ALLEGATO I

PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI (ver. 1.0)

Sommario

Acronimi

Si riportano, di seguito, gli acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea;
- **RSP** - Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **PdP** - Prodotto di Protocollo informatico – l'applicativo acquisito dall'amministrazione/AOO per implementare il servizio di protocollo informatico;
- **UOP** - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UOR** - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;

Obiettivi

Il piano di sicurezza garantisce che le informazioni siano disponibili, integre, riservate e che per i documenti informatici sia assicurata l'autenticità, la non ripudiabilità, la validità temporale, l'estensione della validità temporale. I dati, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento, vengono 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.

Generalità

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o 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 decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, in caso di trattamento di dati personali.

Il servizio informatico dell'Ente 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:

- protezione della rete 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 (user ID), di una password e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno semestrale durante la fase di esercizio;
- continuità del servizio con particolare riferimento, sia all'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, a cura del servizio informatico dell'Ente, 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;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo;
- registrazione in apposito log della banca dati dell'AOO delle attività di protocollo effettuate da ciascun utente durante l'arco della giornata, comprese le modifiche autorizzate.

I dati registrati nei log dei sistemi operativi, e nella banca dati del sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità da soggetti autorizzati in virtù delle norme di legge.

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

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Per il formato finale del documento si adottano preferibilmente i formati PDF, XML e TIFF, in accordo con le regole tecniche individuate dal CAD (Codice dell'Amministrazione Digitale).

I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nel formato standard PDF/A 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 decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza.

Gestione dei documenti informatici

Il sistema operativo del PdP utilizzato dall'amministrazione/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), come richiesto dalla circolare nr. 31 del 21/06/2001 *(Il decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 (Gazzetta Ufficiale n. 272 del 21 novembre 2000), recante "Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428", stabilisce all'art. 7, comma 6, che "L'Autorità per l'informatica nella pubblica amministrazione compila e mantiene aggiornata la lista dei sistemi operativi disponibili commercialmente che soddisfano i requisiti minimi di sicurezza e la rende pubblica sul proprio sito Internet". In tal senso, si stabilisce che la lista dei sistemi operativi disponibili commercialmente che soddisfano i requisiti minimi di sicurezza e' costituita da quelli conformi almeno alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni. La conformità deve essere attestata dal fornitore del sistema operativo. Il fornitore del sistema di protocollo informatico dovrà esplicitamente dichiarare soddisfatti i requisiti minimi di sicurezza anche per quanto attiene alla configurazione del sistema operativo per la specifica applicazione. Adeguata documentazione dovrà essere presente nella fornitura. La configurazione sarà oggetto di verifica in sede di collaudo.)*

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- l'accesso al server del protocollo informatico in modo che qualsiasi 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.
- 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 informatico dell'amministrazione/AOO.

Componente fisica della sicurezza

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:

- accesso al personale dei Sistemi Informativi mediante dispositivo di controllo accessi con badge;
- accesso al personale dei lavori pubblici in caso di urgenze e/o per la manutenzione dei locali e degli impianti annessi mediante dispositivo di controllo accessi con badge;
- tutti gli accessi sono registrati in file di log.

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.

Componente infrastrutturale della sicurezza

Il sistema informatico utilizza i seguenti impianti:

- Un server di rete su cui è installata la banca dati e macchina virtuale sui cui è installato il software gestionale.
- Il sistema di protocollo, lato utente, funziona in modalità *web,* il browser previsto per l'utilizzo dei servizi di protocollo è Internet Explorer. L'indirizzo deve essere aggiunto ai siti attendibili e devono essere impostati i livelli di sicurezza personalizzati.
- I server e tutte le postazioni di lavoro sono dotate di un prodotto antivirus installato centralmente dal servizio informatico dell'Ente al fine di prevenire la diffusione di software malevolo (*virus* e *worms*) proteggendo sia la stazione di lavoro sia le reti alle quali l'utente è collegato. L'aggiornamento è automatico ad ogni connessione con il sistema informativo centrale inoltre una volta a settimana viene eseguita una scansione completa delle postazioni.
- Sistema di protezione contro gli accessi indesiderati alla rete comunale (firewall ridondati e proxy).

Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. 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;
- dalle registrazioni delle attività del PdP.

