
- Piano di classificazione: riportare l'URI di pubblicazione del Piano di classificazione

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
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	NO	SI

Definizione del metadato Riservato (element xsd: Riservato)

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.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	• Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato	Boolean	SI	SI

Definizione del metadato Identificativo del formato (element xsd: IdentificativoDelFormato)

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

- 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

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

Definizione del metadato Verifica (element xsd: Verifica)

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
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 del metadato Identificativo dell'Aggregazione documentale (element xsd: Agg)

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Identificativo del fascicolo o della serie come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE.	Alfanumerico	SI	SI

Definizione del metadato Identificativo del Documento Primario (element xsd: IdIdentificativoDocumentoPrimario)

Identificativo univoco e persistente del Documento primario.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	IdDoc del documento primario		SI, nel caso in cui sia presente un documento primario	SI

Definizione del metadato Nome del documento\file (element xsd: NomeDelDocumento)

Nome del documento\file così come riconosciuto all'esterno.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile		Alfanumerico	SI	SI

Definizione del metadato Versione del documento (element xsd: VersioneDelDocumento)

Versione del documento

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare la versione del documento	Alfanumerico	SI	SI

Definizione del metadato Tracciature modifiche documento (element xsd: TracciatureModificheDocumento)

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".

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipo modifica	• Annullamento • Rettifica • Integrazione • Annotazione	Alfanumerico	SI, nel caso di versione > 1 o in caso di annullamento	SI
Soggetto autore della modifica	Come da ruolo = Operatore definito nel metadato Soggetti	Alfanumerico	SI, nel caso di versione > 1 o in caso di annullamento	SI
Data modifica/Ora modifica		Date/Time	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 del metadato Tempo di conservazione (element xsd: TempoDiConservazione)

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”.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare il numero di anni come da Piano di classificazione; indicare 9999 per un tempo di conservazione perenne	Numerico	NO	SI

Definizione del metadato Note (element xsd: Note)

Eventuali indicazioni aggiuntive utili ad indicare situazioni particolari.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Testo Libero	Alfanumerico	NO	SI

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" type="DocumentoAmministrativoInformaticoType"/>
          <xs:complexType name="DocumentoAmministrativoInformaticoType">
                        <xs:sequence>
                                <xs:element name="IdDoc" type="IdDocType"/>
                                <xs:element name="ModalitaDiFormazione" type="ModalitaDiFormazioneType"/>
                                <xs:element name="TipologiaDocumentale" type="xs:string" />
                                <xs:element name="DatiDiRegistrazione" type="DatiDiRegistrazioneType"/>
                                <xs:element name="Soggetti" type="SoggettiType"/>
                                <xs:element name="ChiaveDescrittiva" type="ChiaveDescrittivaType"/>
                                <xs:element name="Allegati" type="AllegatiType"/>
                                <xs:element name="Classificazione" type="ClassificazioneType"/>
                                <xs:element name="Riservato" type="xs:boolean" />
                                <xs:element name="IdentificativoDelFormato" type="IdentificativoDelFormatoType"/>
                                <xs:element name="Verifica" type="VerificaType"/>
                                <xs:element name="Agg" type="AggType"/>
                                <xs:element name="IdIdentificativoDocumentoPrimario" type="IdDocType" minOccurs="0"/>
                                <xs:element name="NomeDelDocumento" type="xs:string" />
                                <xs:element name="VersioneDelDocumento" type="xs:string" />
                                <xs:element      name="TracciatureModificheDocumento"      type="TracciatureModificheDocumentoType"
minOccurs="0" />
                                <xs:element name="TempoDiConservazione" type="TempoDiConservazioneType" minOccurs="0"/>
                                <xs:element name="Note" type="xs:string" minOccurs="0" />
                        </xs:sequence>
```

```
        </xs:complexType>
        <xs:complexType name="IdDocType">
                        <xs:sequence>
                                <xs:element                                                     name="ImprontaCrittograficaDelDocumento"
type="ImprontaCrittograficaDelDocumentoType" />
                                <xs:element name="Identificativo" type="xs:string" />
                                <xs:element name="Segnatura" type="xs:string" minOccurs="0" />
                        </xs:sequence>
        </xs:complexType>
                                        <xs:complexType name="ImprontaCrittograficaDelDocumentoType">
                                                <xs:sequence>
                                                        <xs:element name="Impronta" type="xs:base64Binary" />
                                                        <xs:element name="Algoritmo" type="xs:string" default="SHA-256"/>
                                                </xs:sequence>
                                        </xs:complexType>
        <xs:simpleType name="ModalitaDiFormazioneType">
                <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:complexType name="DatiDiRegistrazioneType">
                <xs:sequence>
```

```
                        <xs:element name="TipologiaDiFlusso" type="TipologiaDiFlussoType"/>
                        <xs:element name="TipoRegistro" type="TipoRegistroType"/>
                </xs:sequence>
        </xs:complexType>
                                <xs:simpleType name="TipologiaDiFlussoType">
                                        <xs:restriction base="xs:string">
                                        <xs:enumeration value="E"/>
                                        <xs:enumeration value="U"/>
                                        <xs:enumeration value="I"/>
                                        </xs:restriction>
                                </xs:simpleType>
                                <xs:complexType name="TipoRegistroType">
                                        <xs:sequence>
                                                <xs:choice>
                                                        <xs:element                     name="ProtocolloOrdinario_ProtocolloEmergenza"
type="ProtocolloType"/>
                                                        <xs:element name="Repertorio_Registro" type="NoProtocolloType"/>
                                                </xs:choice>
                                        </xs:sequence>
                                </xs:complexType>
                                        <xs:complexType name="ProtocolloType">
                                                <xs:sequence>
                                                <xs:element          name="TipoRegistro"          type="xs:string"          fixed          =
'ProtocolloOrdinario\ProtocolloEmergenza'/>
                                                        <xs:element name="DataProtocollazioneDocumento" type="xs:date"/>
                                                        <xs:element        name="OraProtocollazioneDocumento"        type="xs:time"
minOccurs="0"/>
                                                        <xs:element name="NumeroProtocolloDocumento" type="NumProtType"/>
                                                        <xs:element name="CodiceRegistro" type="CodiceRegistroType"/>
                                                </xs:sequence>
```

