COMUNE DI
GUSPINI

SERVIZIO SEGRETERIA, AFFARI GENERALI

INNOVAZIONE TECNOLOGICA – SERVIZIO SISTEMI INFORMATIVI, E-GOVERNMENT E COMUNICAZIONE

MANUALE DI GESTIONE

PROTOCOLLO, DOCUMENTI ED ARCHIVIO

AI SENSI DEL D.P.C.M. 3 DICEMBRE 2013

ALLEGATO 02 – PIANO DI SICUREZZA

INDICE

1. PIANO DI SICUREZZA

Nel presente allegato sono riportate 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.

1.1. OBIETTIVI DEL PIANO DI SICUREZZA

Il piano di sicurezza ha lo scopo di garantire:

- l'integrità e la riservatezza, oltre che la disponibilità, dei documenti e delle informazioni trattate dall'AOO;
- la custodia dei dati personali comuni, sensibili e/o giudiziari al fine di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, sia pure 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.

1.2. GENERALITÀ

Il Piano per la sicurezza informatica, redatto ai sensi della normativa vigente, è contenuto nel "Documento Programmatico sulla Sicurezza dei dati (DPS)", la cui ultima versione è quella approvata con deliberazione della Giunta Comunale n. 161 del 14.07.2011.

Il piano di sicurezza contenuto nel DPS:

- descrive le competenze dalla AOO;
- è basato sulle risultanze delle analisi dei rischi a cui sono esposti i dati e i documenti trattati, e sulle direttive impartite dal Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi per la AOO;

Definisce pertanto:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- gli aspetti operativi della sicurezza, con particolare riferimento alle misure minime di sicurezza, di cui all'Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" del D.Lgs 196/2003 "Codice in materia di protezione dei dati personali";
- i piani specifici di formazione degli addetti;
- le modalità esecutive delle attività di monitoraggio dell'efficacia e dell'efficienza delle misure di sicurezza da effettuarsi periodicamente;

Venuti meno gli obblighi a seguito dell'abrogazione dell'art. 50 bis del CAD (D.Lgs 82/2005) resta in piedi la necessità di mantenere adeguate le misure di sicurezza, pertanto il piano di sicurezza, sarà

comunque soggetto a revisione ogni qualvolta intervengano eventi (sia di natura organizzativa che normativa, nonché tecnologica) che ne determinino la non adeguatezza.

1.3. FORMAZIONE DEI DOCUMENTI INFORMATICI AMMINISTRATIVI DAL PUNTO DI VISTA DELLA 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'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 nuove eventuali AOO.

In fase di creazione, gestione e conservazione del documento si applicano le regole per la formazione, l'archiviazione e la trasmissione dei documenti con strumenti informatici e telematici di cui al DPCM 13 novembre 2014.

1.4. GESTIONE DEI DOCUMENTI INFORMATICI

Il sistema operativo utilizzato per l'erogazione del servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente:

Il sistema operativo del server che ospita i files utilizzati come deposito dei documenti è configurato in maniera che sia consentito:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non abbia in mai accesso 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 ai fini di con 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;
- assicura 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.

Per la gestione dei documenti informatici all'interno dell'AOO, il Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi fa riferimento alle norme stabilite dal Responsabile del sistema informativo dell'Amministrazione.

1.4.1. COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte dai tecnici professionisti del CED per l'erogazione del Gestionale di Protocollo informatico.

Nella conduzione del servizio destinato ad erogare il Gestionale di Protocollo informatico, le qualifiche funzionali individuate sono:

- responsabile della sicurezza;
- responsabile della tutela dei dati personali;

1.4.2. COMPONENTE FISICA DELLA SICUREZZA

Il controllo degli accessi fisici dalle risorse del CED è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti non possono entrare e trattenersi nell'area protetta se non accompagnati dal personale del CED autorizzato;

1.4.3. COMPONENTE LOGICA DELLA SICUREZZA

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, nel Gestionale di Protocollo Informatico, viene realizzata attraverso l'attivazione dei seguenti servizi di sicurezza che prevengono i possibili danni derivanti delle minacce sulle vulnerabilità del sistema informatico:

- identificazione, autenticazione ed autorizzazione degli addetti della AOO;
- riservatezza dei dati;
- integrità dei dati;
- integrità del flusso dei messaggi;
- non ripudio dell'origine (da parte del mittente);
- non ripudio della ricezione (da parte del destinatario).

