Automobile Club Ponente Ligure

PIANO DI SICUREZZA
Allegato al Manuale di Gestione Documentale

1. Scopo e Ambito di Applicazione

Il presente Piano per la Sicurezza Informatica costituisce parte integrante del Manuale di Gestione Documentale, in ottemperanza alle disposizioni vigenti in materia di gestione e conservazione dei documenti informatici.

La sua redazione è prevista dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, emanate da AgID. Nello specifico, il paragrafo 3.4, "Compiti del responsabile della gestione documentale", stabilisce che il responsabile della gestione documentale (o il coordinatore, ove nominato) ha il compito di predisporre il Manuale di gestione documentale, il quale "conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza". Tale previsione è ulteriormente dettagliata nel paragrafo 3.9, "Misure di sicurezza", che ribadisce i requisiti per tale piano.

Il Piano di Sicurezza ha lo scopo di garantire la protezione, l'affidabilità e la resilienza del sistema di gestione informatica dei documenti dell'Amministrazione. In particolare, il Piano è finalizzato a:

- contrastare le minacce di natura informatica (ICT) che possono compromettere l'integrità, la disponibilità e la riservatezza delle informazioni;
- assicurare la protezione dei dati personali trattati nell'ambito della gestione documentale, in conformità alla normativa vigente;
- tutelare la corretta formazione, gestione, accessibilità e conservazione dei documenti informatici, quale patrimonio informativo dell'Amministrazione.

Il Piano è redatto in conformità alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate da AgID, nonché alla Circolare AgID n. 2/2017 – Misure minime di sicurezza ICT per le pubbliche amministrazioni, adottando i principi e le misure ivi previsti come quadro di riferimento per la sicurezza.

Il documento si colloca nell'ambito del più ampio Piano generale di sicurezza dell'Amministrazione, con il quale è integrato e coordinato. Esso è inoltre elaborato in coerenza con le linee di indirizzo strategiche del Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente, al fine di assicurare un approccio unitario e armonizzato alla gestione della sicurezza informatica, alla continuità operativa e alla protezione del patrimonio informativo dell'Ente.

2. Riferimenti Normativi Principali

Il Piano di Sicurezza si basa sulle seguenti normative:

- Circolare AGID 18 aprile 2017, n. 2/2017 – "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (Maggio 2021), in particolare i paragrafi 3.9 (Misure di sicurezza per la gestione documentale) e 4.11 (Misure di sicurezza per la conservazione).
- Regolamento (UE) 2016/679 (GDPR) – In particolare gli artt. 28, 32, 33 e 34, relativi alla protezione dei dati personali, all'adozione di misure di sicurezza adeguate al rischio e alla gestione delle violazioni dei dati.
- D.lgs 82/2005 e ss.mm.ii. (Codice dell'Amministrazione Digitale - CAD).

3. Ruoli e Responsabilità in Materia di Sicurezza ICT

L'Automobile Club Ponente Ligure (Titolare del Trattamento):

- è responsabile dell'adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza idoneo al rischio.
- il Responsabile della Gestione Documentale: ha la responsabilità dell'attuazione delle misure minime di sicurezza ICT. Predispone il piano della sicurezza del sistema di gestione informatica dei documenti, d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali;
- il Responsabile della Conservazione: predispone il piano della sicurezza del sistema di conservazione, di concerto con il responsabile della transizione digitale, il responsabile della gestione documentale e acquisito il parere del responsabile della protezione dei dati personali;
- [nome della Software House Esterna] (Responsabile del Trattamento):
    - è formalmente individuata come Responsabile del trattamento dei dati ai sensi dell'art. 28 del Regolamento UE 679/2016.
    - deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del GDPR e garantire la tutela dei diritti dell'interessato.
    - è incaricata dell'implementazione e della manutenzione delle misure di sicurezza ICT per i sistemi e le infrastrutture gestite.

Le misure di sicurezza adottate e le responsabilità specifiche sono definite chiaramente nel contratto di servizio o nella convenzione con [nome della Software House Esterna];
il Responsabile della Protezione dei Dati Personali (DPO): fornisce parere sul piano e sulle misure in relazione alla protezione dei dati personali.

4. Misure Minime di Sicurezza ICT (Livello Essenziale)

Le misure di sicurezza devono essere tecniche e organizzative, adeguate al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione.

4.1. Inventario e Gestione degli Asset

Inventario dei Dispositivi e Software Autorizzati: Mantenere un elenco aggiornato di tutti i computer, stampanti, e altri dispositivi connessi alla rete, indicando la proprietà e l'ubicazione. Identificare tutto il software installato sui sistemi, distinguendo tra autorizzato e non autorizzato.
Configurazione Standardizzata: Assicurare che tutti i computer abbiano configurazioni standardizzate e documentate, gestite dalla [nome della Software House esterna].

4.2. Protezione della Configurazione

Hardening dei Sistemi: [nome della Software House esterna] deve garantire che i sistemi operativi e le applicazioni sui computer siano configurati in modo sicuro, disabilitando servizi non necessari e implementando le migliori pratiche di sicurezza.

Controllo delle Modifiche: qualsiasi modifica alle configurazioni standard deve essere autorizzata e documentata.
Limitazione dei Privilegi: gli utenti devono operare con i privilegi minimi necessari per svolgere le proprie mansioni.