```
                                        </xs:complexType>
                                        <xs:complexType name="NoProtocolloType">
                                                <xs:sequence>
                                           <xs:element name="TipoRegistro" type="xs:string" fixed = 'Repertorio\Registro'/>
                                                        <xs:element name="DataRegistrazioneDocumento" type="xs:date"/>
                                                        <xs:element        name="OraRegistrazioneDocumento"        type="xs:time"
minOccurs="0"/>
                                                        <xs:element name="NumeroRegistrazioneDocumento" type="xs:string"/>
                                                        <xs:element name="CodiceRegistro" type="CodiceRegistroType"/>
                                                </xs:sequence>
                                        </xs:complexType>
                                                <xs:simpleType name="NumProtType">
                                                                        <xs:restriction base="xs:string">
                                                                                                <xs:pattern value="[0-9]{7,}"/>
                                                                        </xs:restriction>
                                                        </xs:simpleType>
                                <xs:simpleType name="CodiceRegistroType">
                                        <xs:restriction base="xs:string">
                                                <xs:pattern value="[A-Za-z0-9_\.\-]{1,16}"/>
                                        </xs:restriction>
                                </xs:simpleType>

                                <xs:complexType name="SoggettiType">
                                <xs:sequence>
                                        <xs:element name="Ruolo" type="RuoloType" minOccurs="1" maxOccurs="unbounded"/>
                                </xs:sequence>
                                </xs:complexType>

                                 <xs:complexType name="RuoloType">
                                        <xs:choice>
```

```
            <xs:element name="AmministrazioneCheEffettuaLaRegistrazione" type="TipoSoggetto1Type"/>
            <xs:element name="Assegnatario" type="TipoSoggetto2Type"/>
            <xs:element name="Destinatario" type="TipoSoggetto31Type"/>
            <xs:element name="Mittente"          type="TipoSoggetto32Type"/>
            <xs:element name="Autore" type="TipoSoggetto41Type"/>
            <xs:element name="Operatore" type="TipoSoggetto42Type"/>
            <xs:element name="ResponsabileGestioneDocumentale" type="TipoSoggetto43Type"/>
            <xs:element name="ResponsabileServizioProtocollo" type="TipoSoggetto44Type"/>
            <xs:element name="Produttore" type="TipoSoggetto5Type"/>
            <xs:element name="RUP" type="TipoSoggetto6Type"/>
                                    </xs:choice>
                                </xs:complexType>

                                <xs:complexType name="TipoSoggetto1Type">
                                        <xs:sequence>
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Amministrazione Che Effettua
La Registrazione'/>
                                        <xs:element name="PAI" type="PAIType"/>
                                        </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="TipoSoggetto2Type">
                                        <xs:sequence>
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Assegnatario'/>
                                        <xs:element name="AS" type="ASType"/>
                                        </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="TipoSoggetto31Type">
                                        <xs:sequence>
```

```
                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Destinatario'/>
                                <xs:choice>
                                        <xs:element name="PF" type="PFType"/>
                                        <xs:element name="PG" type="PGType"/>
                                        <xs:element name="PAI" type="PAIType"/>
                                        <xs:element name="PAE" type="PAEType"/>
                                </xs:choice>
                        </xs:sequence>
                </xs:complexType>

        <xs:complexType name="TipoSoggetto32Type">
                        <xs:sequence>
                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Mittente'/>
                                <xs:choice>
                                        <xs:element name="PF" type="PFType"/>
                                        <xs:element name="PG" type="PGType"/>
                                        <xs:element name="PAI" type="PAIType"/>
                                        <xs:element name="PAE" type="PAEType"/>
                                </xs:choice>
                        </xs:sequence>
        </xs:complexType>

        <xs:complexType name="TipoSoggetto41Type">
                        <xs:sequence>
                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Autore'/>
                                <xs:choice>
                                        <xs:element name="PF" type="PFType"/>
                                        <xs:element name="PG" type="PGType"/>
                                        <xs:element name="PAI" type="PAIType"/>
                                        <xs:element name="PAE" type="PAEType"/>
```

```
                                        </xs:choice>
                                </xs:sequence>
                        </xs:complexType>

                                <xs:complexType name="TipoSoggetto42Type">
                                        <xs:sequence>
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Operatore'/>
                                                        <xs:element name="PF" type="PFType"/>
                                        </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="TipoSoggetto43Type">
                                        <xs:sequence>
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Responsabile della Gestione
Documentale'/>
                                                        <xs:element name="PF" type="PFType"/>
                                        </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="TipoSoggetto44Type">
                                        <xs:sequence>
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Responsabile del Servizio di
Protocollo'/>
                                                        <xs:element name="PF" type="PFType"/>
                                        </xs:sequence>
                                </xs:complexType>


                                <xs:complexType name="TipoSoggetto5Type">
                                        <xs:sequence>
```

```
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Produttore'/>
                                                <xs:element name="SW" type="SWType"/>
                                        </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="TipoSoggetto6Type">
                                        <xs:sequence>
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'RUP'/>
                                                <xs:element name="RUP" type="RUPType"/>
                                        </xs:sequence>
                                </xs:complexType>

                                        <xs:complexType name="ASType" >
                                                <xs:sequence>
        <xs:element name="Cognome" type="xs:string" minOccurs="0"/>
        <xs:element name="Nome" type="xs:string" minOccurs="0" />
        <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
        <xs:element name="IPAAmm" type="CodiceIPAType" />
        <xs:element name="IPAAOO" type="CodiceIPAType" />
        <xs:element name="IPAUOR" type="CodiceIPAType" />
        <xs:element name="IndirizziDigitaliDiRiferimento" type="xs:string" minOccurs="1" maxOccurs="unbounded"/>
</xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="RUPType" >
                                        <xs:sequence>
                                                <xs:element name="Cognome" type="xs:string" />
                                                <xs:element name="Nome" type="xs:string" />
                                                <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
                                        <xs:element name="IPAAmm" type="CodiceIPAType" />
```

```
                                        <xs:element name="IPAAOO" type="CodiceIPAType"  />
                                        <xs:element name="IPAUOR" type="CodiceIPAType" />
                                        <xs:element        name="IndirizziDigitaliDiRiferimento"        type="xs:string"
minOccurs="1"    maxOccurs="unbounded"/>
                                </xs:sequence>
                        </xs:complexType>

                        <xs:complexType name="PFType" >
                                <xs:sequence>
                                        <xs:element name="Cognome" type="xs:string" />
                                        <xs:element name="Nome" type="xs:string" />
                                        <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
                                <xs:element name="IPAAmm" type="CodiceIPAType" minOccurs="0"/>
                                        <xs:element name="IPAAOO" type="CodiceIPAType" minOccurs="0" />
                                        <xs:element name="IPAUOR" type="CodiceIPAType" minOccurs="0"/>
                                        <xs:element        name="IndirizziDigitaliDiRiferimento"        type="xs:string"
minOccurs="0"    maxOccurs="unbounded"/>
                                </xs:sequence>
                        </xs:complexType>