Il sistema prevede un sistema centralizzato per l'identificazione, l'autenticazione e l'autorizzazione degli addetti della AOO, con le seguenti caratteristiche:

- un unico login server per la gestione dei diritti di accesso ai servizi applicativi;
- unico sistema di repository delle credenziali di accesso degli utenti;
- unico database delle anagrafiche contenente tutti i profili utenza.

1.4.4. COMPONENTE INFRASTRUTTURALE DELLA SICUREZZA

Presso il centro servizi dell'erogatore sono disponibili i seguenti impianti:

- Antincendio;
- Continuità elettrica;
- Controllo degli accessi e dei varchi fisici.

Essendo il centro servizi lontano da insediamenti industriali e posto all'interno di un edificio adibito ad uffici, le sue condizioni ambientali per quanto riguarda polvere, temperatura, umidità, vibrazioni meccaniche, interferenze elettriche e radiazioni elettromagnetiche e livelli di inquinamento chimico e biologico, sono tali da non richiedere misure specifiche di prevenzione oltre quelle già adottate per le sedi di uffici di civile impiego.

1.4.5. GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO E DI SICUREZZA

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo presenti o transitate sul Gestionale di Protocollo che occorre mantenere, sia dal punto di vista regolamentare, sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul Gestionale di Protocollo, 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, (sensori di rete e firewall);
- dalle registrazioni dell'applicativo Gestionale di Protocollo.

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:

- l'accesso alle registrazioni è limitato, esclusivamente, ai sistemisti o agli operatori di sicurezza addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- le registrazioni sono elaborate tramite procedure automatiche da parte degli operatori di sicurezza;
- l'accesso dall'esterno da parte di persone non autorizzate non è consentito in base all'architettura stessa del servizio, essendo controllato dal sistema di autenticazione e di autorizzazione e dal firewall;
- i supporti con le registrazioni di sicurezza sono conservati all'interno di un armadio ignifugo in un locale con controllo biometrico per l'accesso;
- i log di sistema sono accessibili ai sistemisti in sola lettura al fine di impedirne la modifica;

- l'operazione di scrittura delle registrazioni del Gestionale di Protocollo, è effettuata direttamente dagli applicativi;
- le registrazioni sono soggette a copia giornaliera su disco e a salvataggio su supporto ottico rimovibile;
- il periodo di conservazione del supporto ottico è conforme alla normativa vigente in materia.

Una volta avviati gli iter di conservazione dei documenti informatici di cui al punto 1.7 non occorrerà più provvedere alla memorizzazione su supporto ottico dei log.

1.5. TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti delle AOO 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. A fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre AOO, 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 certifica del fornitore esterno (provider) di cui si avvale l'AOO, 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 i ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO 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.

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 o altra firma elettronica a disposizione delle amministrazioni coinvolte nello scambio di messaggi.

1.5.1. ALL'ESTERNO DELLA AOO (INTEROPERABILITÀ)

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 (art. 55, comma 4, ed art. 60 del DPR 28 dicembre 2000 n. 445 e art. 10 del DPCM 3 dicembre 2013 riguardante il protocollo).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalla 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 3 dicembre 2013 riguardante il protocollo, 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 fatta salva la possibilità di avvalersi della modalità di trasmissione dei documenti informatici in cooperazione applicativa secondo quanto previsto dal DPCM 1 aprile 2009 recante le regole tecniche per il funzionamento del Sistema Pubblico di Connettività (SPC) e secondo gli standard e il modello architetturale di cui agli artt. 72 e seguenti del D.LGS. 7 marzo 2005 n. 82.

La trasmissione dei documenti informatici firmati digitalmente e inviati attraverso l'utilizzo di posta elettronica è regolata dalla circolare dell'AgID n. 60 del 23 gennaio 2013.

1.5.2. 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 organizzativi di riferimento (UOR) della AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica ordinaria (PEO) 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.

1.6. ACCESSO AI DOCUMENTI INFORMATICI

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso, pubblica (UserID) e privata (Password) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Queste, in sintesi, sono:

- consultazione, per visualizzare in modo selettivo, le registrazioni di protocollo eseguite da altri;
- inserimento, per inserire gli estremi di protocollo e effettuare una registrazione di protocollo ed associare i documenti;
- modifica, per modificare i dati opzionali di una registrazione di protocollo;
- annullamento, per annullare una registrazione di protocollo autorizzata dal Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi (RSP).

