

Manuale di gestione documentale di Informatica Alto Adige S.p.A.

Ultimo aggiornamento Agosto 2024

Approvato dal CdA in data 21-08-2024

Sommario

<u>1. Principi generali e organizzativi</u>	4
<u>1.1 Ambito di applicazione e normativa di riferimento</u>	4
<u>1.2 AOO e registro unico di protocollo</u>	4
<u>1.3 Responsabile della gestione documentale</u>	5
<u>1.4 Delegato del Responsabile del servizio di gestione documentale</u>	5
<u>1.5 Caselle di posta elettronica certificata (PEC)</u>	5
<u>1.6 Caselle di posta elettronica ordinaria</u>	6
<u>1.7 Firma digitale</u>	6
<u>1.8 Firma elettronica</u>	6
<u>2. Documento informatico</u>	6
<u>2.1 Formazione dei documenti informatici</u>	6
<u>2.2 Sottoscrizione dei documenti informatici</u>	7
<u>2.3 Validità della firma digitale nel tempo</u>	7
<u>3. Documento cartaceo</u>	8
<u>4. Sistema di protocollo informatico</u>	8
<u>4.1 Protocollazione</u>	8
<u>4.2 Registro di protocollo</u>	9
<u>4.3 Numero di protocollo e segnatura di protocollo</u>	10
<u>4.4 Fascicolo informatico</u>	10
<u>4.4.1 Tipologie di fascicoli</u>	11
<u>4.4.1.1 Fascicoli del personale</u>	11
<u>4.5 Titolario di classificazione</u>	11
<u>4.6 Annullamento</u>	12
<u>4.7 Cronologia</u>	12
<u>4.8 Registro giornaliero di protocollo</u>	13
<u>4.9 Registro di emergenza</u>	13
<u>5. Protocollo in ingresso</u>	13
<u>5.1 Rilascio delle ricevute</u>	15



5.2 Ricezione dei documenti informatici	15
5.3 Validità di istanze e dichiarazioni presentate per via telematica	15
6. Protocollo in uscita	15
6.1 Notificazione e comunicazione degli atti amministrativi	15
6.1.1 Imprese e professionisti	16
6.1.2 Pubbliche amministrazioni	16
6.1.3 Cittadini e enti di diritto privato	16
6.1.4 Domicilio digitale speciale	16
6.1.5 Copia cartacea	16
6.2 Invio per interoperabilità	17
6.3 Protocollazione di messaggi di posta elettronica in uscita	17
6.4 Comunicazioni non soggette a protocollazione	17
7. Protocollo interno	17
7.1 Competenza e conoscenza	18
8. Protocollo differito	19
9. Abilitazione all'accesso al protocollo informatico	19
9.01 Utente protocollista	19
10. Conservazione dei documenti informatici caricati nel protocollo	20
11. Documenti relativi a gare e offerte relative all'attività contrattuale	20
12. Attestazioni di conformità all'originale	20
13. Fatture elettroniche	21
14. Log di navigazione	21
15. Log dei sistemi	21
16. Formati di file ammessi	21
17. Piano di sicurezza	21
17.1 Sicurezza dei sistemi informatici	22
17.2 Sicurezza nella conservazione dei documenti	22
17.3 Politiche di sicurezza di SIAG	22
18. Disposizioni finali	22

1. Principi generali e organizzativi

1.1 Ambito di applicazione e normativa di riferimento

Il presente Manuale di gestione documentale è adottato da Informatica Alto Adige SpA (di seguito “SIAG”) ai sensi dell’articolo 5 del DPCM 3 dicembre 2013, recante “Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell’Amministrazione digitale di cui al D.Lgs. n. 82 del 2005” e delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, emanate dall’Agenzia per l’Italia Digitale (AgID) con propria determinazione n. 407 del 9 settembre 2020.

Nell’ambito del quadro normativo sopraindicato, il manuale di gestione dei flussi documentali (d’ora in avanti “Manuale”), stante la sua natura di documento operativo interno, da rendere pubblico anche all’esterno, ricopre il duplice ruolo di strumento di supporto ai processi operativi e decisionali interni e di documento pubblico funzionale al perseguimento del principio di trasparenza dell’azione amministrativa. Destinato alla più ampia diffusione e conoscenza, anche esterna, il Manuale si rivolge non solo agli operatori del protocollo ma, in generale, a tutti i dipendenti della struttura che a diverso titolo si avvalgono del sistema di gestione documentale.

Modalità di comunicazione del Manuale di gestione documentale

In ottemperanza a quanto previsto dall’articolo 4.7 delle linee Guida Agid sulla formazione, gestione e conservazione dei documenti informatici, il presente Manuale viene reso accessibile nelle seguenti forme:

- a) per il personale di Informatica Alto Adige, mediante pubblicazione sulla pagina SharePoint “Business Unit Human Resources” nella sezione Manuals/Lavoro
https://provbz.sharepoint.com/sites/SIAG/Area_HR/SitePages/Manuals.aspx;
- b) per il pubblico, mediante pubblicazione sul sito di Informatica Alto Adige SpA (www.siag.it).

1.2 AOO e registro unico di protocollo

Secondo quanto previsto dal comma 4, articolo 50, del DPR 445/2000 “Ciascuna pubblica amministrazione individua, nell’ambito del proprio ordinamento, gli Uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché comunicazione interna tra le aree stesse”. SIAG ha individuato al suo interno un’unica area organizzativa omogenea (AOO), alla quale corrisponde un registro unico di protocollo.

Il registro di protocollo di SIAG presenta le caratteristiche del protocollo informatico ai sensi del DPR 28 dicembre 2000, n. 445, e successive modifiche, e del sovra indicato DPCM 3 dicembre 2013.

La protocollazione avviene presso la sede unica di SIAG e i permessi per la protocollazione sono assegnati dal Responsabile della Gestione documentale.