                                <xs:complexType name="PGType">
                                        <xs:sequence>
                                                <xs:element name="DenominazioneOrganizzazione" type="xs:string"
/>
                                                <xs:element      name="CodiceFiscale_PartitaIva"      type="PIType"
minOccurs="0"/>
                                                <xs:element       name="DenominazioneUfficio"       type="xs:string"
minOccurs="0" />
                                                <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                        </xs:sequence>
```

```
                                        </xs:complexType>

                                        <xs:complexType name="PAIType" >
                                                <xs:sequence>
                                                        <xs:element name="IPAAmm" type="CodiceIPAType" />
                                                        <xs:element name="IPAAOO" type="CodiceIPAType" />
                                                        <xs:element          name="IPAUOR"          type="CodiceIPAType"
minOccurs="0"/>
                                                        <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="1" maxOccurs="unbounded"/>
                                                        </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="PAEType" >
                                          <xs:sequence>
                                                        <xs:element                  name="DenominazioneAmministrazione"
type="xs:string"/>
                                                        <xs:element      name="DenominazioneUfficio"      type="xs:string"
minOccurs="0"/>
                                                <xs:element    name="IndirizziDigitaliDiRiferimento"    type="xs:string"    minOccurs="1"
maxOccurs="unbounded"/>
                                                </xs:sequence>
                </xs:complexType>


                                                <xs:complexType name="CodiceIPAType" >
                                                        <xs:sequence>
                                                                <xs:element name="Denominazione" type="xs:string" />
                                                                <xs:element name="CodiceIPA" type="xs:string" />
                                                        </xs:sequence>
                                                </xs:complexType>
```

```
                                        <xs:complexType name="SWType">
                                                <xs:sequence>
                                                        <xs:element name="DenominazioneSistema" type="xs:string" />
                                                </xs:sequence>
                                        </xs:complexType>


<xs:complexType name="ChiaveDescrittivaType">
                <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:complexType name="AllegatiType">
                <xs:sequence>
                        <xs:element name="NumeroAllegati" type="NumeroAllegatiType" />
                        <xs:element name="IndiceAllegati" type="IndiceAllegatiType" minOccurs="0" maxOccurs="9999" />
                </xs:sequence>
        </xs:complexType>

                                <xs:simpleType name="NumeroAllegatiType">
                                        <xs:restriction base="xs:integer">
                                                <xs:minInclusive value="0"/>
                                                <xs:maxInclusive value="9999"/>
                                        </xs:restriction>
                                </xs:simpleType>

                                <xs:complexType name="IndiceAllegatiType">
```

```
                                        <xs:sequence>
                                                <xs:element name="IdDoc" type="IdDocType" />
                                                <xs:element name="Descrizione" type="xs:string" />
                                        </xs:sequence>
                                </xs:complexType>

<xs:complexType name="ClassificazioneType">
        <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:complexType name="IdentificativoDelFormatoType">
        <xs:sequence>
                <xs:element name="Formato" type="xs:string" />
                <xs:element name="ProdottoSoftware" type="ProdottoSoftwareType" minOccurs="0"/>
        </xs:sequence>
</xs:complexType>

                                <xs:complexType name="ProdottoSoftwareType">
                                        <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:complexType name="VerificaType">
```

```
            <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:complexType name="AggType">
                                    <xs:sequence>
                                                <xs:element name="TipoAgg" type="IdAggType" minOccurs="1" maxOccurs="unbounded"/>
                                    </xs:sequence>
            </xs:complexType>

            <xs:complexType name="IdAggType">
            <xs:sequence>
                        <xs:element name="TipoAggregazione" type="TipoAggregazioneType"/>
                        <xs:element name="IdAggregazione" type="xs:string" />
            </xs:sequence>
</xs:complexType>

                        <xs:simpleType name="TipoAggregazioneType">
                                    <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:complexType name="TracciatureModificheDocumentoType">
```

```
            <xs:sequence>
                <xs:element name="TipoModifica" type="TipoModificaType"/>
                <xs:element name="SoggettoAutoreDellaModifica" type="PFType" />
                <xs:element name="DataModifica" type="xs:date"/>
                <xs:element name="OraModifica" type="xs:time" minOccurs="0"/>
                <xs:element name="IdDocVersionePrecedente" type="IdDocType"/>
            </xs:sequence>
        </xs:complexType>

                <xs:simpleType name="TipoModificaType">
                    <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:simpleType name="CFType">
                                        <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:simpleType name="PIType">
                                        <xs:restriction base="xs:string">
                                            <xs:pattern value="\d{11}"/>
                                        </xs:restriction>
                                    </xs:simpleType>
```

```
        <xs:simpleType name="TempoDiConservazioneType">
                <xs:restriction base="xs:integer">
                        <xs:minInclusive value="1"/>
                        <xs:maxInclusive value="9999"/>
                </xs:restriction>
        </xs:simpleType>

