Allegato 9

Piano della sicurezza informatica

Premesse
Come già indicato nel manuale, la sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici archiviati sono garantiti, ad oggi, dall'applicazione informatica adottata dall'Ente di Governo dell'Ambito, ossia dalla Provincia di Como.
Il piano di sicurezza informatica del sistema informativo dell'amministrazione è definito dall'organizzazione dell'Ente che gestisce il sistema informatico generale.
Viene di seguito riportato, pertanto, il piano della sicurezza adottato dalla Provincia di Como, ed allegato al manuale di gestione documentale della stessa.

Glossario – Abbreviazioni
La terminologia utilizzata è definita nell'allegato 1 del DPCM del 3.12.2013 recante le Regole tecniche per il protocollo informatico ai sensi degli artt. 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'Amministrazione Digitale di cui al D.Lgs. n. 82/2005.
Nella tabella seguente si esplicitano le abbreviazioni:

- RGD: Responsabile Gestione Documentale
- AOO: Area Organizzativa Omogenea.
- PDP: Prodotto di Protocollo informatico.
- UU: Ufficio Utente

Normativa di riferimento
DPCM del 3.12.2013 - le Regole tecniche per il protocollo informatico ai sensi degli artt. 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'Amministrazione Digitale di cui al D.Lgs. n. 82/2005.

Piano di sicurezza
Il presente documento riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

Obiettivi del piano di sicurezza
Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dalla AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Generalità
Il RGD ha predisposto il piano di sicurezza in collaborazione con il Responsabile del sistema informativo. Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non) e i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato b) del D.Lgs. 30.06.2003, n. 196 - Codice in materia di protezione dei

dati personali, in caso di trattamento di dati personali;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.
Il RGD 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 rete della AOO;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di credenziali di identificazione (user ID) ed autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno trimestrale durante la fase di esercizio;
- piano di backup con particolare riferimento alla esecuzione e gestione delle copie di riserva dei dati e dei documenti;
- 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 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 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.
- invio del registro giornaliero di protocollo, entro la giornata lavorativa successiva, al sistema di conservazione, garantendone l'immodificabilità del contenuto.

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 RGD e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

Formazione dei documenti – aspetti di sicurezza
Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e la AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF e TIFF. I documenti informatici prodotti dall'AOO con altri applicativi di videoscrittura sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard PDF e TIFF, come previsto dalle regole tecniche per la

conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.
Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al DPCM del 13 novembre 2014 recante le "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al Decreto Legislativo n. 82 del 2005".
La marcatura temporale consente di associare al documento informatico una data ed un'ora legalmente validi ed opponibili a terzi. Con l'utilizzo della marcatura temporale si certifica l'esistenza del documento con un determinato contenuto ad una precisa data e ora. Inoltre, la validità del documento informatico firmato digitalmente si estende del tempo anche quando il certificato associato risulterà scaduto, revocato o sospeso.
L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto alla AOO.

Gestione dei documenti informatici
Il sistema operativo del PdP utilizzato dalla AOO, è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).
L'infrastruttura tecnologica che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Componente organizzativa della sicurezza
La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informativo della Provincia di Como al fine di garantire l'accesso e le abilitazioni alla gestione dei documenti

informatici solo alle persone espressamente autorizzate.
Il Pdp adottato dall'Ente è progettato in modo da consentire diversi livelli si sicurezza per l'accesso ai dati. Ad esempio, solo l'utente amministratore è abilitato alla creazione degli utenti ed alla definizione dei ruoli. Dal punto di vista organizzativo sono state definite le seguenti figure specifiche:

- il Responsabile della Gestione Documentale (RGD);
- l'utente amministratore del prodotto di protocollo informatico;
- gli utenti abilitati al protocollo previsti da ciascun settore;

ed è stata individuata la seguente procedura:

- il RGD individua l'utente amministratore del prodotto di protocollo informatico;
- i tecnici del settore Innovazione Tecnologica creano l'utente amministratore del prodotto di protocollo informatico e rilasciano formalmente le credenziali;
- ciascun dirigente individua formalmente per il proprio settore gli utenti abilitati al protocollo ed allo smistamento dei documenti;
- l'utente amministratore del prodotto di protocollo informatico provvede alla creazione ed abilitazione degli utenti;
- ciascun utente riceve formalmente le credenziali di accesso.