1.3 Responsabile della gestione documentale

Il Responsabile della gestione documentale dell'AOO è individuato nella persona del Presidente del CdA, dott. Oscar de Iorio, giusta delibera di nomina del Consiglio di Amministrazione di data 03/08/2022.

Al Responsabile della gestione documentale sono affidate le seguenti funzioni:

- fornire supporto all'Alta Dirigenza/ai Responsabili di Reparto per il corretto funzionamento delle attività di protocollo e di gestione dei documenti, sulla base dei criteri e delle regole dettate dal presente Manuale;
- verificare l'osservanza delle disposizioni del presente Manuale da parte del personale autorizzato e degli incaricati;
- attribuire, su richiesta dell'Alta Dirigenza/dei Responsabili di Reparto, il livello di autorizzazione agli operatori/utenti per l'accesso alle funzioni del sistema di protocollo informatico e alle caselle di PEC, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento delle informazioni.

1.4 Delegato del Responsabile del servizio di gestione documentale

La signora Cicchetti Michela è individuata quale delegata del Responsabile del Servizio di gestione documentale con delibera del Cda di data 03/08/2022, a svolgere le seguenti attività:

- Definizione di criteri uniformi di gestione dei documenti informatici;
- Aggiornamento e implementazione dello schema del Manuale di gestione documentale e coordinamento con il piano di sicurezza informatica relativo con il supporto dell'ufficio legale;
- Formare ed informare il personale in merito agli strumenti che l'organizzazione intende adottare;
- Coordinare le altre risorse che all'interno dell'azienda si occupano di gestione documentale e conservazione;
- Riferire periodicamente al Responsabile della Conservazione e della gestione documentale in merito all'andamento delle attività affinché questo possa procedere ad indicare le eventuali ed opportune attività correttive.

1.5 Caselle di posta elettronica certificata (PEC)

La casella principale di posta elettronica certificata (PEC) di SIAG è: siag@legalmail.it. Questo indirizzo è indicato nell'“Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi” (IPA) <http://www.indicepa.gov.it> e sul sito web dell'SIAG <https://www.siag.it/it/home>.

Altri indirizzi PEC interni all'azienda sono i seguenti:

- dpo@pec.siag.it
- finance@pec.siag.it
- info@pec.siag.it
- supply@pec.siag.it

- pmo-smo@pec.siag.it

1.6 Caselle di posta elettronica ordinaria

L'indirizzo istituzionale della casella di posta elettronica di SIAG è pubblicato sul sito web dell'SIAG <https://www.siag.it/it/home>.

1.7 Firma digitale

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, SIAG fornisce la firma digitale ai soggetti da essa delegati a rappresentarla. I documenti amministrativi sottoscritti con firma digitale devono essere sottoposti a registrazione di protocollo. Il documento registrato nel sistema di protocollazione rappresenta il documento originale. All'atto della registrazione, il sistema verifica l'autenticità ed integrità del documento e ne registra, in modo immutabile, la data e l'ora di protocollazione nonché l'esito dei controlli di autenticità ed integrità del documento. Tutti i dirigenti di SIAG sono muniti di firma digitale.

1.8 Firma elettronica

In conformità alla normativa vigente in materia di amministrazione digitale, le credenziali di accesso costituiscono la "firma elettronica" dell'utente che utilizza il sistema e qualsiasi azione e attività svolta nel protocollo costituisce atto valido ai fini amministrativi.

2. Documento informatico

2.1 Formazione dei documenti informatici

SIAG forma gli originali dei propri documenti come documenti informatici, nel rispetto delle disposizioni del Codice dell'amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82, e successive modifiche) e delle relative regole tecniche e Linee Guida.

I documenti informatici devono essere prodotti:

- in conformità a quanto disposto dall'allegato n. 2 al DPCM 3/12/2013;
- mediante strumenti informatici di elaborazione testi (per es. Microsoft Word, Office);
- mediante applicazioni informatiche che gestiscono procedimenti amministrativi e producono automaticamente i documenti;
- in conformità ai modelli standard definiti secondo il Regolamento interno sull'utilizzo di carta intestata e logo aziendale.

Nel documento deve essere sempre indicata una data che deve coincidere con la data della sottoscrizione con firma digitale.

Si precisa che nel documento informatico non è riportata la segnatura di protocollo, in quanto la protocollazione deve avvenire per legge in un momento successivo alla sottoscrizione del documento.

Prima della loro sottoscrizione con firma digitale, i documenti informatici sono convertiti in formati non modificabili (vedi Regole tecniche e Linee Guida sopra citate).

2.2 Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici prodotti da SIAG avviene in conformità a quanto previsto dal D.Lgs. 82/05 e dal DPCM 22/02/2013 “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”

Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle suddette regole tecniche, emanate ai sensi dell’art. 20, comma 3 e dell’art. 71 del D. Lgs. 82/05, che garantisca, pertanto, l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia della scrittura privata prevista dall'articolo 2702 del Codice Civile. Il dispositivo per la generazione della firma digitale è usato esclusivamente dal titolare designato di SIAG, ai sensi della normativa vigente tale utilizzo si presume comunque riconducibile al titolare, salvo che questi dia prova contraria.

I documenti di SIAG sono firmati con firma digitale in formato PAdES (in tal caso l’estensione del file “.pdf” non cambia), o in formato CAdES (in tal caso, l’estensione del file sarà “.p7m”).

Sigle e visti, sono invece apposti sui documenti mediante firma elettronica semplice (per es. credenziali di identificazione personale).

Le credenziali di identificazione personale (username e password) sono anch’esse strettamente personali; l’utilizzo delle stesse da parte di persona diversa dal/dalla titolare costituisce un illecito.

2.3 Validità della firma digitale nel tempo

Se a un documento informatico è apposta una firma digitale basata su un certificato scaduto, revocato o sospeso, questo equivale a mancata sottoscrizione, a meno che non sia rinvenibile altrove un riferimento temporale opponibile a terzi che consenta di collocare la generazione della firma, rispettivamente, in un momento precedente alla scadenza, revoca o sospensione del certificato stesso (articolo 62 del DPCM 22 febbraio 2013).