</xs:schema>
```

3. METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE

Definizione del metadato Identificativo dell'Aggregazione documentale (element xsd: IdAgg)

L' Identificativo dell'Aggregazione documentale 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 di 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.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
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 del metadato Tipologia fascicolo (element xsd: TipologiaFascicolo)

I fascicoli sono organizzati 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.
- 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.
- persona fisica: comprende 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, costituendo serie aperte.
- persona giuridica: comprende 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, costituendo serie aperte
- procedimento amministrativo: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
NON Applicabile	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 del metadato Soggetti (element xsd: Soggetti)

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
  - Assegnatario
  - Soggetto intestatario persona fisica
  - Soggetto intestatario persona giuridica
  - RUP: da indicare solo in caso di TipoAggregazione = 'Fascicolo'
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere) in funzione del Ruolo. Per ogni tipo soggetto sono indicati i metadati di riferimento. Nel caso in cui sia stato definito un Ruolo=RUP è obbligatorio indicare anche l'UOR corrispondente.

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Ruolo		• Amministrazione titolare • Amministrazioni partecipanti • Assegnatario • Soggetto intestatario persona fisica • Soggetto intestatario persona giuridica • RUP Da indicare solo in caso di TipoAggregazione = 'Fascicolo'	Alfanumerico	SI	SI

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipo soggetto		Se Ruolo = Amministrazione titolare ✓ PAI per le Amministrazioni Pubbliche italiane Se Ruolo = Amministrazioni partecipanti ✓ PAI per le Amministrazioni Pubbliche italiane ✓ PAE per le Amministrazioni Pubbliche estere Se Ruolo = Assegnatario ✓ AS Se Ruolo = Soggetto intestatario persona giuridica • PG per Organizzazione • PAI per le Amministrazioni Pubbliche Italiane • PAE per le Amministrazioni Pubbliche estere Se Ruolo = Soggetto intestatario persona fisica ✓ PF per Persona Fisica Se Ruolo = RUP ✓ RUP	Alfanumerico	SI	SI
	PF	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	
		Codice Fiscale	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PG	Denominazione Organizzazione	Alfanumerico	SI	SI
		Codice fiscale\Partita Iva	Alfanumerico	NO	
		Denominazione Ufficio	Alfanumerico	NO	

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PAI	Denominazione Amministrazione \ Codice IPA	Alfanumerico	SI	SI
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	PAE	Denominazione Amministrazione	Alfanumerico	SI	SI
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	AS	Cognome	Alfanumerico	NO	SI
		Nome	Alfanumerico	NO	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	SI	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	RUP	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	SI	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	

Definizione del metadato Assegnazione (element xsd: Assegnazione)

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
- Soggetto assegnatario
- Data inizio assegnazione
- Data fine assegnazione

Il metadato ha una struttura ricorsiva.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipo assegnazione	• Per competenza • Per conoscenza	Alfanumerico	SI, in caso di fascicolo	SI
Soggetto Assegnatario	Come da Ruolo = Assegnatario definito del metadato Soggetti.	Alfanumerico	SI, in caso di fascicolo	SI
Data inizio assegnazione / Ora inizio assegnazione	Data inizio assegnazione	Date/Time	SI, in caso di fascicolo	SI
Data fine assegnazione / Ora fine assegnazione	Data fine assegnazione	Date/Time	NO	SI

Definizione del metadato Data Apertura (element xsd: DataApertura)

Data di apertura dell'aggregazione documentale.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
NON Applicabile	Data di apertura dell'aggregazione documentale	Date	SI	SI

Definizione del metadato Classificazione (element xsd: Classificazione)

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
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	NO	SI

Definizione del metadato Progressivo (element xsd: Progressivo)

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
NON Applicabile		Numerico	SI	SI

Definizione del metadato Chiave descrittiva (element xsd: ChiaveDescrittiva)

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

- 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. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Oggetto	Testo libero	Alfanumerico	SI	SI
Parole chiave	Testo libero	Alfanumerico	NO	SI

Definizione del metadato DataChiusura (element xsd: DataChiusura)

Data di chiusura dell’aggregazione documentale.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
NON Applicabile	Data di chiusura dell’aggregazione documentale	Date	SI, quando l'aggregazione viene chiusa	SI

Definizione del metadato Procedimento Amministrativo (element xsd: ProcedimentoAmministrativo)

Metadato funzionale volto ad indicare il procedimento a cui il fascicolo afferisce, nonché lo stato di avanzamento e le relative fasi.

Il campo “Fase”, a sua volta costituito da “Tipo Fase”:

- Preparatoria
- Istruttoria
- Consultiva
- Decisoria o deliberativa
- Integrazione dell’efficacia

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

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
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.	NO
Fasi		A sua volta suddiviso, in una struttura ricorsiva:			

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
	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 del metadato Indice documenti (element xsd: IndiceDocumenti)

Elenco degli identificativi dei documenti contenuti nell'aggregazione, definiti secondo le regole indicate per i documenti informatici o i documenti amministrativi informatici. Metadato ricorsivo.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
Tipo documento	• documento amministrativo informatico • documento informatico		SI	NO, ma ridefinito
IdDoc	Se documento amministrativo informatico ✓ IdDoc come definito nel precedente paragrafo dei METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO Se documento informatico ✓ IdDoc come definito nel precedente paragrafo dei METADATI DEL DOCUMENTO INFORMATICO		SI	NO, ma ridefinito

Definizione del metadato Posizione fisica Aggregazione Documentale (element xsd: PosizioneFisicaAggregazioneDocumentale)

Posizione fisica dell'aggregazione. Nel caso di fascicoli ibridi indica la posizione della componente cartacea del fascicolo.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
NON Applicabile	Testo libero	Alfanumerico	SI, solo nel caso di fascicoli cartacei digitalizzati o di fascicoli ibridi	SI

Definizione del metadato Identificativo dell'Aggregazione Primaria (element xsd: IdAggPrimario)

Identificativo univoco e persistente del livello superiore di fascicolazione nel caso in cui si stia definendo un sottofascicolo o una sottoserie.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
NON Applicabile	Come da sistema di identificazione formalmente definito	Alfanumerico	NO	SI

Definizione del metadato Tempo di conservazione (element xsd: TempoDiConservazione)

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". Il dato, inizialmente non obbligatorio, deve essere indicato a fronte dell'indicazione della data di chiusura dell'aggregazione.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare il numero di anni come da Piano di classificazione; indicare 9999 per un tempo di conservazione perenne	Numerico	NO, obbligatorio se è indicata la data di chiusura	SI

Definizione del metadato Note (element xsd: Note)

Eventuali indicazioni aggiuntive utili ad indicare situazioni particolari.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
NON Applicabile	Testo Libero	Alfanumerico	NO	SI

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" type="AggregazioneDocumentaliInformaticheType"/>