Le registrazioni di sicurezza sono soggette alle seguenti misure:
Il backup dei dati e del software è giornaliero e viene effettuato con il software "Symantec Backup Exec 15". Avviene sia su nastri, che sono conservati in cassaforte, che su NAS (Network Area Storage). Il controllo dell'esito dei backup notturni viene eseguito tutti i giorni a cura del personale del servizio informatico dell'Ente, in caso di errore si provvede a sostituire i nastri e/o ad attivare le procedure di diagnosi dei problemi riscontrati.
E' possibile il recupero dati al giorno precedente in caso di guasti, malfunzionamenti, indisponibilità degli strumenti ed il recupero dati progressivo, fino al recupero totale al massimo al mese precedente, in caso di disastro. A fine mese i nastri dei backup sono portati in banca e depositati nella cassetta di sicurezza dell'Ente.

Trasmissione e interscambio dei documenti informatici

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 consentito il trattamento 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.

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 decreto del Presidente del Consiglio dei Ministri 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 dal decreto del 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata".
Inoltre nella circolare n. 60 del 23 gennaio 2013, emanata dall'Agenzia per l'Italia digitale, vengono definiti il formato e la tipologia di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni.
Al fine di favorire l'interoperabilità dei sistemi di protocollo informatico l'Amministrazione è iscritta all'IPA (Indice della Pubblica Amministrazione).

All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica e/o attraverso le scrivanie virtuali del gestionale di protocollo 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" e successivamente dalla direttiva 18 novembre 2005 del Ministro per l'Innovazione e le Tecnologie "Linee guida per la Pubblica Amministrazione digitale" oppure attraverso il gestionale di protocollo informatico attraverso le scrivanie virtuali individuate all'interno della struttura dell'organizzazione codificata nello stesso.

Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (userid e password) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni delle attività che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale, es. consultazione, inserimento, modifica, annullamento.

Una stessa username può essere attribuita ad un unico utente, trattandosi di una chiave univoca nel database degli utenti. I codici identificativi personali sono assegnati e gestiti in modo da prevederne la disattivazione in caso di perdita della qualità che ne consentiva l'accesso alla procedura.
La password prevede un minimo di 8 caratteri ed ha durata semestrale, inoltre è previsto un controllo che se l'utenza non viene utilizzata per almeno sei mesi viene automaticamente bloccata ed è necessario l'intervento del servizio informatico dell'Ente per la riattivazione.
Il PdP adottato dall'amministrazione/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, se autorizzata, e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.
Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RSP dell'amministrazione/AOO. La gestione delle utenze rispetta i seguenti criteri operativi:

- tutti gli utenti possono consultare ed inserire documenti in base al ruolo di appartenenza;
- esiste un ruolo specifico per l'annullamento dei protocolli, assegnato al personale dell'ufficio protocollo;
- solo gli amministratori posso effettuare la cancellazione di protocolli.

Politiche di sicurezza adottate dalla AOO

Responsabilità

La responsabilità delle azioni compiute nella fruizione del servizio di protocollo è dell'utente fruitore del servizio.
Gli utenti autorizzati ad accedere al servizio di protocollo dispongono di una propria credenziale personale (userid e password).
La richiesta delle credenziali per l'accesso al PdP deve essere effettuata dal dirigente/responsabile il quale definisce il profilo di accesso e le relative autorizzazioni in merito alla visibilità ed alla gestione delle informazioni che l'utilizzatore deve avere.
Ogni nuovo utente autorizzato viene registrato secondo una specifica procedura con la quale vengono annotate le informazioni relative all'utente e ai ruoli di appartenenza.
Le credenziali per l'accesso non devono mai essere cedute a terzi. La responsabilità delle operazioni compiute tramite un'utenza è sempre del legittimo titolare, anche se compiute in sua assenza.

Postazioni di lavoro degli utenti del servizio

Per la corretta fruizione del servizio di protocollo informatico e di gestione documentale e al fine di tutelarne l'accesso è necessario che l'utente adotti almeno le seguenti buone norme di comportamento relative alla gestione del proprio posto di lavoro:

- la stazione di lavoro non deve essere lasciata incustodita, anche per brevi periodi, con la sessione attiva;
- prima di allontanarsi, anche momentaneamente, devono essere attivati i sistemi di protezione esistenti relativamente alla stazione di lavoro (ad esempio, blocco tramite Ctrl-Alt-Canc).

In generale, deve essere adottata la politica della cosiddetta "scrivania pulita" che obbliga a non lasciare materiale riservato incustodito al di fuori dell'orario di lavoro e invita a riporre il materiale di lavoro (documenti, supporti) negli appositi armadi, secondo il livello di sicurezza, di disattivare o bloccare la stazione di lavoro, di tenere chiusi i locali.