Componente fisica della sicurezza
La componente fisica della sicurezza ha lo scopo di proteggere il sistema informativo dai rischi originati da furti e atti vandalici, calamità naturali, accesso illecito ai locali dove risiedono le postazioni di lavoro di accesso e fruizione delle funzionalità del prodotto di protocollo informatico e dove sono ubicate le componenti hardware e software del sistema informativo.
All'interno della sede dell'Ente è stato progettato ed allestito un piccolo data center nel rispetto delle normative vigenti. Nel data center sono ubicati i server che erogano i servizi informatici e gestiscono il sistema di protocollazione informatico e la SAN dedicata alla memorizzazione ed alla distribuzione dei dati.
Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:

- il data center è accessibile solo al personale autorizzato (alcuni dipendenti dell'Ente ed i fornitori esterni solo se accompagnati dal personale interno);
- gli accessi sono gestiti tramite un sistema automatico di autenticazione basato su un codice numerico. I tecnici del settore Innovazione Tecnologica ed alcuni tecnici dell'Ufficio Tecnico sono dotati di codice di accesso nominativo. I tecnici esterni che eventualmente necessitano di accedere fisicamente all'infrastruttura informatica allocata nel data center, al fine di eseguire le attività previste dai contratti, sono sempre accompagnati da un tecnico interno che supervisiona le attività. Gli accessi al data center sono memorizzati sotto forma di log, per consentire l'identificazione del soggetto e dell'istante temporale in cui si è verificato l'evento.
- il data center è supervisionato 24 ore su 24. All'interno sono dislocati una serie di sensori collegati alla centralina che invia, a seconda dell'evento, i relativi allarmi.

Le misure di sicurezza fisica hanno un'architettura multi livello:

- i sistemi per la gestione e la memorizzazione dei dati del protocollo informatico sono centralizzati presso il data center. Il database del protocollo è replicato in modo asincrono presso la sede del fornitore degli applicativi;
- la consultazione dei dati è consentita mediante il prodotto di protocollo, installato sulle postazioni di lavoro degli utenti;
- l'accesso al prodotto di protocollo avviene a seguito di un processo di autenticazione basato su username e password. Tali credenziali sono rilasciate dall'amministratore del prodotto di protocollo informatico.

Componente logica della sicurezza
La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.
Tale componente, nell'ambito del prodotto di protocollo, viene realizzata attraverso la

configurazione di diversi profili di autorizzazione che consentono di assegnare ruoli diversi agli utenti a seconda dei loro compiti (amministrativi o operativi). L'applicativo inoltre, consente di tenere traccia delle sessioni di lavoro attivate da ogni utente.
L'accesso al prodotto di protocollo è consentito previa digitazione di credenziali di identificazione (user ID) ed autenticazione (password). La memorizzazione della password nel sistema avviene in forma cifrata. Le credenziali di autenticazione al PDP sono note solo all'utente abilitato.
I tecnici del settore Innovazione Tecnologica, nominati formalmente amministratori di sistema, sono dotati di credenziali nominative per l'accesso ai sistemi con ruolo di amministratore. Gli accessi effettuati dagli amministratori di sistema sono tracciati e registrati, come previsto dalla normativa vigente ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" - provvedimento del 27 novembre 2008), tramite l'utilizzo di un software dedicato. In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura costituita da:

- firewall: filtra tutti i pacchetti entranti ed uscenti dalla rete informatica dell'Ente;
- IPS (Intrusion Prevention System): protegge contro possibili attacchi diretti verso i sistemi interni, rilevando i tentativi di intrusione;
- sistema di controllo degli accessi alla rete locale: consente di individuare i dispositivi che accedono ad una LAN al fine di bloccare quelli non autorizzati;
- sistema di protezione della posta elettronica da spam e virus;
- proxy con funzionalità avanzate di autenticazione del client e controllo del contenuto delle pagine web;
- sistema di filtraggio degli URL della navigazione internet avente come finalità il blocco di siti pericolosi o non attinenti alle attività lavorative.

Componente infrastrutturale della sicurezza
La componente infrastrutturale della sicurezza assicura la continuità elettrica dei sistemi e le condizioni climatiche adeguate al corretto funzionamento delle risorse strumentali e garantisce l'efficienza del sistema di rilevazione e di spegnimento degli incendi.
Il data center dell'Ente parlare del sistema di climatizzazione del data center, sistema di allarme per incendio/allagamento… (inserire CED).

Gestione delle registrazioni di protocollo e di sicurezza
Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad esempio dati o transazioni), presenti o transitate sul PdP, che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.
Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico;
- dalle registrazioni del PdP.

Le registrazioni di sicurezza sono memorizzate in modo tale da garantirne l'integrità nel tempo.

Trasmissione e interscambio dei documenti informatici
Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario. Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità

personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse. Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'amministrazione, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196. Inoltre, per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272). Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

Ai sensi del DPCM del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi. La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28.

All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture. Gli Uffici dell'amministrazione (UOR) si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica (eventualmente certificata ai sensi del decreto del Presidente della Repubblica n. 68 dell'11 febbraio 2005) in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente l'impiego della posta elettronica nelle pubbliche amministrazioni.

Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva. La profilazione preventiva consente di definire le abilitazioni che possono essere effettuate da un utente del servizio di protocollo e gestione documentale. Queste, in sintesi, sono la consultazione, l'inserimento, la modifica, la cancellazione di dati / utenti.