	<xs:complexType name="AggregazioneDocumentaliInformaticheType">
		<xs:sequence>
			<xs:element name="IdAgg" type="IdAggType"/>
			<xs:element name="TipologiaFascicolo" type="TipologiaFascicoloType" minOccurs="0"/>
			<xs:element name="Soggetti" type="SoggettiType"/>
			<xs:element name="Assegnazione" type="AssegnazioneType"/>
			<xs:element name="DataApertura" type="xs:date"/>
			<xs:element name="Classificazione" type="ClassificazioneType"/>
			<xs:element name="Progressivo" type="ProgressivoType" />
			<xs:element name="ChiaveDescrittiva" type="ChiaveDescrittivaType"/>
			<xs:element name="DataChiusura" type="xs:date" minOccurs="0"/>
			<xs:element name="ProcedimentoAmministrativo" type="ProcedimentoAmministrativoType"
minOccurs="0" />
			<xs:element name="IndiceDocumenti" type="IndiceDocumentiType"/>
			<xs:element name="PosizioneFisicaAggregazioneDocumentale" type="xs:string" minOccurs="0" />
			<xs:element name="IdAggPrimario" type="IdAggType" minOccurs="0" />
			<xs:element name="TempoDiConservazione" type="TempoDiConservazioneType" minOccurs="0"/>
			<xs:element name="Note" type="xs:string" minOccurs="0" />
		</xs:sequence>
	</xs:complexType>

	<xs:complexType name="IdAggType">
		<xs:sequence>
			<xs:element name="TipoAggregazione" type="TipoAggregazioneType"/>
```

```
                        <xs:element name="IdAggregazione" type="xs:string" />
                </xs:sequence>
        </xs:complexType>

                        <xs:simpleType name="TipoAggregazioneType">
                                <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:simpleType name="TipologiaFascicoloType">
   <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:complexType name="SoggettiType">
                <xs:sequence>
                        <xs:element name="Ruolo" type="RuoloType" minOccurs="1" maxOccurs="unbounded"/>
                </xs:sequence>
        </xs:complexType>

                                <xs:complexType name="RuoloType">
```

```
                        <xs:choice>
                    <xs:element name="AmministrazioneTitolare" type="TipoSoggetto1Type" />
                    <xs:element name="AmministrazionePartecipante" type="TipoSoggetto6Type"/>
                    <xs:element name="SoggettoIntestatarioPersonaGiuridica" type="TipoSoggetto2Type"/>
                    <xs:element name="SoggettoIntestatarioPersonaFisica" type="TipoSoggetto3Type"/>
                    <xs:element name="RUP" type="TipoSoggetto4Type"/>
                    <xs:element name="Assegnatario" type="TipoSoggetto5Type"/>
                        </xs:choice>
                </xs:complexType>

                        <xs:complexType name="TipoSoggetto1Type">
                                <xs:sequence>
                                        <xs:element  name="TipoRuolo"  type="xs:string"  fixed  =  'Amministrazione
Titolare'/>
                                        <xs:element name="PAI" type="PAIType"></xs:element>
                                </xs:sequence>
                        </xs:complexType>

                        <xs:complexType name="TipoSoggetto6Type">
                                <xs:sequence>
                                <xs:element    name="TipoRuolo"    type="xs:string"    fixed    =    'Amministrazione
Partecipante'/>
                                        <xs:choice>
                                                <xs:element name="PAI" type="PAIType"/>
                                                <xs:element name="PAE" type="PAEType"/>
                                        </xs:choice>
                                </xs:sequence>
                        </xs:complexType>

                        <xs:complexType name="TipoSoggetto2Type">
```

```
                                        <xs:sequence>
                                                <xs:element name="TipoRuolo" type="xs:string" fixed = 'Soggetto Intestatario
Persona Giuridica'/>
                                                <xs:choice>
                                                        <xs:element name="PG" type="PGType"/>
                                                        <xs:element name="PAI" type="PAIType"/>
                                                        <xs:element name="PAE" type="PAEType"/>
                                                </xs:choice>
                                        </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="TipoSoggetto3Type">
                                        <xs:sequence>
                                                <xs:element name="TipoRuolo" type="xs:string" fixed = 'Soggetto Intestatario
Persona Fisica'/>
                                                <xs:choice>
                                                        <xs:element name="PF" type="PFType"/>
                                                </xs:choice>
                                        </xs:sequence>
                                </xs:complexType>

                                <xs:complexType name="TipoSoggetto4Type">
                                        <xs:sequence>
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'RUP'/>
                                                <xs:element name="RUP" type="RUPType"/>
                                        </xs:sequence>
                                </xs:complexType>

                                        <xs:complexType name="RUPType" >
                                                <xs:sequence>
```

```
                                                        <xs:element name="Cognome" type="xs:string" />
                                                        <xs:element name="Nome" type="xs:string" />
                                                        <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
                                                        <xs:element name="IPAAmm" type="CodiceIPAType" />
                                                        <xs:element name="IPAAOO" type="CodiceIPAType"  />
                                                        <xs:element name="IPAUOR" type="CodiceIPAType" />
                                                        <xs:element name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="1" maxOccurs="unbounded"/>
                                                </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="TipoSoggetto5Type">
                                                <xs:sequence>
                                                        <xs:element     name="TipoRuolo"     type="xs:string"     fixed     =
'Assegnatario'/>
                                                        <xs:element name="AS" type="ASType"/>
                                                </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="ASType" >
                                                        <xs:sequence>
                <xs:element name="Cognome" type="xs:string" minOccurs="0"/>
                <xs:element name="Nome" type="xs:string" minOccurs="0" />
                <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
                <xs:element name="IPAAmm" type="CodiceIPAType" />
                <xs:element name="IPAAOO" type="CodiceIPAType" />
                <xs:element name="IPAUOR" type="CodiceIPAType" />
                <xs:element name="IndirizziDigitaliDiRiferimento" type="xs:string" minOccurs="1" maxOccurs="unbounded"/>
        </xs:sequence>
                                        </xs:complexType>
```

```
                                        <xs:complexType name="PFType">
                                                <xs:sequence>
                                                        <xs:element name="Cognome" type="xs:string" />
                                                        <xs:element name="Nome" type="xs:string" />
                                                        <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
                                                        <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                                </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="PGType">