Ai sensi dell’art. 41, comma 4, dello stesso DPCM costituiscono, inoltre, validazione temporale:

- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- il riferimento temporale ottenuto attraverso l’utilizzo della posta elettronica certificata;
- il riferimento temporale ottenuto attraverso l’utilizzo della marcatura postale elettronica.

3. Documento cartaceo

Per documento cartaceo si intende tutta la documentazione prodotta con strumenti analogici (ad esempio, una lettera scritta a mano) o con strumenti informatici (ad esempio, una lettera prodotta tramite sistema di videoscrittura) e stampata. In questo ultimo caso, come originale, si considera quello cartaceo stampato e, di norma, sottoscritto con firma autografa.

Per originale si intende la stesura definitiva del documento, perfetto nei suoi elementi sostanziali e formali. Di uno stesso documento possono esistere più esemplari originali.

4. Sistema di protocollo informatico

SIAG adotta un sistema di protocollo informatico denominato eProcs. La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili utente e password. Con l'entrata in funzione del sistema di gestione informatica dei documenti, sono eliminati tutti i sistemi di registrazione di protocollo alternativi al protocollo informatico.

4.1 Protocollazione

La protocollazione certifica l'ingresso e l'uscita dei documenti.

Sono soggetti a protocollazione tutti i documenti cartacei e informatici aventi rilevanza giuridico probatoria o amministrativa.

Rientrano tra i documenti informatici anche i messaggi di posta elettronica ordinaria e certificata.

Non sono soggetti a protocollazione: i materiali statistici, i documenti in elaborazione (bozze), i giornali, le riviste, i libri, i materiali pubblicitari, gli opuscoli, gli inviti a manifestazioni, la corrispondenza riservata, le informative.

La registrazione a protocollo è consentita solo se è presente il documento in originale e, per quanto concerne i documenti in uscita e interni, se i documenti sono sottoscritti.

Nel caso di protocollazione di un documento cartaceo in ingresso, è consigliato allegare alla registrazione di protocollo una scansione del documento e degli eventuali allegati. Si precisa che la scansione del documento cartaceo non sostituisce l'originale, il quale deve essere conservato negli archivi cartacei.

Nel caso di protocollazione di documenti informatici, il caricamento del documento e degli eventuali allegati nel registro di protocollo è obbligatorio sia in caso di protocollazione manuale sia in caso di protocollazione automatica e indipendentemente dal fatto che si tratti di un protocollo in ingresso, in uscita, interno o differito.

Il caricamento del documento informatico nel registro di protocollo è contestuale alla protocollazione.

I documenti informatici caricati nel registro di protocollo sono automaticamente versati nel sistema di conservazione digitale che ne garantisce l'integrità e la leggibilità nel tempo e, se sottoscritti con firma digitale, la validità della firma.

4.2 Registro di protocollo

Di seguito sono illustrate le regole "comuni" di registrazione del protocollo valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi, interni formali, informatici e analogici)

La protocollazione dei documenti è effettuata in un'unica operazione, utilizzando le apposite funzioni previste dal protocollo informatico.

Per la registrazione di protocollo sono obbligatorie le seguenti informazioni:

- numero di protocollo, generato automaticamente dal protocollo informatico e registrato in forma non modificabile;
- data di protocollo, assegnata automaticamente dal protocollo informatico e registrata in forma non modificabile;
- tipo di protocollo (ingresso, uscita, interno, differito);
- tipologia del documento ("default" o "fattura");
- indice di classificazione;
- mittente per i documenti in ingresso, o, in alternativa, destinatario o destinatari per i documenti interni e in uscita;
- oggetto del documento (l'oggetto deve far comprendere il contenuto di un documento; evitare l'uso di abbreviazioni);
- fascicolo informatico;
- numero e descrizione sintetica degli allegati cartacei (se presenti);
- data di ingresso del documento per le protocollazioni differite;
- nome dell'autore/autrice della registrazione di protocollo, compilato automaticamente dal protocollo informatico e registrato in forma non modificabile;
- assegnazione della registrazione di protocollo alla struttura organizzativa dell'autore/autrice della registrazione di protocollo, registrata in forma non modificabile;
- assegnazione della registrazione di protocollo alla eventuale struttura organizzativa destinataria/alle eventuali strutture organizzative destinatarie del documento;
- numero e data del protocollo del mittente per i documenti provenienti da enti pubblici;
- numero e data del protocollo di riferimento (se presente);
- mezzo di ricezione/spedizione.

Nel caso di protocollazione di documenti informatici sono altresì obbligatori:

- il caricamento del documento informatico e degli eventuali allegati, memorizzati nel sistema di gestione documentale del protocollo informatico senza possibilità di modifica o cancellazione;

- il calcolo dell'impronta del documento informatico (c.d. hash del file), eseguito dal protocollo informatico e memorizzato nel sistema di gestione documentale del protocollo informatico in forma non modificabile.

L'insieme delle registrazioni di protocollo costituisce il registro di protocollo.

4.3 Numero di protocollo e segnatura di protocollo

All'atto del salvataggio della registrazione di protocollo, il protocollo informatico genera automaticamente un numero progressivo, che è il numero di protocollo attribuito al documento nonché la segnatura di protocollo.

Nel registro di protocollo la numerazione delle registrazioni di protocollo è unica e progressiva, senza distinzione tra i diversi tipi di protocollo. La numerazione ricomincia ogni anno solare. Nel corso dell'anno solare, ogni numero di protocollo è assegnato a un solo documento; non è consentita l'attribuzione del medesimo numero di protocollo a altri documenti, anche se strettamente correlati tra loro.

Per quanto concerne i documenti cartacei in ingresso, l'utente vi appone l'indicazione del numero di protocollo.

