ALLEGATO A

Ordine Ingegneri della Provincia di Imperia

Piano della Sicurezza Informatica

Emissione del documento

Azione	Data	Nominativo	Funzione
Redazione	*20/12/2018*	*Ing. Simone Zanella*	*Responsabile della sicurezza informatica*
Approvazione	*18/12/2018*	*Consiglio dell'Ordine degli Ingegneri della Provincia di Imperia*	*Ente*

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1 - Bozza	17/11/2018	Prima stesura	
2 - Bozza	06/12/2018	Revisione	
3	20/12/2018	Versione revisionata, con delibere approvazione.	

INDICE

1. PREMESSA
2. NORMATIVA E STANDARD DI RIFERIMENTO
3. ORGANIZZAZIONE DEL SISTEMA DI CONSERVAZIONE
    3.1 Ruoli, responsabilità e formazione del personale
4. PERIMETRO DEL SISTEMA DI CONSERVAZIONE
    4.1 Infrastruttura tecnologica informatica di rete
    4.2 Piano di Manutenzione delle infrastrutture
    4.3 Organizzazione della sicurezza dei dati
    4.4 Misure adottate per la protezione e la sicurezza dell'infrastruttura informatica di rete
        4.4.1 Backup
        4.4.2 Firewall
        4.4.3 Antivirus
        4.4.4 Aggiornamenti software
        4.4.5 Sistema di autenticazione
    4.5 Disaster Recovery e Continuità Operativa
5. ANALISI DELLE MINACCE E DELLE VULNERABILITÀ DELL'INFRASTRUTTURA INFORMATICA DI RETE
6. POLITICHE DI SICUREZZA
    6.1 Protezione fisica delle risorse
    6.2 Protezione logica delle informazioni
    6.3 Norme per il personale

1. PREMESSA

Il presente Piano della Sicurezza (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) dell'Ente "Ordine Ingegneri della Provincia di Imperia" esclusivamente per quanto attiene le attività di conservazione documentale ex DPCM 3 dicembre 2013 e, quindi, inerenti quanto definito nell'ambito del Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni). Pertanto, ogni indicazione contenuta nel PdS è da intendersi riferita, ove altrimenti non indicato, esclusivamente alle predette attività di conservazione documentale.

Il Piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dalla'Ente siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano 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, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Il documento, allegato al Manuale di Gestione Documentale dell'Ente, riprende e approfondisce i contenuti dei paragrafi VIII, IX, X del Manuale.

2. NORMATIVA E STANDARD DI RIFERIMENTO

Normativa di riferimento

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD) e in particolare art. 50 bis;
- Decreto del Presidente del Consiglio dei Ministri 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 ex al Decreto Legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l’accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Standard di riferimento

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l’archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V 1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- ETSI TR 101 533-2 V 1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The *Dublin Core* metadata element set, Sistema di metadata del *Dublin Core*.

3. ORGANIZZAZIONE DEL SISTEMA DI CONSERVAZIONE

Lo svolgimento delle attività di conservatore richiede la presenza di più attori coinvolti nel progetto, ognuno dei quali ha la responsabilità di specifiche attività da svolgere.

Questi ruoli si inseriscono nell'organigramma generale dell'Ente, arricchendo i ruoli e le procedure già previste per la gestione dei processi interni.

Per ogni figura prevista nel processo di gestione del sistema di conservazione sono richiesti specifici requisiti di onorabilità e di esperienza minima nel ruolo. Peraltro, così com'è previsto che alcune attività possano essere svolte dal medesimo soggetto è, altresì, previsto che alcune funzioni possano essere delegate ad altri soggetti, fermo restando i predetti vincoli di onorabilità e di requisiti di esperienza del delegato.

Nell'ambito del personale dell'organizzazione destinato alla gestione del sistema di conservazione è necessario definire quale di questo personale sia dedicato alla sicurezza informatica della conservazione, con le relative responsabilità.

Segue un organigramma dell'organizzazione:

- Responsabile della Sicurezza Informatica (responsabile della sicurezza dei sistemi per la conservazione), incaricato della sicurezza informatica della conservazione:
- Responsabile della Conservazione (responsabile della gestione documentale), incaricato della definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione:
- Responsabile del Trattamento dei Dati Personali, incaricato della elaborazione dei dati personali per conto del Titolare del Trattamento (art. 4, par. 1, n. 8 GDPR).

