Allegato 4

Piano di sicurezza dei documenti informatici

La normativa attualmente da prendere in considerazione consiste in :

Codice della Amministrazione Digitale, D.Lgs. 82/2005 e s.m.i;
Misure Minime di Sicurezza ICT per le pubbliche amministrazioni , DPCM 1 agosto 2015;
D.P.C.M. 03/12/2013, regole tecniche su protocollo informatico e conservazione;
DPCM 13/11/2014, regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici;
Regolamento Europeo per la Protezione dei Dati Personali EU 679/2016 (GDPR).

Il Piano di sicurezza garantisce che:

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

Le misure adottate e finalizzate a rendere sicuro il sistema informatico in relazione alla formazione e alla conservazione del protocollo e dei documenti informatici vengono raggruppate in base alla:

1. Sicurezza Fisica
2. Sicurezza Organizzativa
3. Sicurezza Logica

1. SICUREZZA FISICA

Il ruolo della sicurezza fisica è quello di proteggere le persone che operano sui sistemi, le aree e le componenti del sistema informativo. Essa è stata suddivisa in due parti: Sicurezza di area e sicurezza delle apparecchiature hardware.

- **Sicurezza di area**

Le chiavi di accesso ai locali sono distribuite al personale dei Servizi Informatici. L'applicativo ed il database sono duplicati e mantenuti sincronizzati giornalmente in due siti: via Garibaldi 114, Rieti e via Saredo 52, Roma

- **Sicurezza delle apparecchiature hardware**

I locali in cui sono situate le apparecchiature garantiscono la protezione delle stesse da danneggiamenti accidentali o intenzionali, durante la permanenza del personale dipendente. Gli impianti di alimentazione sono protetti da un gruppo di continuità. elettrica.

Tutti i dispositivi sono coperti da un servizio di manutenzione che garantisce tempi brevi di intervento per il ripristino delle funzionalità in caso di guasto.

2. SICUREZZA ORGANIZZATIVA

La sicurezza organizzativa è attualmente in fase di revisione al fine di ottemperare al Regolamento Europeo per la Protezione dei Dati Personali. In primis verrà eseguita la nomina del DPO (Data Protection Officer).
I controlli sulla consistenza e affidabilità degli apparati rimane comunque in carico al Responsabile dei Servizi Informatici.

3. SICUREZZA LOGICA

Per sicurezza logica si intende il sottosistema di sicurezza finalizzato all'implementazione dei requisiti di sicurezza nelle architetture informatiche, dotato quindi di meccanismi opportuni e di specifiche funzioni di gestione e controllo.

L'architettura si basa sulla realizzazione di servizi di sicurezza, ovvero su funzioni garantite dal sistema utilizzato.

I servizi attivi sono i seguenti:

- controllo e limitazione accessi
- autenticazione
- confidenzialità
- integrità

Le modalità tecniche attraverso le quali è possibile realizzare i servizi di sicurezza sono le seguenti:

- meccanismi per il controllo degli accessi
- meccanismi per l'autenticazione
- meccanismi di salvataggio dati
- meccanismi di protezione dati e software

Meccanismi per il controllo e limitazione degli accessi

Il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informatico avvengano esclusivamente secondo modalità prestabilite. Il controllo degli accessi viene visto come un sistema caratterizzato da soggetti (utenti, processi) che accedono a oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione). Gli operatori del protocollo, in base alla struttura di appartenenza, hanno abilitazioni di accesso differenziate, secondo le tipologie di operazioni che essi sono autorizzati ad effettuare. Ad ogni operatore è assegnata una "login" ed una "password" d'accesso al sistema informatico di gestione del protocollo. Ogni operatore, identificato dal sistema informatico di gestione del protocollo attraverso la propria login, è responsabile della corrispondenza dei dati desunti dal documento protocollato con quelli immessi nel programma di protocollo, e della corrispondenza del numero di protocollo di un documento all'immagine o file del documento stesso archiviato nel sistema informatico. I livelli di autorizzazione sono assegnati dal Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi, secondo i principi contenuti nel presente documento.

Le abilitazioni possono limitare le seguenti attività:

L'utente abilitato visualizza una registrazione di protocollo, con l'esclusione dei documenti riservati; l'utente abilitato inserisce i dati e provvede ad una registrazione di protocollo oppure al completamento dei dati di una registrazione di protocollo; l'utente è abilitato a modificare tutti o alcuni dei dati gestionali di una registrazione di protocollo, con l'esclusione dei dati obbligatori (cioè numero e data di protocollo, oggetto, mittente/destinatario, riferimenti del protocollo ed eventualmente l'impronta digitale); l'utente è abilitato ad annullare una registrazione di protocollo oppure i dati relativi a mittente/destinatario, oggetto del documento e ai riferimenti del protocollo.