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo. Le credenziali di autenticazione sono nominative e la password di accesso deve essere costituita da almeno otto caratteri (alfanumerici, maiuscole e minuscole).

Inoltre, il Pdp prevede un sistema per il blocco delle utenze in caso di ripetuti inserimenti errati delle credenziali di accesso.Gli utenti che non effettuano l'accesso per un determinato periodo di tempo sono disattivati automaticamente. Il PdP adottato dalla AOO:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o

gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire
- modifiche non autorizzate.

Ciascun utente del PdP può consultare tutti i documenti della AOO, eccetto per quelli riservati ad un determinato Ufficio Utente (UU).

Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RGD della AOO. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni. Le utenze possono essere gestite solo dall'utente amministratore del PdP.

Accesso al registro di protocollo per utenti interni alla AOO

L'autorizzazione all'accesso ai registri di protocollo è consentita solo agli utenti abilitati al Pdp.

In particolare:
- l'utente amministratore del PdP ha visibilità completa sul registro di protocollo;
- l'operatore che gestisce lo smistamento dei documenti può assegnare i documenti ai settori della AOO;
- il Responsabile del Protocollo di Settore (RPS) può inserire e consultare documenti;
- il Responsabile della Gestione documentale (RGD) può cancellare e modificare i documenti protocollati.

Nel caso in cui sia effettuata la registrazione di un documento sul protocollo riservato, la visibilità completa sul documento stesso è possibile solo agli utenti di quel settore.

Utenti esterni alla AOO - altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 42.

Le AOO che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzano funzioni di accesso per ottenere le seguenti informazioni:

numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;

identificazione dell'Ufficio Utente di appartenenza del Responsabile della Procedura Amministrativa (RPA).

Utenti esterni alla AOO - Privati

Per l'esercizio del diritto di accesso ai documenti, sono possibili due alternative: l'accesso diretto per via telematica e l'accesso attraverso l'Ufficio Relazioni con il Pubblico (URP).

L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente, quali: firme elettroniche, firme digitali, Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE), sistemi di autenticazione riconosciuti dall'AOO. L'accesso attraverso l'URP prevede che questo ufficio sia direttamente collegato con il sistema di protocollo informatico e di gestione documentale sulla base di apposite abilitazioni di sola consultazione concesse al personale addetto.

Se la consultazione avviene allo sportello, di fronte all'interessato, a tutela della riservatezza delle registrazioni di protocollo, l'addetto posiziona il video in modo da evitare la diffusione di informazioni di carattere personale. Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

Conservazione dei documenti informatici
La conservazione dei documenti informatici verrà regolata con l'attuazione del manuale di conservazione secondo il DPCM 3 dicembre 2013, in materia di conservazione dei documenti informatici.

Servizio archivistico
Il responsabile del sistema archivistico dell'AOO ha individuato nella sede i locali dell'archivio dell'amministrazione. Il responsabile del servizio in argomento ha effettuato la scelta a seguito della valutazione dei fattori di rischio che incombono sui documenti (ad es. rischi dovuti all'ambiente in cui si opera, rischi nelle attività di gestione, rischi dovuti a situazioni di emergenza). Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha predisposto e reso noto, un piano individuando i soggetti incaricati di ciascuna fase. Sono state pure regolamentate minutamente le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato. Il responsabile del servizio di gestione archivistica è a conoscenza, in ogni momento, della collocazione del materiale archivistico e ha predisposto degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.
Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalle regole tecniche vigenti, (ovvero altri formati non proprietari di seguito indicati).

Servizio di conservazione sostitutiva
Il responsabile della conservazione sostitutiva dei documenti fornisce le disposizioni, in sintonia con il piano generale di sicurezza e con le linee guida tracciate dal RGD, per una corretta esecuzione delle operazioni di salvataggio dei dati.
Le registrazioni di protocollo sono salvate giornalmente su un sistema di backup, secondo delle procedure definite dal Settore Innovazione Tecnologica. Le registrazioni giornaliere di protocollo sono inoltre riportate nel registro giornaliero di protocollo, da inviare in conservazione sostitutiva entro il giorno lavorativo successivo.

Politiche di sicurezza adottate dalla AOO
Le politiche di sicurezza stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo e sia le misure per la gestione degli incidenti informatici. Tali politiche sono regolamentate dal Settore Innovazione Tecnologica e attuate dai tecnici autorizzati, nominati formalmente amministratori di sistema, che, tra i loro compiti, devono garantire il salvataggio quotidiano dei dati.
È compito del RGD, assistito dal responsabile del sistema informativo, procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza. Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dall'AgID o a seguito dei risultati delle attività di audit. In ogni caso, tale attività è svolta almeno con cadenza annuale.