4.3. Gestione delle Vulnerabilità

Aggiornamenti Regolari: [nome della Software House esterna] è responsabile di garantire che i sistemi operativi, i browser e le applicazioni siano costantemente aggiornati con le ultime patch di sicurezza per eliminare vulnerabilità note.
Software Antimalware Aggiornato: Assicurare che su ogni computer sia installato e regolarmente aggiornato un software antivirus/antimalware.

4.4. Gestione degli Accessi (Utenti e Amministratori)

Identificazione e Autenticazione: ogni utente deve avere credenziali univoche (username e password complesse). [nome della Software House esterna] deve implementare meccanismi di autenticazione robusti.
Principio del Minimo Privilegio: gli account utente devono avere solo i diritti necessari per le proprie mansioni. Gli account amministrativi devono essere usati solo quando strettamente necessario.
Protezione degli Account Amministrativi: Le credenziali amministrative devono essere gestite con la massima cautela dalla Software House, possibilmente con autenticazione a più fattori.
Tracciamento degli Accessi: Il sistema di protocollo informatico deve garantire l'univoca identificazione e autenticazione degli utenti e il tracciamento permanente di qualsiasi evento di modifica delle informazioni e l'individuazione del suo autore.

4.5. Difese contro il Malware

Antivirus/Antimalware: Implementazione e gestione centralizzata di soluzioni antivirus e antimalware da parte della [nome della Software House esterna] su tutti i dispositivi. Le definizioni devono essere aggiornate frequentemente.
Email Security: filtri antispam e antimalware per la posta elettronica, gestiti dalla [nome della Software House esterna].
Consapevolezza degli Utenti: Sensibilizzazione degli utenti sui rischi del malware (es. phishing, allegati sospetti).

4.6. Copie di Sicurezza (Backup)

Backup Regolari: La [nome della Software House esterna] deve implementare e gestire una procedura di backup regolare e automatica di tutti i dati essenziali (documenti, configurazioni, database).
Verifica dei Backup: I backup devono essere regolarmente verificati per assicurarne l'integrità e la recuperabilità.
Conservazione Sicura: Le copie di sicurezza devono essere conservate in luoghi sicuri e distinti dai sistemi originali, preferibilmente con almeno una copia off-site.
Test di Ripristino: almeno annualmente, deve essere effettuato un test di ripristino di una porzione di dati per validare l'efficacia della procedura.

4.7. Protezione dei Dati Rilevanti

Identificazione Dati Sensibili: Identificare i documenti e i dati contenenti informazioni personali o sensibili che richiedono una protezione maggiore.
Controllo degli Accessi ai Dati: Implementare controlli granulari sugli accessi ai dati basati sui ruoli degli utenti.
Pseudonimizzazione/Cifratura: Valutare con la Software House l'opportunità e la fattibilità di pseudonimizzare o cifrare dati personali, se del caso, per aumentarne la protezione.

Monitoraggio: Monitorare attività sospette sui dati rilevanti per prevenire esfiltrazioni.

5. Gestione degli incidenti informatici e delle violazioni dati

Procedura di Incident Response: La [nome della Software House esterna] deve disporre di una procedura definita per la gestione degli incidenti informatici, inclusa la rilevazione, l'analisi e la risposta agli attacchi.

Notifica delle violazioni: In caso di violazione dei dati personali (data breach), la [nome della Software House esterna] è tenuta a informare tempestivamente l'Automobile Club Ponente Ligure. L'Automobile Club Ponente Ligure, a sua volta, dovrà procedere alla notifica all'Autorità di controllo (Garante Privacy) entro 72 ore e, se del caso, alla comunicazione agli interessati, secondo gli artt. 33 e 34 del GDPR. Questa procedura deve essere descritta nel dettaglio nel contratto con la Software House e nel piano generale di sicurezza.

Tracciamento: tutte le operazioni e le modifiche ai dati devono essere tracciate per permettere l'analisi post-incidente.

6. Continuità Operativa e Ripristino

Ripristino tempestivo: Il piano deve assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico.

Registro di emergenza: In caso di malfunzionamento del sistema di protocollo informatico, deve essere prevista la possibilità di utilizzare un registro di emergenza manuale, con procedure definite per il recupero dei dati nel sistema informatico una volta ripristinato il servizio.

7. Monitoraggio e Aggiornamento

Verifica periodica: La [nome della Software House esterna] e l'Automobile Club Ponente Ligure devono collaborare per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative adottate, con una cadenza almeno annuale o in occasione di cambiamenti significativi.

Aggiornamento del piano: Il presente Piano di Sicurezza deve essere sottoposto a revisione e aggiornamento periodico (almeno annuale) o in caso di cambiamenti normativi, tecnologici o organizzativi rilevanti, per garantire che rimanga efficace e allineato ai rischi.

8. Specifiche per la [nome della Software House esterna]

Contratto di Servizio: Il contratto con la [nome della Software House esterna] dettaglia esplicitamente le responsabilità in materia di sicurezza ICT e protezione dei dati, includendo:

- le misure tecniche e organizzative che la Software House si impegna ad adottare.
- le procedure di backup e ripristino.
- le procedure di gestione degli incidenti e di notifica delle violazioni dei dati.
- l'obbligo di fornire garanzie sufficienti in termini di qualità e sicurezza.
- la conformità della [nome della Software House esterna] al Regolamento UE 679/2016 e alle misure minime di sicurezza AGID come modello di riferimento.

Documentazione: La [nome della Software House esterna] deve fornire all'Automobile Club Ponente Ligure la documentazione relativa alle architetture e alle infrastrutture utilizzate, alle procedure di gestione e di evoluzione, nonché alle misure di sicurezza adottate per i sistemi gestiti.