Gli operatori di protocollo, in base al loro livello di abilitazione, sono:

- il Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi (responsabile DAG);
- i Protocollatori;
- i Consultatori;

Un ruolo a parte è riservato al Responsabile informatico della sicurezza dei dati del protocollo informatico (responsabile USI) e agli amministratori di sistema.

Il Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi

Il Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi, in quanto supervisore del protocollo, ha tutte le abilitazioni consentite dal programma di gestione del protocollo, in particolare quelle di:

- individuare, in attuazione delle direttive della struttura richiedente, gli utenti da abilitare, attribuendo loro un livello di autorizzazione all'uso di funzioni della procedura, secondo gli uffici di appartenenza, distinguendo tra quelli abilitati alla consultazione dell'archivio, o di parti di esso, da quelli abilitati anche all'inserimento, modifica e aggiunta di dati;
- disporre, in coordinamento con il responsabile informatico della sicurezza dei dati del protocollo informatico, di cui al comma successivo, affinché le funzionalità del sistema in caso di guasti o anomalie siano ripristinate al più presto, di norma entro 24 ore dal fermo delle attività di protocollazione;
- garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di protocollazione;
- autorizzare le operazioni di annullamento e di modifica del protocollo;
- controllare l'osservanza delle disposizioni contenute nel presente documento da parte del personale addetto;
- promuovere la formazione e l'aggiornamento degli operatori;
- promuove, periodicamente, opportune verifiche sulle tipologie di documenti protocollati.

Protocollatori

Sono tutti gli addetti degli uffici protocollo dell'Agenzia. Le abilitazioni concesse sono:

- immissione protocollo in entrata, uscita e posta interna se non sono state previste eventuali restrizioni;
- modifica ed annullamento dei protocolli già inseriti su autorizzazione del RSP;
- ricerca dati;
- visione di tutti i documenti archiviati se non sono state previste eventuali restrinzioni.

Consultatori

Sono tutti gli altri utenti di ARPA Lazio che utilizzano il protocollo informatico. Le abilitazioni concesse sono:

- ricerca dati;
- visione dei documenti di competenza dell'ufficio o di tutti gli uffici a seconda delle limitazioni imposte.

Responsabile dei Servizi Informatici – Amministratori di sistema

Il Responsabile dei Servizi Informatici e gli amministratori di sistema svolgono i seguenti compiti:

- garantiscono la funzionalità del sistema di gestione del protocollo informatico;
- provvedono a ripristinare al più presto le funzionalità del sistema in caso di interruzioni o anomalie;
- effettuano le copie e cura la conservazione delle stesse su supporto informatico removibile.

Le abilitazioni consentite dal programma sono possedute dagli Amministratori del sistema e consistono in:

- immissione protocollo in entrata, in uscita e posta interna;
- annullamento di protocolli già inseriti solo se autorizzati dal Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi;
- ricerca dati; visione di tutti i documenti archiviati;
- gestione delle tabelle degli operatori e della relativa definizione delle abilitazioni;
- creazione e tenuta delle login e password di tutti gli operatori. gestione;
- tenuta della tabella degli indirizzi e-mail per l'inoltro della corrispondenza

Meccanismi per Autenticazione

Per garantire quanto sopra esposto, il sistema informatico agenziale è basato su un meccanismo che costringe ogni utente ad autenticarsi (cioè dimostrare la propria identità) prima di poter accedere ad un calcolatore. Ogni nome utente è associato ad una ed una sola password, disabilitata dagli amministratori di sistema qualora non sia più autorizzata.

Confidenzialità

Ogni utente autorizzato può accedere ad un'area di lavoro riservata per il settore di appartenenza a cui hanno diritto di accesso i soli componenti del gruppo di appartenenza. Egli può inoltre impostare particolari restrizioni di accesso ai file.

Integrità fisica

L'integrità fisica dei dati viene garantita con un duplice meccanismo. L'applicativo per la gestione del protocollo dispone di un meccanismo tramite il quale ogni dato viene memorizzato contemporaneamente su due archivi digitali residenti in due sedi dell'Agenzia. L'applicativo è programmato per effettuare, con frequenza giornaliera, la copia di backup della banca. Inoltre mensilmente sono effettuate operazioni di salvataggio della banca dati su supporto informatico removibile da parte del Responsabile dei Servizi Informatici o degli addetti alle operazioni di copia. Il Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi vigila sulla corretta esecuzione delle operazioni di salvataggio della banca dati.

I supporti magnetici vengono conservati in cassaforte ed in un locale separato.

Integrità logica

L'integrità logica si ottiene con il meccanismo di verifica dei privilegi di accesso ai file, garantito dal sistema operativo e con il sistema antivirus.

Ogni utente, superata la fase di autenticazione, avendo accesso ai propri dati residenti nella propria area di lavoro, non può accedere alle aree non di competenza.