

## Sommario

1. - Premessa
2. - Il piano di sicurezza
  - 2.1 - Revisione e modifica del piano di sicurezza
  - 2.2 - Revisione e modifica delle politiche di sicurezza
3. - Componenti e configurazioni del sistema informatico
  - 3.1 - Caratteristiche di sedi e locali
  - 3.2 - Locale CED e componenti server
  - 3.3 - Connettività
  - 3.4 - Archivi
  - 3.5 - Posta elettronica
  - 3.6 - Posta elettronica certificata
  - 3.7 - Sicurezza perimetrale
  - 3.8 - Sistemi di protezione da malware
  - 3.9 - Sistemi e politiche di backup
  - 3.10 - Log e tracciamento delle attività
  - 3.11 - Accesso logico alle reti e ai sistemi
  - 3.12 - Sistemi di autenticazione
  - 3.13 - Modalità di accesso remoto
  - 3.14 - Lavoro Agile / Smart Working
  - 3.15 - Inventario degli asset e postazioni di lavoro
  - 3.16 - Notebook, smartphone e altri supporti mobili
  - 3.17 - Responsabilità degli utenti e formazione

## **1 - Premessa**

Il presente Piano della Sicurezza (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica del Parco Regionale del Serio.

Lo scopo del documento è quello di poter stabilire, attuare, mantenere e migliorare in modo continuo il sistema di gestione per la sicurezza delle informazioni. Il sistema di gestione della sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità delle informazioni mediante l'applicazione di un processo di gestione del rischio e dà fiducia alle parti interessate sull'adeguatezza della gestione dei rischi.

## **2 - Il piano di sicurezza**

Le Pubbliche Amministrazioni, nell'ottica di sviluppare concretamente il Sistema di gestione informatica dei documenti, devono predisporre: "Il Piano per la sicurezza informatica" relativo alla formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici, nel rispetto delle misure minime di sicurezza previste nel GDPR (Regolamento Europeo per la protezione dei dati 679/2016). Il suddetto Piano deve essere predisposto dal Responsabile della gestione documentale, d'intesa con il Responsabile della conservazione e il Responsabile del trattamento dei dati personali.

La sicurezza di un sistema informativo è da intendersi come:

- La protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali.
- La limitazione degli effetti causati dall'eventuale occorrenza delle cause sopraindicate.

La sicurezza informatica è una caratteristica globale in grado di fornire il desiderato livello di disponibilità, integrità e riservatezza dei dati, informazioni, documenti e dei servizi erogati.

### **2.1 - Revisione e modifica del piano di sicurezza**

Periodicamente l'Ente effettua la revisione del piano sicurezza al fine di assicurarne la continua idoneità, adeguatezza ed efficacia o, in ogni caso, ad ogni variazione significativa della struttura informatica.

### **2.2 - Revisione e modifica delle politiche di sicurezza**

Tutta la documentazione, ed in particolare le politiche di sicurezza, vengono riesaminate periodicamente mediante un'apposita pianificazione o quando al verificarsi di cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

Il riesame comprende una valutazione delle opportunità di miglioramento delle politiche dell'organizzazione e dell'approccio alla gestione della sicurezza delle informazioni in risposta ai cambiamenti dell'ambiente organizzativo, dei servizi erogati, delle clausole legali o dell'ambiente tecnico.

Revisione delle politiche estemporanee vengono effettuate nei seguenti casi:

- verificarsi di incidenti di sicurezza
- variazioni tecnologiche significative;
- modifiche all'architettura informatica;
- aggiornamenti delle prescrizioni normative;
- risultati delle eventuali attività di audit interni.

### **3 - Componenti e configurazioni del sistema informatico**

In questo paragrafo vengono descritte le risorse e le configurazioni in essere che compongono o supportano il sistema informatico.

#### **3.1 - Caratteristiche di sedi e locali**

Il Parco Regionale del Serio attualmente ha una sede in Piazza Rocca n.1 a Romano di Lombardia, n. 03 Centri Parco: uno a Romano di Lombardia in località Pascolo (denominato "Orto Botanico", uno a Casale Cremasco in Via Roma (denominato "Museo dell'Acqua") e uno a Crema in Viale Santa Maria della Croce, n.14 (denominato "Casa di Camperia") a cui si aggiunge la sede delle Guardie ecologiche Volontarie in Località Pascolo a Romano di Lombardia.

Sistemi antincendio - I sistemi antincendio sono costituiti da estintori dislocati in vari punti degli edifici.

#### **3.2 - Locale CED e componenti server**

Il Server fisico, presso la sede dell'Ente, è posizionato all'interno di apposito armadio Rack chiuso a chiave, che a loro volta risiedono all'interno di un apposito locale adibito a CED.

L'Amministratore di Sistema esterno all'Ente mantiene l'elenco dei server e dei dispositivi attivi presso l'Ente e lo aggiorna in caso di variazione, controllandone periodicamente lo stato e la correttezza al fine di garantirne l'affidabilità e la corrispondenza alla situazione esistente, specificando se il server presenta caratteristiche di sicurezza e continuità di mantenere la documentazione descrittiva.