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Viene effettuata contemporaneamente all'operazione di registrazione di protocollo. I dati della segnatura di protocollo di un documento informatico sono contenuti in un file XML conforme alle specifiche tecniche previste dalla normativa vigente (art. 55, comma 1, del "Testo Unico").

4.4 Fascicolo informatico

I documenti registrati nel protocollo informatico devono essere riuniti in fascicoli.

Il fascicolo è la raccolta ordinata di documenti relativi a un medesimo procedimento, affare, a una medesima attività o a una medesima persona (fisica o giuridica).

Ogni documento che non è inseribile in un fascicolo preesistente deve dar luogo all'apertura di un nuovo fascicolo, al quale devono essere associati anche tutti i documenti successivi relativi al medesimo procedimento, affare, alla medesima attività o persona.

I fascicoli sono aperti dalla struttura organizzativa responsabile del procedimento ovvero della gestione dell'affare, dell'attività o del fascicolo di persona fisica o giuridica, la quale ne definisce altresì la denominazione, il corrispondente indice di classificazione nonché i tempi di conservazione.

La denominazione del fascicolo deve riportare tutti gli elementi necessari ai fini della sua individuazione e deve garantire una corretta strutturazione delle informazioni, seguendo un ordine dal generale al particolare ai fini dell'individuazione univoca del singolo fascicolo.

Il protocollo informatico assegna a ogni fascicolo un codice univoco composto dalle seguenti informazioni: indice di classificazione, anno di apertura del fascicolo, numero progressivo del fascicolo all'interno dell'indice di classificazione, riferito all'anno di apertura.

Qualora il documento attenga alla competenza di più strutture organizzative, il fascicolo viene aperto dalla struttura organizzativa responsabile del procedimento e reso accessibile anche alle ulteriori strutture organizzative di SIAG coinvolte nel procedimento, ai fini della sua gestione condivisa.

La visibilità dei singoli documenti contenuti nel fascicolo non è, però, implicita, ma è data attraverso l'assegnazione di singoli privilegi (o per gruppi) alle strutture organizzative coinvolte nel procedimento. In casi particolari è ammessa l'associazione di un documento a due o più fascicoli (multi-fascicolazione).

Il fascicolo viene chiuso al termine del procedimento amministrativo o una volta esaurito l'affare. La data di chiusura del fascicolo coincide con la data dell'ultimo documento prodotto o acquisito. Dalla data di chiusura decorrono i termini per lo scarto archivistico, qualora esso sia previsto dal piano di conservazione.

4.4.1 Tipologie di fascicoli

I distinguono le seguenti tipologie di fascicolo:

- fascicoli relativi a procedimenti e affari particolari: la durata del fascicolo è strettamente connessa alla natura dell'affare, del procedimento o dell'attività trattata;
- fascicoli relativi ad attività generali per documenti che non siano collegabili strettamente ad un processo amministrativo specifico (es. corrispondenza di varia natura);
- fascicoli permanenti: Secondo una prassi comunemente diffusa, spesso si riuniscono, per finalità pratiche e conservative, fascicoli con diversa classificazione che si riferiscono ad uno stesso soggetto od oggetto (ad esempio: una persona, un'associazione, ecc.), creando dei "fascicoli permanenti" o "pratiche speciali", che rimangono "correnti" ben oltre la durata dei singoli affari o procedimenti dai quali sono composti. I fascicoli del personale rappresentano il caso più comunemente diffuso di fascicoli permanenti.

Qualora si ritenga necessario, la documentazione contenuta nei fascicoli può essere articolata in sottofascicoli.

4.4.1.1 Fascicoli del personale

Per ciascun dipendente viene istituito un fascicolo nominativo, aperto all'atto dell'assunzione in cui sono inseriti tutti i documenti che fanno riferimento al rapporto di lavoro intercorrente tra l'Amministrazione e la persona stessa.

4.5 Titolario di classificazione

Il Titolario di classificazione si articola, secondo uno schema che va dal generale al particolare. Tale schema rappresenta un sistema logico che suddivide i documenti secondo le funzioni esercitate da SIAG,

indipendentemente dagli uffici che le esercitano, dato che l'organizzazione di questi ultimi può variare nel tempo, mentre le funzioni si mantengono costanti.

Il Titolario di classificazione è corredato da una descrizione del titolare, per titoli e classi.

Il Titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Il Titolario è uno strumento tendenzialmente stabile nel tempo, ma non statico. Esso può essere modificato o integrato a seguito di assegnazioni di nuove funzioni, ovvero di sviluppo o modifica di funzioni istituzionali già possedute.

4.6 Annullamento

Le registrazioni di protocollo possono essere annullate solo previa autorizzazione dei responsabili delle strutture organizzative a cui il protocollo è assegnato per competenza.

Nell'autorizzazione all'annullamento devono essere indicati il numero e la data di protocollo della registrazione di protocollo da annullare nonché la motivazione dell'annullamento.

Autorizzazioni cumulative sono ammesse solo qualora la motivazione dell'annullamento sia la stessa per tutte le registrazioni di protocollo indicate nell'autorizzazione.

L'autorizzazione all'annullamento deve essere protocollata; la scheda di protocollo viene compilata come segue:

- tipo protocollo: interno;
- titolare: indice di classificazione della registrazione di protocollo da annullare;
- destinatario: interno;
- oggetto: "Autorizzazione all'annullamento della registrazione di protocollo *data di protocollo numero di protocollo*";
- fascicolo informatico: fascicolo del documento da annullare;
- caricamento dell'autorizzazione sottoscritta con firma digitale.

Dopo aver protocollato l'autorizzazione all'annullamento, l'utente richiama la registrazione di protocollo da annullare e procede all'annullamento.

L'avvenuto annullamento di una registrazione di protocollo è riconoscibile da un'apposita dicitura o da un segno, generati in automatico. Le registrazioni di protocollo annullate possono essere visualizzate, ma non modificate. L'avvenuto annullamento di una registrazione di protocollo è tracciato in cronologia.