                                                <xs:sequence>
                                                        <xs:element name="DenominazioneOrganizzazione" type="xs:string"
/>
                                                        <xs:element      name="CodiceFiscale_PartitaIva"      type="PIType"
minOccurs="0" />
                                                        <xs:element      name="DenominazioneUfficio"      type="xs:string"
minOccurs="0" />
                                                        <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                                </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="PAIType" >
                                                <xs:sequence>
                                                        <xs:element name="IPAAmm" type="CodiceIPAType" />
                                                        <xs:element name="IPAAOO" type="CodiceIPAType" />
                                                        <xs:element          name="IPAUOR"          type="CodiceIPAType"
minOccurs="0"/>
```

```
                                                    <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="1" maxOccurs="unbounded"/>
                                                    </xs:sequence>
                                            </xs:complexType>

                                                <xs:complexType name="CodiceIPAType" >
                                                    <xs:sequence>
                                                        <xs:element name="Denominazione" type="xs:string" />
                                                        <xs:element name="CodiceIPA" type="xs:string" />
                                                    </xs:sequence>
                                                </xs:complexType>

                                            <xs:complexType name="PAEType" >
                                              <xs:sequence>
                                                    <xs:element                 name="DenominazioneAmministrazione"
type="xs:string"/>
                                                    <xs:element      name="DenominazioneUfficio"      type="xs:string"
minOccurs="0"/>
                                                    <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="1" maxOccurs="unbounded"/>
                                                </xs:sequence>
        </xs:complexType>


            <xs:complexType name="AssegnazioneType">
                    <xs:sequence>
                        <xs:element     name="TipoAssegnazione"     type="TipoAssegnazioneType"     minOccurs="0"
maxOccurs="unbounded"/>
                    </xs:sequence>
            </xs:complexType>

                    <xs:complexType name="TipoAssegnazioneType">
```

```
                                        <xs:choice>
                                <xs:element name="PerCompetenza" type="AssType"/>
                                <xs:element name="PerConoscenza" type="Ass1Type"/>
                                                </xs:choice>
                                        </xs:complexType>

                <xs:complexType name="AssType">
            <xs:sequence>
                                                                        <xs:element name="TipoAssegnazioneRuolo" type="xs:string" fixed
= 'Per Competenza'/>

              <xs:element name="SoggettoAssegnatario" type="ASType" />
                    <xs:element name="DataInizioAssegnazione" type="xs:date"/>
                    <xs:element name="OraInizioAssegnazione" type="xs:time" minOccurs="0"/>
                    <xs:element name="DataFineAssegnazione" type="xs:date" minOccurs="0"/>
                    <xs:element name="OraFineAssegnazione" type="xs:time" minOccurs="0"/>
            </xs:sequence>
          </xs:complexType>

                <xs:complexType name="Ass1Type">
            <xs:sequence>
                                                                        <xs:element name="TipoAssegnazioneRuolo" type="xs:string" fixed
= 'Per Conoscenza'/>

              <xs:element name="SoggettoAssegnatario" type="ASType" />
                    <xs:element name="DataInizioAssegnazione" type="xs:date"/>
                    <xs:element name="OraInizioAssegnazione" type="xs:time" minOccurs="0"/>
                    <xs:element name="DataFineAssegnazione" type="xs:date" minOccurs="0"/>
                    <xs:element name="OraFineAssegnazione" type="xs:time" minOccurs="0"/>
            </xs:sequence>
          </xs:complexType>
```

```
        <xs:complexType name="ClassificazioneType">
                <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:simpleType name="ProgressivoType">
                <xs:restriction base="xs:integer">
                        <xs:minInclusive value="1"/>
                        <xs:maxInclusive value="999999999"/>
                </xs:restriction>
        </xs:simpleType>

<xs:complexType name="ChiaveDescrittivaType">
                <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:complexType name="ProcedimentoAmministrativoType" >
   <xs:sequence>
      <xs:element name="MateriaArgomentoStruttura" type="xs:string" />
      <xs:element name="Procedimento" type="xs:string" />
      <xs:element name="CatalogoProcedimenti"  type="xs:string" minOccurs="0"/>
      <xs:element name="Fasi" type="FaseType" />
   </xs:sequence>
</xs:complexType>
```

```
    <xs:complexType name="FaseType">
      <xs:sequence>
                                        <xs:element      name="TipoFase"      type="TipoFaseType"      minOccurs="1"
maxOccurs="unbounded"/>
     </xs:sequence>
                 </xs:complexType>


                          <xs:complexType name="TipoFaseType">
                                        <xs:choice>
              <xs:element name="Preparatoria" type="TipoFase1Type"/>
              <xs:element name="Istruttoria" type="TipoFase2Type"/>
              <xs:element name="Consultiva" type="TipoFase3Type"/>
              <xs:element name="Decisoriaodeliberativa"     type="TipoFase4Type"/>
              <xs:element name="Integrazionedellefficacia" type="TipoFase5Type"/>
                                        </xs:choice>
                                    </xs:complexType>

       <xs:complexType name="TipoFase1Type">
                                                <xs:sequence>
                                                <xs:element name="Fase" type="xs:string" fixed = 'Preparatoria'/>
                                        <xs:element name="DataInizioFase" type="xs:date"/>
                                        <xs:element name="DataFineFase" type="xs:date" minOccurs="0"/>
                                                </xs:sequence>
                                        </xs:complexType>
       <xs:complexType name="TipoFase2Type">
                                                <xs:sequence>
                                                <xs:element name="Fase" type="xs:string" fixed = 'Istruttoria'/>
                                        <xs:element name="DataInizioFase" type="xs:date"/>
                                        <xs:element name="DataFineFase" type="xs:date" minOccurs="0"/>
```

```
                                        </xs:sequence>
                                    </xs:complexType>
    <xs:complexType name="TipoFase3Type">
                                        <xs:sequence>
                                        <xs:element name="Fase" type="xs:string" fixed = 'Consultiva'/>
                                    <xs:element name="DataInizioFase" type="xs:date"/>
                                    <xs:element name="DataFineFase" type="xs:date" minOccurs="0"/>
                                        </xs:sequence>
                                    </xs:complexType>
    <xs:complexType name="TipoFase4Type">
                                        <xs:sequence>
                                        <xs:element name="Fase" type="xs:string" fixed = 'Decisoria o deliberativa'/>