L'Ente inoltre ha dotato la parte server di gruppi di continuità, in modo da permettere la tenuta o lo spegnimento controllato dei dispositivi ad essi collegati in caso di mancanza di energia elettrica.

#### **3.3 - Connettività**

La gestione delle linee dati è affidata al Settore Finanziario, che ne tiene costantemente monitorato lo stato e ne tiene aggiornato l'elenco.

Tale elenco contiene la descrizione e le caratteristiche di ogni linea, le informazioni riguardo il fornitore che ne cura la manutenzione e gli eventuali dettagli contrattuali rilevanti, insieme alle eventuali specifiche di sicurezza.

### **3.4 – Archivi**

L'amministratore di Sistema tiene monitorato l'aggiornamento degli archivi e delle banche dati principali dell'Ente.

In un elenco aggiorna le informazioni rilevanti e caratteristiche di ogni banca dati quali: funzione, fornitore, ubicazione, effettuando quindi verifiche di attendibilità e correttezza dell'elenco attraverso controlli a campione o verifiche complete.

### **3.5 - Posta elettronica**

Le caselle di posta elettronica vengono gestite attraverso un software installato sul server, tramite il quale l'amministrazione di sistema (esterno) cura, per quanto di competenza, sia la gestione amministrativa delle caselle e di configurazione del sistema, sia la gestione degli aspetti legati alla sicurezza. L'amministratore di sistema (esterno) mantiene l'elenco con le caratteristiche del sistema di posta e delle caselle.

Ogni dipendente ha un indirizzo di posta nominale.

La creazione di una nuova casella avviene tramite apposita richiesta al Settore Ecologia e Ambiente, tramite richiesta scritta.

### **3.6 - Posta elettronica certificata**

Anche le caselle di PEC sono gestite tramite un fornitore accreditato esterno (.....). La casella `parco.serio@pec.regione.lombardia.it` sono direttamente integrate al software di protocollo informatico e fatturazione elettronica, quindi, il backup dei messaggi avviene seguendo il naturale percorso di gestione dei relativi flussi documentali. La continuità operativa e la manutenzione del servizio sono gestite a livello contrattuale con il fornitore.

### **3.7 - Sicurezza perimetrale**

Il sistema informatico dell'Ente è protetto tramite l'utilizzo di firewall di rete, appositamente configurati per gestire la sicurezza perimetrale e, nel caso, l'applicazione di opportuni content filtering gestiti ed avvallati dall'Amministratore di Sistema (Esterno).

Anche le configurazioni dei firewall sono mantenute dall'amministratore di Sistema che ne effettua una copia prima di ogni modifica, oltre a prevedere e pianificare gli aggiornamenti e tenerne monitorato il corretto funzionamento.

I sistemi di sicurezza perimetrale sono coperti da apposito contratto di assistenza e manutenzione.

### **3.8 - Sistemi di protezione da malware**

Presso le postazioni di lavoro e i server dell'ente è installato e attivo un sistema antivirus. Il software, cloud-based, viene gestito a livello centralizzato dall'Amministratore di Sistema, che ne cura gli aggiornamenti, le installazioni sulle postazioni ed il monitoring delle segnalazioni e dei risultati delle scansioni.

In occasione di criticità relativa a virus o malware l'Amministratore di Sistema adotta le azioni opportune ed effettua le comunicazioni del caso, sia a livello di formazione e consapevolezza.

### **3.9 - Sistemi e politiche di backup**

La gestione dei backup viene effettuata dall'Amministratore di Sistema, per ciò che riguarda i dati che risiedono presso l'Ente, e dai fornitori esterni i servizi dati in concessione esterna o su cloud.

L'Ente, mediante apposito software Altaro Backup, mantiene l'elenco delle risorse sottoposte a backup e delle relative procedure adottate per l'esecuzione delle copie di salvataggio, oltre ad effettuare verifiche giornaliere della corretta esecuzione dei processi di backup ed effettuare una verifica periodica della correttezza delle impostazioni dei sistemi di backup e della adeguatezza dei processi di backup.

Periodicamente viene effettuato un riesame delle risorse sottoposte a backup, in modo da assicurare che venga salvata la totalità dei dati facenti parte del sistema informatico; la definizione ed il mantenimento di quali sono i dati che si riferiscono al sistema spetta all'Amministratore di Sistema.

I backup vengono effettuati con cadenza giornaliera presso supporti di rete e in cloud; più precisamente è stata implementata la strategia 123, che prescrive di:

1. Possedere almeno tre copie dei propri dati.
2. Conservare le copie su due supporti diversi.
3. Conservare una copia del backup offline. realizzandola in questo modo:
  1. Prima copia dati, compreso il cluster di Sintesi, su un Nas (Network-attached Storage) in sala server;
  2. Seconda copia dati su Nas custodito nella saletta tecnologica su supporto USB con 15 giorni di storico.
  3. Terza copia dei dati (offline) su cloud

### **3.10 - Log e tracciamento delle attività**

L'Amministratore di Sistema accede ai log generati da applicativi, sistemi operativi e apparati specifici, disciplinati attraverso una specifica politica che regola i tempi e le modalità di creazione, gestione, eliminazione salvataggio e conservazione, nonché una specifica procedura che determini le modalità ed i tempi di definizione delle analisi e delle modalità di salvataggio e conservazione dei log delle nuove risorse messe a disposizione dall'Ente.