4.7 Cronologia

A ogni registrazione di protocollo corrisponde una precisa cronologia, dalla quale risultano il nome, il cognome e la struttura organizzativa dell'autore/autrice della registrazione di protocollo nonché la data e l'ora di protocollazione. Ogni operazione (visualizzazione, modifica, annullamento) compiuta in relazione alle singole registrazioni di protocollo è tracciata nella corrispondente cronologia, unitamente al nome, al cognome e alla struttura organizzativa di appartenenza dell'autore/autrice dell'intervento, alla relativa data e ora. In caso di modifica di una registrazione di protocollo, in cronologia vengono tracciate anche le

informazioni originarie. La scheda della cronologia è legata indissolubilmente alla corrispondente registrazione di protocollo e i dati in essa contenuti non possono essere cancellati. Per il calcolo della data e dell'ora della protocollazione nonché di tutti i successivi interventi sulle singole registrazioni di protocollo, il protocollo informatico utilizza l'orario di sistema dei server, sincronizzati tra loro tramite il protocollo NTP (Network Time Protocol), e collegati a un elenco di server NTP ufficiali.

4.8 Registro giornaliero di protocollo

A fine giornata, il protocollo informatico genera in automatico il registro giornaliero di protocollo, il quale viene versato, entro la giornata lavorativa successiva, nel sistema di conservazione digitale, al fine di garantirne l'immodificabilità e la validità legale nel tempo, (articolo 7, comma 5, del DPCM 3 dicembre 2013 in materia di protocollo informatico).

Il registro giornaliero di protocollo contiene, in modo ordinato e progressivo, l'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Non è consentita la stampa su carta del registro giornaliero di protocollo, in quanto la versione digitale è l'unica avente valore legale. Per esigenze di consultazione, gli utenti possono generare in autonomia esportazioni delle registrazioni di protocollo in base ai criteri di ricerca impostati.

4.9 Registro di emergenza

Nell'impossibilità di utilizzare il registro di protocollo per un lasso di tempo superiore alle 48 ore, ai soli fini di gestire l'emergenza e consentire l'operatività, il direttore generale autorizza la protocollazione sul registro di emergenza di cui all'articolo 63 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modifiche, e ai sensi dell'articolo 5, comma 2, lettera q), del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 in materia di protocollo informatico. Tale funzione viene affidata al Direttore generale in quanto soggetto operativo all'interno dell'azienda in considerazione della circostanza che il mero compito di autorizzare l'attivazione del registro di emergenza di cui al paragrafo che precede, non integra alcuna responsabilità specifica del Ruolo di Responsabile della gestione documentale che rimane in capo al Presidente del CdA.

5. Protocollo in ingresso

La protocollazione dei documenti in ingresso è effettuata entro la giornata di arrivo.

La corrispondenza riportante la dicitura "riservata", "personale" o indicazioni analoghe, e la corrispondenza sigillata non devono essere aperte, in quanto considerate corrispondenza riservata.

I documenti pervenuti via posta vanno protocollati. Le buste della posta in ingresso vanno conservate in tutti i casi in cui la data di spedizione assuma rilevanza giuridica (per es. raccomandata pervenuta dopo la

scadenza di un termine perentorio). La busta va annotata nel registro di protocollo come allegato, unitamente alla data e all'ora risultanti dal timbro postale.

I documenti pervenuti via fax vanno protocollati. Nel caso in cui alla trasmissione via fax segua l'invio del documento per posta, non si procede a nuova protocollazione, a meno che il documento non abbia subito modifiche.

I documenti cartacei pervenuti per errore non vanno protocollati e devono essere spediti immediatamente al destinatario corretto. Qualora il destinatario non sia individuabile, il documento va rispedito al mittente.

Ai sensi di quanto previsto dalla lettera c) del secondo comma dell'art. 47 del D. Lgs. 82/2005 (Codice dell'amministrazione digitale) le Pubbliche Amministrazioni non possono più scambiare tra loro documenti tramite fax. L'utilizzo del fax è ammesso solo per lo scambio documentale con i privati cittadini sprovvisti di domicilio digitale e con i soggetti che non siano tenuti a possedere una casella di posta elettronica certificata.

Tenuto presente quanto sopra, i documenti ricevuti tramite fax, qualora ne venga accertata la provenienza, soddisfano il requisito della forma scritta e la loro trasmissione, a norma di legge, non deve essere seguita dalla trasmissione dell'originale. Pertanto, anche al fine di evitare inutili duplicazioni nel sistema documentario e aggravio di lavoro per il protocollo, non solo non è necessario richiedere ai mittenti di far seguire all'invio via fax la spedizione dell'originale del documento, ma è anche buona prassi disincentivarne l'invio.

Se al fax segue l'originale cartaceo, ad esso non deve essere attribuito un nuovo numero di protocollo, ma può essere conservato nel fascicolo fino a chiusura della pratica.

Il documento originale che riporta integrazioni o modifiche rispetto al fax precedentemente pervenuto costituisce invece a tutti gli effetti un nuovo documento.

La protocollazione dei messaggi di posta elettronica avviene direttamente attraverso il protocollo informatico e comporta, altresì, il caricamento automatico del testo del messaggio, degli eventuali allegati e del messaggio nel suo formato originale nelle rispettive sezioni della scheda di protocollo.

Se i messaggi di posta elettronica contengono documenti relativi a procedimenti distinti, gli allegati devono essere protocollati singolarmente e poi caricati nel protocollo informatico tramite la funzione di upload.

Nel caso di protocollazione automatica, anche il documento informatico e gli eventuali allegati sono caricati nel registro di protocollo in automatico.

Nel caso di consegna del documento informatico su supporti di memoria esterni o in cloud, l'utente deve caricare il documento nel registro di protocollo contestualmente alla protocollazione.

Nel caso in cui il documento sia recapitato per errore alla casella di posta elettronica certificata il messaggio viene rispedito al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa Società.