Le regole per la composizione delle password e il blocco delle utenze valgono sia per l'amministratore dell'unica AOO che per gli utenti delle AOO.

Le relative politiche di composizione, aggiornamento e, in generale di sicurezza, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.

Il gestionale di protocollo fruito dall'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 da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una Access Control List (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

Considerato che il gestionale di protocollo segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo ufficio organizzativo di riferimento (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'AOO.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca full text.

1.6.1. UTENTI INTERNI ALLA AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi dell'AOO. Questi livelli sono distinti in:

- abilitazione alla consultazione;
- abilitazione all'inserimento;
- abilitazione alla cancellazione e alla modifica di informazioni.

La gestione delle utenze prevede che gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta esplicita dell'amministratore dell'AOO o per errori di inserimento).

1.6.2. ACCESSO AL REGISTRO DI PROTOCOLLO PER GLI UTENTI INTERNI ALL'AOO

L'autorizzazione all'accesso ai registri di protocollo viene regolata con i seguenti criteri:

- *liste di competenza.* Queste sono gestite dall'amministratore di AOO, e vengono utilizzate per la definizione degli utenti abilitati ad accedere a determinate voci del titolario. Attualmente il gestionale in uso non consente tale tipo di profilazione;
- *ruoli degli utenti.* Questi sono gestiti dall'amministratore di ente (Amministrazione), per la specificazione delle macro-funzioni alle quali vengono abilitati;
- protocollazione "particolare o riservata". Questa è gestita dall'amministrazione di ente, relativa a documenti sottratti alla consultazione da parte di chi non sia espressamente abilitato.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di "Responsabile del registro" e limitatamente al registro dall'AOO sul quale è abilitato ad operare.

L'utente assegnatario dei documenti protocollati è invece abilitato ad una vista parziale sul registro di protocollo.

L'operatore che gestisce lo smistamento dei documenti può definire riservato un protocollo ed assegnarlo per competenza ad un utente assegnatario.

Nel caso in cui sia effettuata una protocollazione riservata la visibilità completa sul documento è possibile solo all'utente a cui il protocollo è stato assegnato per competenza e ai protocollatori che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo).

Tutti gli altri utenti (seppure inclusi nella giusta lista di competenza) possono accedere solo ai dai di registrazione (ad esempio: progressivo di protocollo, data di protocollazione) mentre vedono mascherati i dati relativi al profilo di protocollo (ad esempio: classificazione).

1.6.3. UTENTI ESTERNI ALLA AOO – ALTRE AOO / AMMINISTRAZIONI

Attualmente non sono attive o previste altre AOO. Nel caso queste venissero attivate, l'accesso al sistema di gestione informatica dei documenti dell'Amministrazione da parte di altre AOO avverrà secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui agli art. 72 e seguenti del D.Lgs. 7 marzo 2005 n. 82 nel rispetto dei principi di cooperazione applicativa.

1.6.4. UTENTI ESTERNI ALLA AOO – PRIVATI ACCESSO CIVICO

Non sono al momento disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.

L'accesso civico è il diritto riconosciuto a qualunque cittadino di richiedere documenti, informazioni e dati, oggetto di pubblicazione obbligatoria ai sensi della normativa vigente in materia di Trasparenza (D.Lgs. n. 33 del 14 marzo 2013), nei casi in cui l'amministrazione pubblica interessata non li abbia pubblicati sul proprio sito web istituzionale.

1.7. CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La conservazione dei documenti informatici avverrà attraverso il conferimento dei documenti da inviare in conservazione presso un conservatore accreditato. E' attualmente in fase di attivazione l'iter per la conservazione, nel rispetto delle modalità e delle tecniche specificate dal DPCM 3 dicembre 2013 "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" nonché a quanto indicato dal DPCM 13 novembre 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 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"

1.7.1. CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO

Per quanto attiene la conservazione del registro di protocollo è già attivo un iter di invio in conservazione sostitutiva del registro di protocollo. L'invio avviene giornalmente secondo la normativa vigente.

1.7.2. CONSERVAZIONE DELLE REGISTRAZIONI DI SICUREZZA

In attesa dell'attivazione del sistema di conservazione di cui al 1.7, un operatore del CED, provvede con periodicità almeno mensile, alla memorizzazione su supporto ottico dei seguenti oggetti:

- i file contenenti i log originali;
- le firme dei file.