                                    <xs:element name="DataInizioFase" type="xs:date"/>
                                    <xs:element name="DataFineFase" type="xs:date" minOccurs="0"/>
                                        </xs:sequence>
                                    </xs:complexType>

   <xs:complexType name="TipoFase5Type">
                                        <xs:sequence>
                                        <xs:element name="Fase" type="xs:string" fixed = 'Integrazione dell'efficacia'/>
                                    <xs:element name="DataInizioFase" type="xs:date"/>
                                    <xs:element name="DataFineFase" type="xs:date" minOccurs="0"/>
                                        </xs:sequence>
                                    </xs:complexType>

            <xs:complexType name="IndiceDocumentiType">
                                <xs:sequence>
                                        <xs:element      name="TipoDocumento"      type="TipoDocumentoType"      minOccurs="1"
maxOccurs="unbounded"/>
                                </xs:sequence>
```

```
                </xs:complexType>

                                        <xs:complexType name="TipoDocumentoType">
                                                <xs:choice>
                                <xs:element name="DocumentoAmministativoinformatico" type="IdDoc_DAIType"/>
                                <xs:element name="Documentoinformatico" type="IdDoc_DIType"/>
                                                        </xs:choice>
                                        </xs:complexType>

                <xs:complexType name="IdDoc_DAIType">
                        <xs:sequence>
                                <xs:element                                                     name="ImprontaCrittograficaDelDocumento"
type="ImprontaCrittograficaDelDocumentoType" />
                                <xs:element name="Identificativo" type="xs:string" />
                                <xs:element name="Segnatura" type="xs:string" minOccurs="0" />
                        </xs:sequence>
        </xs:complexType>

                <xs:complexType name="IdDoc_DIType">
                                <xs:sequence>
                                <xs:element                                                     name="ImprontaCrittograficaDelDocumento"
type="ImprontaCrittograficaDelDocumentoType" />
                                <xs:element name="Identificativo" type="xs:string" />
                        </xs:sequence>
   </xs:complexType>

                                                <xs:complexType name="ImprontaCrittograficaDelDocumentoType">
                                                        <xs:sequence>
                                                                <xs:element name="Impronta" type="xs:base64Binary" />
                                                                <xs:element name="Algoritmo" type="xs:string" default="SHA-256"/>
```

```
                                        </xs:sequence>
                                    </xs:complexType>

                                                <xs:simpleType name="CFType">
                                            <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:simpleType name="PIType">
                                            <xs:restriction base="xs:string">
                                                <xs:pattern value="\d{11}"/>
                                            </xs:restriction>
                                        </xs:simpleType>

    <xs:simpleType name="TempoDiConservazioneType">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="1"/>
            <xs:maxInclusive value="9999"/>
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Numero Metadato	Metadato	N. Campo	Campi	Sottocampi	Valori	Obbligatorietà documento informatico	Valore metadato	Fase di associazione al documento	Modalità associazione
1	**IdDoc**	1.1	Impronta	Impronta	Rappresenta l'hash del documento	SI	Impronta base 64		
1	**IdDoc**	1.1	Impronta	Algoritmo	Rappresenta l'algoritmo applicato	SI	SHA-256		
1	**IdDoc**	1.2	Identificativo		Come da sistema di identificazione definito	SI	Identificativo SDI / Identificativo composto secondo le regole stabilite		
1	**IdDoc**	1.3	Segnatura del protocollo		Segnatura del protocollo	NO	NA		
2	**Modalità di formazione**	2.1	NON Applicabile		A) strumenti software (elettronico) B) via telematica (elettronico da mail) - Copia per immagine di un documento analogico (elettronico - copia conforme) C) Transazioni o processi informatici (es moduli somministrati ad utenti) (elettronico) D) Raggruppamento dati (elettronico)	SI	a		
3	**Tipologia documentale**	3.1	NON Applicabile		Testo libero per indicare le tipologie documentali trattate	SI	Fatture		
4	**Dati di registrazione**	4.1	Tipologia di flusso		E (entrata) / U(uscita) / I(interno)	SI	E/U/I		
4	**Dati di registrazione**	4.2	Tipo registro		Nessuno / Protocollo Ordinario-Protocollo Emergenza / Repertorio-Registro	SI	Nessuno		
4	**Dati di registrazione**	4.3	Data registrazione del documento/Ora di registrazione del documento (nel caso di documento protocollato Data/Ora di registrazione di protocollo)		Date/Time	SI	Data del documento in formato gg/mm/aaaa hh:mm:ss (esempio 31/12/2020 00:00:00)		
4	**Dati di registrazione**	4.4	Numero documento		Numero di registrazione del documento / Numero protocollo	SI	Numero fattura		

Numero Metadato	Metadato	N. Campo	Campi	Sottocampi	Valori	Obbligatorietà documento informatico	Valore metadato	Fase di associazione al documento	Modalità associazione
4	**Dati di registrazione**	4.5	Codice del Registro		Codice identificativo del registro in cui il documento viene registrato.	SI, nel caso in cui il tipo registro sia protocollo ordinario/protocollo emergenza, o Repertorio/Registro	Codice registro se esiste altrimenti vuoto		
5	**Soggetti**	5.1	Ruolo		• Amministrazione che effettua la registrazione • Assegnatario • Autore • Destinatario • Mittente • Operatore • Produttore • RGD (Responsabile della Gestione Documentale) • RSP (Responsabile del Servizio di Protocollo) • RUP	SI	Soggetto che effettua la registrazione Mittente Destinatario		

Numero Metadato	Metadato	N. Campo	Campi	Sottocampi	Valori	Obbligatorietà documento informatico	Valore metadato	Fase di associazione al documento	Modalità associazione
5	**Soggetti**	5.2	Tipo soggetto		Se Ruolo = **Assegnatario** • AS Se Ruolo = **Amministrazione che effettua la registrazione** • PAI per le Amministrazioni Pubbliche italiane Se Ruolo = **Mittente** o **Destinatario** • PF per Persona Fisica • PG per Organizzazione • PAI per le Amministrazioni Pubbliche Italiane • PAE per le Amministrazioni Pubbliche Estere Se Ruolo = **Autore** • PF per Persona Fisica • PG per Organizzazione (valido solo nei flussi in entrata) • PAI per le Amministrazioni Pubbliche italiane • PAE per le Amministrazioni Pubbliche Estere (valido solo nei flussi in entrata) Se **Operatore** o **Responsabile della Gestione Documentale o Responsabile del Servizio Protocollo** • PF per Persona Fisica Se Ruolo = **RUP** • RUP Se Ruolo = **Produttore** • SW per i documenti prodotti automaticamente	SI	PF PG PAI		

Numero Metadato	Metadato	N. Campo	Campi	Sottocampi	Valori	Obbligatorietà documento informatico	Valore metadato	Fase di associazione al documento	Modalità associazione
5	**Soggetti**	5.3		**PF:** • Cognome • Nome • Codice Fiscale • Denominazione Amministrazione\ Codice IPA • Denominazione Amministrazione AOO \ Codice IPA AOO • Denominazione Amministrazione UOR \ Codice IPA UOR • Indirizzi Digitali di Riferimento **PG:** • Denominazione Organizzazione • Codice fiscale\Partita Iva • Denominazione Ufficio • Indirizzi Digitali Di Riferimento **PAI:** • Denominazione Amministrazione \ Codice IPA • Denominazione Amministrazione AOO \ Codice IPA AOO • Denominazione Amministrazione UOR \ Codice IPA UOR • Indirizzi Digitali Di Riferimento **PAE:** • Denominazione Amministrazione • Denominazione Ufficio • Indirizzi Digitali Di Riferimento **AS:** • Cognome • Nome • Codice Fiscale • Denominazione Organizzazione • Denominazione Ufficio • Indirizzi Digitali Di Riferimento **RUP:** • Cognome • Nome • Codice Fiscale • Denominazione Amministrazione\ Codice IPA • Denominazione Amministrazione AOO \ Codice IPA AOO • Denominazione Amministrazione UOR \ Codice IPA UOR • Indirizzi Digitali di Riferimento **SW:** • Denominazione Sistema		**PF:** • SI • SI • NO • Obbligatorio solo se indicato AOO o UOR • Obbligatorio solo se indicato AMM o UOR • NO • NO **PG:** • SI • NO • NO • NO **PAI:** • SI • SI • NO • SI **PAE:** • SI • NO • SI **AS:** • NO • NO • NO • SI • SI • SI **RUP:** • SI • SI • NO • SI • SI • SI • SI **SW:** • SI	Denominazioni secondo legenda colonna E		