Periodicamente l'Amministratore di Sistema effettua un riesame dell'elenco dei log e delle procedure adottate per la loro gestione.

Su ogni personal computer e server è installato un software per la gestione delle patch di sistema e controllo delle applicazioni installate e lo stato dello stesso.

### **3.11 - Accesso logico alle reti e ai sistemi**

L'accesso alla rete può avvenire esclusivamente tramite un processo di autenticazione che prevede un nome utente ed una password. La password è composta da almeno otto caratteri alfanumerici e non deve contenere riferimenti agevolmente riconducibili all'assegnatario.

L'Amministratore di sistema gestisce l'assegnazione delle password di accesso al sistema informatico.

Nome utente e password sono strettamente personali.

L'utente è tenuto a:

- Non comunicare a terzi la password;
- A non annotare la password su supporti posti in vicinanza della propria postazione di lavoro o comunque incustoditi.

La password di accesso alla rete viene cambiata autonomamente ogni 3 mesi secondo quanto stabilito dalla normativa vigente.

In caso di assenza, anche temporanea, del personale incaricato dei trattamenti dei dati, sui P.C. devono essere chiuse le procedure di accesso ai dati o attivato il blocco attraverso lo screen saver con password.

Le credenziali di accesso ai sistemi informatici sono rilasciate su richiesta che avviene tramite la compilazione di format specifici - che gestiscono anche i processi di autorizzazione e revoca - a seconda dei servizi per i quali si richiede l'accesso.

### **3.12 - Sistemi di autenticazione**

Gli utenti autorizzati accedono alle risorse informative dell'Ente tramite diversi livelli di autenticazione, a seconda dei privilegi autorizzativi che vengono loro rilasciati.

In generale, l'accesso alle postazioni di lavoro, ai sistemi di navigazione internet e ai documenti residenti sul file server (cartelle di rete condivise), viene disciplinato in fase di rilascio delle credenziali da parte dell'Amministratore di Sistema, previa apposita richiesta fatta pervenire dal Responsabile di Settore.

### **3.13 - Modalità di accesso remoto**

L'Amministratore di Sistema si occupa della gestione e del controllo degli accessi effettuati da parte di terze parti e manutentori esterni del sistema informatico. Di volta in volta, in base alle specifiche attività da effettuare l'Amministratore di Sistema autorizza l'accesso alle risorse, fisiche e logiche, del sistema informatico con credenziali identificate e con livelli di autorizzazione minimi per l'attività che deve essere effettuata.

### **3.14 - Lavoro Agile / Smart Working**

La modalità del lavoro agile è abilitata in casi di emergenza e/o nel rispetto della normativa contrattuale e nazionale vigente, nonché della regolamentazione dell'Ente. L'Amministratore di Sistema fornisce gli strumenti necessari per permettere agli utenti di effettuare connessioni sicure con il sistema dell'Ente.

### **3.15 - Inventario degli asset e postazioni di lavoro**

L'Amministratore di Sistema mantiene aggiornato, tramite l'utilizzo e la configurazione di un apposito software, un inventario delle risorse hardware e software presenti presso l'Ente.

L'Amministratore di Sistema definisce, aggiorna e utilizza delle configurazioni standard per l'installazione di tutti gli apparati (firewall, switch, etc.), dispositivi (server, memorie di rete, etc..) e postazioni di lavoro (fisse, mobili).

Le postazioni sono tenute in costante aggiornamento dall'Amministratore di Sistema, che ha il compito, inoltre, di segnalare prontamente quando queste hanno bisogno di essere sostituite con delle nuove, evitando così di rappresentare una minaccia alla sicurezza dell'Ente.

Le utenze ed i privilegi agli utenti vengono gestiti a livello centralizzato dall'Amministratore di Sistema, che li assegna a seconda delle effettive necessità e competenze, concordate con gli appositi Responsabili di Settore.

### **3.16 – Notebook, smartphone e altri supporti mobili**

Ai dipendenti e alle Guardie Ecologiche Volontarie possono essere forniti dispositivi mobili, quali notebook.

Il Settore Ecologia e Ambiente tiene aggiornato l'elenco degli strumenti di supporto mobile o memorizzazione esterna forniti in dotazione.

La corretta gestione di questi strumenti, la custodia e le metodologie di protezione delle informazioni in esse contenute sono gestite dal Settore Ecologia e Ambiente stesso, attraverso adeguate azioni di informazione agli utenti finali sui rischi che corrono utilizzando tali strumenti.

### **3.17 - Responsabilità degli utenti e formazione**

Nel piano formativo definito annualmente dall'Ente sono talvolta previste sessioni formative relative all'utilizzo sicuro delle risorse informatiche del personale.