I documenti cartacei e informatici pervenuti presso una struttura organizzativa non responsabile per la loro trattazione, devono da quest'ultima essere assegnati alla struttura organizzativa di competenza e alla segreteria per la protocollazione.

La verifica della firma digitale viene effettuata con l'applicazione "GoSign".

La corrispondenza anonima o priva di firma o con firma illeggibile o proveniente da mittente non identificabile è soggetta a registrazione di protocollo. È demandata ai responsabili delle strutture organizzative destinatarie la valutazione della sua validità ai fini del procedimento/procedura. Nel caso di corrispondenza anonima il campo mittente nel protocollo riporterà la dicitura “anonimo”.

5.1 Rilascio delle ricevute

Al fine del rilascio di una ricevuta che attesti l'avvenuta consegna di un documento cartaceo consegnato personalmente dal mittente o da una persona incaricata, il personale consegna una fotocopia della prima pagina del documento protocollato, su cui è apposta la segnatura di protocollo.

5.2 Ricezione dei documenti informatici

La ricezione dei documenti informatici avviene tramite:

- le caselle di posta elettronica certificata (PEC);
- le caselle di posta istituzionali;
- per il tramite del SDI (vedi paragrafo 13 Fatturazione elettronica);
- per il tramite dei portali relativi a gare telematiche (vedi paragrafo 11. Documenti relativi a gare e offerte relative all'attività contrattuale);
- supporti di memoria esterni o cloud.

5.3 Validità di istanze e dichiarazioni presentate per via telematica

Le istanze e le dichiarazioni presentate a SIAG per via elettronica sono valide:

- se sottoscritte con firma digitale;
- oppure se sottoscritte con firma autografa e presentate unitamente alla copia del documento di identità.

6. Protocollo in uscita

Per quanto concerne la formazione e la sottoscrizione dei documenti informatici si rimanda al capitolo 2 “Documento informatico”.

Sono protocollati in uscita i documenti redatti e diretti a destinatari esterni a SIAG, inviati tramite PEC o notificati come da paragrafo 6.1.

La protocollazione dei documenti in uscita è effettuata subito dopo la loro sottoscrizione. Il caricamento dei documenti informatici nel registro di protocollo è obbligatorio e contestuale alla protocollazione.

6.1 Notificazione e comunicazione degli atti amministrativi

SIAG provvede alla comunicazione degli atti e dei documenti e alla relativa notificazione, utilizzando le tecnologie dell'informazione e della comunicazione. Le comunicazioni trasmesse ai domicili digitali

producono, quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con avviso di ricevimento ed equivalgono alla notificazione per mezzo della posta salvo che la legge disponga diversamente.

6.1.1 Imprese e professionisti

Le comunicazioni ai soggetti tenuti all'iscrizione nel registro delle imprese e ai professionisti tenuti all'iscrizione in albi ed elenchi avvengono esclusivamente tramite il domicilio digitale indicato nell' "Indice nazionale dei domicili digitali delle imprese e dei professionisti" (INI-PEC) www.inipepec.gov.it. L'INI-PEC è stato istituito dal Ministero dello Sviluppo Economico.

6.1.2 Pubbliche amministrazioni

Le comunicazioni alle pubbliche amministrazioni, ai gestori di pubblici servizi e alle società a controllo pubblico avvengono tramite il domicilio digitale indicato nell'IPA www.indicapa.gov.it o tramite gli indirizzi concordati con gli stessi. I documenti possono essere, altresì, resi disponibili previa comunicazione delle modalità di accesso telematico agli stessi.

6.1.3 Cittadini e enti di diritto privato

Con l'avvio dell'operatività dell' "Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel registro delle imprese", le comunicazioni ai cittadini e ai soggetti diversi da quelli di cui ai capitoli 6.2.1 e 6.2.2 avvengono tramite il domicilio digitale ivi indicato o tramite gli indirizzi concordati con gli stessi.

6.1.4 Domicilio digitale speciale

I soggetti di cui ai capitoli 6.1.1, 6.1.2 e 6.1.3 possono, altresì, eleggere un domicilio digitale speciale, diverso da quello già riportato nei rispettivi indici. Tale indirizzo deve essere un indirizzo PEC.

6.1.5 Copia cartacea

In alcuni casi è previsto l'invio dell'originale cartaceo o di copia cartacea tratta dal documento informatico originale (articolo 3-bis, commi 4-bis, 4-ter e 4-quater, del D.Lgs. 7 marzo 2005, Nr. 82, e successive modifiche).

La copia cartacea viene realizzata tramite una apposita applicazione e riporta l'indicazione a stampa del nominativo del firmatario, i dati di riferimento del certificato di firma, la segnatura di protocollo, e un'annotazione relativa alla predisposizione del documento originale in conformità alla normativa vigente e alla sua disponibilità presso SIAG.

L'invio della copia cartacea avviene tramite posta tradizionale; nel caso in cui sussista un obbligo di notifica, la copia cartacea è inviata a mezzo raccomandata con avviso di ricevimento, altrimenti è inviata a mezzo posta ordinaria.

La realizzazione della copia cartacea è ammessa esclusivamente nel caso di cui sopra.

6.2 Invio per interoperabilità

Ai fini dell'invio degli atti e dei documenti l'utente ricorre alla funzione di interoperabilità del protocollo informatico. Al destinatario/alla destinataria viene inviato un messaggio di posta elettronica contenente il documento informatico, eventuali allegati e un file "segnatura.xml" contenente la segnatura di protocollo e gli ulteriori metadati relativi alla registrazione di protocollo.

6.3 Protocollazione di messaggi di posta elettronica in uscita

I messaggi di posta elettronica certificata devono essere protocollati, qualora abbiano rilevanza giuridico-probatoria o in caso di richiesta da parte della struttura organizzativa di riferimento. Questa forma di protocollazione, però, non è ammessa per l'invio di atti amministrativi, i quali devono sempre essere caricati nel protocollo informatico come documenti principali e inviati tramite la funzione di interoperabilità.