3.1 Ruoli, responsabilità e formazione del personale

Il Titolare del Trattamento assegna, con proprio provvedimento od ordine di servizio, compiti specifici attinenti il trattamento dei dati e della documentazione e li aggiorna annualmente. Ai dipendenti o membri dell'Ordine nominati incaricati del trattamento dei dati personali sono impartite le disposizioni riguardanti:

- le modalità di conservazione della documentazione;
- le modalità di memorizzazione dei documenti in formato elettronico contenenti dati

personali, specificando quale unico supporto di memorizzazione i dischi dei computer in uso all'Ordine e i dischi di rete ovvero il divieto di utilizzo di supporti removibili e personal computer portatili, per la memorizzazione dei dati in questione;

- la riservatezza dei dati e delle notizie di cui vengono a conoscenza e la non accessibilità a soggetti non autorizzati dello strumento elettronico durante la sessione di trattamento dei dati;
- modalità di predisposizione di atti/provvedimenti amministrativi, destinati alla pubblicazione, nell'osservanza del principio di pertinenza e non eccedenza nell'utilizzo dei dati personali (nonché il principio di indispensabilità se i dati sono sensibili o giudiziari).
- metodi di archiviazione della documentazione in maniera da tutelare e preservare la privacy degli utenti.
- le metodologie di consegna dei documenti agli utenti/cittadini al fine di preservarli dalla diffusione a terzi di notizie riservate.

Il nuovo personale assunto e i nuovi membri incaricati dall'Ordine all'uso del sistema informatico vengono istruiti dal Responsabile del Trattamento sui comportamenti da adottare all' interno dell'Ente secondo quanto sopra esposto.

Il Titolare, inoltre, individua con provvedimento od ordine di servizio, il dipendente o il membro dell'Ordine addetto alla custodia delle passwords. Con lo stesso provvedimento il responsabile del trattamento individua la procedura di disponibilità nella quale vengono indicati i casi e le modalità con cui si potrà accedere alle password.

Il Responsabile della Sicurezza Informatica, valutata l'esperienza, la capacità e l'affidabilità, è individuato quale "Amministratore di Sistema" ai fini della gestione e manutenzione delle strutture informatiche dell'Ente. L'"Amministratore di Sistema" dovrà provvedere a:

- rispettare durante le attività svolte le misure di sicurezza previste dalla Legge;
- garantire la massima riservatezza nel trattamento dei dati;
- individuare per iscritto il/i soggetto/i incaricato/i della custodia delle passwords per l'accesso al sistema informatico e vigilare sulla sua attività;
- impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati

personali e effettuati con strumenti elettronici, conforme lla normativa vigente;

- verificare costantemente che l'Ente abbia adottato le misure minime di sicurezza per il trattamento dei dati personali con strumenti elettronici, provvedendo senza indugio agli adeguamenti eventualmente necessari;
- suggerire, per quanto riguarda l'aspetto informatico, l'adozione e l'aggiornamento delle più ampie misure di sicurezza atte a disporre che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- aggiornare periodicamente, con frequenza opportuna, i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate nell'Ente;
- adottare sistemi idonei alla autenticazione all'accesso ai sistemi di elaborazione e agli archivi elettronici da parte dell' "Amministratore di sistema" e/o suoi incaricati, con password avente privilegi di amministratore di sistema;
- riferire periodicamente, ed in ogni caso con cadenza annuale, al Titolare sullo svolgimento dei suoi compiti, dandogli inoltre piena collaborazione nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate.

Con riferimento alla Formazione del personale, relativamente alla Gestione Documentale, l'Ente garantisce che:

- le iniziative di formazione/aggiornamento siano finalizzate al mantenimento e sviluppo del patrimonio delle conoscenze dell'Ente in un'ottica di formazione continua in grado di recepire le esigenze formative e le evoluzioni normative, istituzionali e tecnologiche;
- la formazione di ogni persona avvenga sulla base di una pianificazione che tenga conto del percorso formativo seguito, della figura professionale di appartenenza e

quindi delle attività che la persona svolge o dovrà svolgere oltreché delle competenze e potenzialità espresse.

Per il personale incaricato del trattamento dei dati sono previsti interventi formativi, da realizzarsi periodicamente e secondo necessità, riguardanti:

- i principi generali in materia di privacy;
- la normativa in vigore;
- le corrette modalità di trattamento dei dati;
- le modalità di accesso ai dati personali;
- i rischi che incombono sui dati personali trattati;
- i comportamenti idonei e le misure adottare per prevenire eventi dannosi.