Numero Metadato	Metadato	N. Campo	Campi	Sottocampi	Valori	Obbligatorietà documento informatico	Valore metadato	Fase di associazione al documento	Modalità associazione
6	**Chiave descrittiva**	6.1	Oggetto		Testo libero		Testo comprensivo della tipologia documentale e altre informazioni per contestualizzare il documento, es. "Tipologia documentale + PIVA / Codice fiscale"		
7	**Chiave descrittiva**	6.2	Parola chiave		Testo libero		Opzionale / per eventuale successiva ricerca		
7	**Allegati**	7.1	Numero allegati		Inserire un numero intero compreso tra 0 e 9999	SI	0		
8	**Allegati**	7.2	Indice allegati		Da indicare per ogni allegato se Numero allegati > 0		vuoto		
9	**Allegati**	7.3		IdDoc	Identificativo del documento relativo all'allegato	SI, se numero allegati > 0	vuoto		
10	**Allegati**	7.4		Descrizione	Testo libero	SI, se numero allegati > 0	vuoto		
8	**Classificazione**	8.1	Indice di classificazione		Codifica del documento secondo il Piano di classificazione utilizzato	NO	se presente il Piano di classificazione		
9	**Classificazione**	8.2	Descrizione		Descrizione per esteso dell'Indice di classificazione indicato.	NO	se presente il Piano di classificazione		
10	**Classificazione**	8.3	Piano di classificazione		URI del Piano di classificazione	NO	se presente il Piano di classificazione		
9	**Riservato**	9.1	Non applicabile		Vero/falso	SI	FALSO		
10	**Identificativo del formato**	10.1	Formato		Previsti dall'Allegato 2 delle Linee guida	SI	XML		
11	**Identificativo del formato**	10.2	Prodotto Software		Prodotto software utilizzato per la creazione del documento e relativa versione	SI	Indicare "Non rilevabile" se non rilevabile		
12	**Identificativo del formato**	10.3		Nome prodotto		SI, quando rilevabile	Indicare "Non rilevabile" se non rilevabile		
13	**Identificativo del formato**	10.4		Versione		SI, quando rilevabile	Indicare "Non rilevabile" se non rilevabile		
14	**Identificativo del formato**	10.5		Produttore		SI, quando rilevabile	Indicare "Non rilevabile" se non rilevabile		

Numero Metadato	Metadato	N. Campo	Campi	Sottocampi	Valori	Obbligatorietà documento informatico	Valore metadato	Fase di associazione al documento	Modalità associazione
11	**Verifica**	11.1	Firmato Digitalmente		(Vero/Falso)	SI, obbligatorio nel caso di modalità di formazione doc = a/b	Vero/Falso		
12	**Verifica**	11.2	Sigillato elettronicamente		(Vero/Falso)	SI, obbligatorio nel caso di modalità di formazione doc = a/b	Vero/Falso		
13	**Verifica**	11.3	Marcatura Temporale		(Vero/Falso)	SI, obbligatorio nel caso di modalità di formazione doc = a/b	Vero/Falso		
14	**Verifica**	11.4	Conformità copie immagine su supporto informatico		(Vero/Falso)	SI, obbligatorio nel caso di modalità di formazione doc = b	Vero/Falso		
12	**IdAgg**	12.1	Non applicabile		Identificativo del fascicolo	NO	se presente un'aggregazione documentale		
13	**Id IdentificativoDocumento Principale**	13.1	Non applicabile		IdDoc del documento principale	SI, nel caso in cui sia presente un documento primario	Vuoto		
14	**NomeDelDocumento**	14.1	Non applicabile		Nome del documento\file	SI	nome file.xml		
15	**Versione del documento**	15.1	Non applicabile		Versione del documento	SI	1		
16	**Tracciature modifiche documento**	16.1	Tipo modifica		Tipo modifica: • Annullamento • Rettifica • Integrazione • Annotazione	SI, nel caso di versione > 1 o in caso di annullamento	Vuoto in caso di versione 1		
16	**Tracciature modifiche documento**	16.2	Soggetto autore della modifica		Come da ruolo = Operatore definito nel metadato Soggetti	SI, nel caso di versione > 1 o in caso di annullamento	Vuoto in caso di versione 1		
16	**Tracciature modifiche documento**	16.3	Data e ora modifica			SI, nel caso di versione > 1 o in caso di annullamento	Vuoto in caso di versione 1		
16	**Tracciature modifiche documento**	16.4	IdDoc versione precedente		Identificativo documento versione precedente	SI, nel caso di versione > 1 o in caso di annullamento	Vuoto in caso di versione 1		
17	**Tempo di conservazione**	17.1	Non Applicabile		Tempo di conservazione espresso in anno (9999=permanente)	NO	10		

Numero Metadato	Metadato	N. Campo	Campi	Sottocampi	Valori	Obbligatorietà documento informatico	Valore metadato	Fase di associazione al documento	Modalità associazione
18	**Note**	18.1	Non Applicabile		Testo libero	NO	eventuale annotazione		

ALLEGATO 1 - Modulo implementazione Misure Minime di Sicurezza

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**	
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 operazioni 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.**	
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.**	
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 divari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.**	

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.**	
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.**	
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.**	
3	**2**	**2**	**M**	**Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.**	
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.**	
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).**	
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.**	
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.**	
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.**	

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.**	
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.**	
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.).**	

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.**	
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.**	
5	**1**	**2**	**M**	**Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.**	
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.**	
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.**	
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).**	
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)**	
5	**7**	**4**	**M**	**Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).**	
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.**	
5	**10**	**2**	**M**	**Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.**	

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.**	
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.**	
5	**11**	**2**	**M**	**Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.**	

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.**	
8	**1**	**2**	**M**	**Installare su tutti i dispositivi firewall ed IPS personali.**	
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.**	
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.**	
8	**7**	**2**	**M**	**Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.**	
8	**7**	**3**	**M**	**Disattivare l'apertura automatica dei messaggi di posta elettronica.**	
8	**7**	**4**	**M**	**Disattivare l'anteprima automatica dei contenuti dei file.**	
8	**8**	**1**	**M**	**Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.**	
8	**9**	**1**	**M**	**Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumentiantispam.**	
8	**9**	**2**	**M**	**Filtrare il contenuto del traffico web.**	
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).**	
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.**	
S10	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 della trasmissione consente la remotizzazione del backup anche nel cloud.**	
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.**	

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**	
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.**	
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.	