6.4 Comunicazioni non soggette a protocollazione

Le comunicazioni non soggette a protocollazione sono di norma inviate tramite le caselle personali di posta elettronica.

La corrispondenza cartacea di tipo personale/riservato pervenuta non viene protocollata ma è assegnata direttamente al destinatario senza aprirla.

Qualora le buste vengano aperte per errore, il personale addetto alla protocollazione provvederà a sigillarle, ad apporre la dicitura "aperta per errore", munita di sottoscrizione dell'incaricato, e a trasmetterle al destinatario.

I destinatari provvedono a inoltrare sollecitamente alla postazione di protocollazione i documenti concernenti l'attività d'ufficio, qualora erroneamente trasmessi loro mediante corrispondenza personale, al fine di espletare le consuete operazioni di registrazione, indicando il grado di riservatezza ritenuto necessario.

7. Protocollo interno

Per quanto concerne la formazione e la sottoscrizione dei documenti informatici, si rimanda al capitolo 2 "Documento informatico".

All'interno di SIAG, lo scambio dei documenti informatici avviene tramite:

- il registro di protocollo (assegnazione);
- la posta elettronica ordinaria;
- altre applicazioni informatiche.

Sono protocollati nel protocollo interno i documenti redatti dalle singole strutture organizzative di SIAG e destinati alla comunicazione interna.

I documenti interni sono protocollati dalla segreteria su indicazione della struttura organizzativa che li redige. La Segreteria provvede altresì al caricamento dei documenti informatici nel registro di protocollo e all'assegnazione della registrazione di protocollo alla struttura organizzativa destinataria/alle strutture organizzative destinatarie.

La protocollazione dei documenti interni è effettuata subito dopo la loro sottoscrizione.

Anche i messaggi di posta elettronica devono essere protocollati, qualora abbiano rilevanza giuridico probatoria. In questo caso, i messaggi sono inviati esclusivamente agli indirizzi istituzionali di posta elettronica delle strutture organizzative destinatarie.

Nelle comunicazioni tra le singole strutture organizzative di SIAG non è consentito l'utilizzo della PEC, salvo nei casi previsti dalla legge.

Le comunicazioni interne di carattere informale non sono soggette a protocollazione e la loro trasmissione avviene tramite le caselle personali di posta elettronica.

7.1 Competenza e conoscenza

Quando un documento è indirizzato sia a destinatari esterni a SIAG, sia a destinatari interni alla stessa, ai fini della scelta del "tipo protocollo" va osservato quanto segue:

- la competenza prevale sulla conoscenza;
- il destinatario esterno prevale sul destinatario interno.

Se un documento è indirizzato a un destinatario interno per competenza e a un destinatario esterno per conoscenza, l'utente seleziona il tipo protocollo "interno", in quanto la competenza prevale sulla conoscenza.

Se un documento è indirizzato a un destinatario esterno e a un destinatario interno, e entrambi i destinatari sono destinatari per competenza, l'utente seleziona il tipo protocollo "uscita", in quanto il destinatario esterno prevale sul destinatario interno.

Se un documento è indirizzato a un destinatario esterno per competenza e a un destinatario interno per conoscenza, l'utente seleziona il tipo protocollo "uscita", in quanto il destinatario esterno prevale sul destinatario interno e la competenza prevale sulla conoscenza.

8. Protocollo differito

La protocollazione può essere differita solo in caso di temporaneo ed eccezionale carico di lavoro che non permetta di protocollare i documenti in giornata. La data di ingresso dei documenti è annotata nel registro di protocollo.

I documenti cartacei, la cui protocollazione viene differita, devono essere datati e siglati dalla persona che li riceve.

Quando la data di ingresso dei messaggi di posta elettronica è anteriore alla data di protocollo, il protocollo informatico compila la scheda del “protocollo differito” in automatico. (Ad esempio, il sistema ha creato il protocollo con data 18.02.2023 ma lo ha classificato come differito impostando la data di arrivo come 17.02.2023)

Nel caso di protocollazione automatica effettuata da sistemi informatici, il sistema provvederà a effettuare una protocollazione differita al ripristino delle sue funzionalità, qualora per problemi tecnici non sia stato possibile eseguire la protocollazione entro la giornata di arrivo.

9. Abilitazione all'accesso al protocollo informatico

La visibilità delle singole registrazioni di protocollo è possibile solo da parte di utenti preventivamente autorizzati ed abilitati.

L'amministratore/amministratrice di registro ha accesso a tutte le registrazioni di protocollo del registro di protocollo.

La Segreteria assolve ai compiti di amministratore del registro di protocollo

L'amministratore/amministratrice del registro di protocollo:

- gestisce la struttura dell'organigramma;
- gestisce le utenze key-user;
- gestisce le tabelle di configurazione del sistema;
- effettua l'importazione dei registri di emergenza nel registro di protocollo.

9.01 Utente protocollista

L'Utente protocollista è la figura incaricata di effettuare le operazioni di registrazione di protocollo o le altre forme di registrazione dei documenti previste dal presente Manuale.

Il Personale utente protocollista è tenuto ad osservare le disposizioni relative alla conforme esecuzione di tutte le operazioni connesse alla registrazione, classificazione e trasmissione della documentazione soggetta a registrazione di protocollo in arrivo, partenza e interna, ed è responsabile del corretto inserimento dei dati.

10. Conservazione dei documenti informatici caricati nel protocollo

I documenti informatici devono essere caricati nel registro di protocollo per garantirne il mantenimento della validità legale fino al momento del successivo versamento nel sistema di conservazione digitale. La regola generale è che il versamento nel sistema di conservazione digitale dei documenti deve avvenire tempestivamente, al fine di consentirne la conservazione almeno una volta l'anno.

Una volta versati nel sistema di conservazione digitale, i documenti informatici restano comunque visibili nel registro di protocollo.

Per maggiori informazioni sulla conservazione dei documenti informatici si rinvia al Manuale di Conservazione di SIAG pubblicato sul sito di SIAG (www.siag.it).

11. Documenti relativi a gare e offerte relative all'attività contrattuale

I documenti relativi alle gare telematiche che riguardano la PAB vengono caricati sul portale SICP di Bandi Alto Adige. Tali documenti vanno importati all'interno del fascicolo contenente la documentazione preliminare alla gara per l'affidamento di un lavoro o della fornitura di beni/servizi, qualora già esistente a sistema, oppure all'interno di un nuovo fascicolo creato ad hoc. La protocollazione della documentazione di gara e delle offerte, caricati sul portale SICP, non è necessaria in quanto il gestore ACP ha implementato il processo di conservazione a norma.

Tutti i documenti relativi alle altre gare d'appalto anche non telematiche vanno protocollati ponendo particolare attenzione alla riservatezza e, in particolar modo, agli elementi della registrazione (oggetto e destinatari/mittenti).

La determina a contrarre di tutte le procedure di affidamento, viene resa pubblica mediante pubblicazione nell'apposita sezione del sito istituzionale all'indirizzo: <https://www.siag.it/it/delibere-a-contrarre-o-atti-equivalenti>.

12. Attestazioni di conformità all'originale

Qualora venga richiesta una copia conforme informatica di originale informatico sarà rilasciato un duplicato informatico con attestazione dell'impronta informatica dei file costituenti il duplicato informatico.

Per generare l'hash di un file, si utilizza l'utilità presente sui nostri sistemi. Accedendo al prompt dei comandi, si lancia il comando: `certutil -hashfile "Nomefile" SHA256`.

SHA256 è un buon algoritmo di crittografia da utilizzare.

13. Fatture elettroniche

Le fatture sono gestite secondo le disposizioni normative vigenti.

Ai fini della ricezione delle fatture elettroniche, a SIAG è assegnato un “codice univoco ufficio” risultante dall’IPA <http://www.indicepa.gov.it>.

14. Log di navigazione

SIAG, in ottemperanza all’art. 132 del Codice privacy ed in qualità di Internet Service Provider, provvede alla conservazione per 12 mesi dei dati relativi al traffico telematico per finalità di accertamento e repressione dei reati.

15. Log dei sistemi

SIAG, in ottemperanza a quanto previsto nei controlli di cui all’allegato B della legge 196/2003, provvede alla conservazione, per sei mesi, dei log di accesso degli amministratori di sistema.

Inoltre, essendo qualificata per l’erogazione di servizi per la PA che impattano sia su dati critici sia su dati ordinari, in ottemperanza a quanto previsto all’interno della determina 307 di ACN e, nello specifico, al controllo PR.PT-1, conserva, in modo sicuro, in maniera centralizzata, i log relativi alla sicurezza dei sistemi, per almeno 24 mesi.

16. Formati di file ammessi

I formati di file ammessi da SIAG per la formazione dei propri documenti e per la gestione di quelli ricevuti, sono indicati nelle disposizioni normative di riferimento ed in particolare nell’Allegato 2 al DPCM 3 dicembre 2013.

17. Piano di sicurezza

Nel maggio 2011 SIAG e la Ripartizione Informatica della Provincia hanno inaugurato un Data Center comune, con sede a Bolzano, che ha la funzione di ospitare l’infrastruttura informatica delle due entità. Con delibera n. 1048 dell’11 luglio 2011, la Giunta provinciale ha deciso di riorganizzare l’intero settore informatico della Provincia, trasferendone la parte operativa a SIAG e la guida strategica alla Ripartizione Informatica.

SIAG è quindi diventata il braccio operativo della Provincia per quanto riguarda l’informatica e ha ora in carico la gestione dell’intera infrastruttura del Data Center e di tutti i servizi informatici offerti dalla

Ripartizione Informatica della Provincia alle altre Ripartizioni. I rapporti tra Provincia autonoma di Bolzano e SIAG sono disciplinati nell'accordo quadro ai sensi della legge provinciale 8 novembre 1982, n. 33.

SIAG è in possesso delle seguenti certificazioni:

- certificazione di qualità UNI EN ISO 9001:2015 "Quality Management System";
- certificazione di sicurezza UNI ISO/IEC 27001:2013 "Information Security Management System" con le certificazioni integrative:
 - ISO/IEC 27017:2015 "Information security controls for cloud services";
 - ISO/IEC 27018:2019 "Protection of personally identifiable Information (PII) in public clouds acting as PII processor";
- certificazione sistema gestione ambientale ISO 14001:2015 "Environmental Management System".

17.1 Sicurezza dei sistemi informatici

SIAG ha introdotto e applica un sistema di gestione della sicurezza delle informazioni in relazione allo sviluppo e all'erogazione di servizi nel settore dell'information technology, così come certificato dallo standard adottato ISO/IEC 27001.

17.2 Sicurezza nella conservazione dei documenti

Il sistema adottato per garantire la sicurezza nella conservazione dei documenti è descritto all'interno del Manuale di conservazione dei Conservatori accreditati coinvolti.

17.3 Politiche di sicurezza di SIAG

In questi anni, in osservanza della normativa vigente ed in particolare, della nuova normativa relativa alla protezione dei dati personali (Regolamento EU di protezione dei dati personali 679/2016) e delle best practice per la sicurezza, sono stati adottati vari regolamenti e policy finalizzati a soddisfare i più elevati requisiti richiesti in termini di sicurezza fisica e logica in parte anche in materia di sicurezza organizzativa; questi regolamenti e queste policy sono ovviamente rivolti al personale di SIAG.

18. Disposizioni finali

Per quanto non espressamente previsto dal presente manuale trova applicazione la normativa vigente in materia.

Il Manuale di gestione documentale di SIAG e le sue eventuali successive modifiche e integrazioni sono approvati con delibera del CdA su proposta del Responsabile della Gestione Documentale.