4. PERIMETRO DEL SISTEMA DI CONSERVAZIONE

4.1 Infrastruttura tecnologica informatica di rete

L'Infrastruttura Tecnologica dell'Ente è interamente collocata presso la sede dell'Ordine e può essere schematizzata come segue:

n° 1 armadio posto in posizione elevata, protetto da serratura, contenente switch di rete, router WiFi, NAS di rete.
N° 2 personal computer utilizzati come postazioni di lavoro per il personale e membri dell'Ordine incaricati,
N° 1 personal computer notebook portatile utilizzato come postazione di lavoro portabile, che può essere utilizzato anche fuori dalla sede dell'Ordine.

I componenti fisici costituenti l'infrastruttura sono:

- Rete LAN 100Mbit su classe di IP 192.168.1.0/24.

- Router con modem Fibra TIM, indirizzo IP 192.168.1.1, con AP che crea doppia rete WiFi: rete "Ordine-IM" protetta con autenticazione con password WPA2, rete guest "Ospiti-Ordine" con autenticazione con password WPA2 con separazione del traffico dalla LAN.

- Switch LAN non amministrabile presente nell'armadio di rete.

- PC Contabilità, dotato di sistema operativo Windows 7, antivirus Kaspersky, contenente il gestionale ISI INFORMATICA dedicato alla gestione contabile, albo e protocollo dell'ordine, con possibilità di accesso da rete esterna alla LAN dell'Ordine a incaricati della società ISI INFORMATICA tramite software di assistenza remota ISI INFORMATICA e Teamviewer.

- PC Segreteria, dotato di sistema operativo Windows 10, antivirus Kaspersky, utilizzato per compiti di segreteria, con connessione via LAN al gestionale ISI INFORMATICA presente sul PC Contabilità.

- PC Notebook, dotato di sistema operativo Windows, antivirus Kaspersky, utilizzato saltuariamente come postazione mobile sia all'interno della LAN dell'Ordine, sia esternamente.

- Stampante di rete Brother con connessione via LAN.

- NAS Zyxel per l’archiviazione di rete, doppio disco da 1 TB in configurazione RAID 1.

Non sono presenti sistemi UPS o antincendio sulla rete.

4.2 Piano di Manutenzione delle infrastrutture

Si prevede un piano di manutenzione della infrastruttura tecnologica con cadenza di almeno 2 volte annue, anche con interventi in connessione remota, affinché sia garantita la riservatezza, la confidenzialità e l’integrità dei dati.

Gli interventi di manutenzione dovranno verificare lo stato dei componenti fisici dell’infrastruttura, il corretto funzionamento degli apparati, dei software di sicurezza e backup e delle configurazioni di rete, anche attraverso l’analisi dei log automatici eseguiti dagli apparati. Particolare attenzione dovrà essere prestata alla verifica delle modalità di accesso ad apparati, postazioni di lavoro, software.

4.3 Organizzazione della sicurezza dei dati

La definizione e l’applicazione delle politiche di sicurezza all’interno dell’Ordine richiedono l’individuazione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, alle procedure d’implementazione e ad altri elementi specifici dell’ambiente e del sistema informativo.

Attualmente, l’individuazione della politica di sicurezza dell’Ordine determina il modello logico della sicurezza fissandone gli obiettivi. La sicurezza viene considerata da tutto il personale, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione. Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

La conversione del Decreto Legge n. 5 del 9 febbraio 2012 (c.d. Decreto semplificazioni), avvenuta con la Legge 4 aprile 2012 n. 35, conferma definitivamente la soppressione

dell’obbligo – in capo a titolari di trattamento di dati sensibili e giudiziari effettuato mediante strumenti elettronici – di redigere, e quindi di tenere aggiornato, il Documento Programmatico sulla Sicurezza (DPS). I titolari del trattamento sono tuttavia ancora tenuti ad osservare tutti gli accorgimenti tecnici e organizzativi idonei a garantirne protezione, privacy e riservatezza.

4.4 Misure adottate per la protezione e la sicurezza dell’infrastruttura informatica di rete

La sicurezza logica si occupa della protezione dell’informazione, dei dati, dei documenti, delle applicazioni, dei sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. La realizzazione della sicurezza logica è pensata in termini architetturali e ciò comporta l’individuazione di tutti i sistemi hardware e software che implementano le attività dei vari servizi dell’Ente, in modo tale da garantirne la fruibilità nel tempo.

4.4.1 Backup

I dati e le informazioni presenti sui dischi locali delle 2 postazioni di lavoro desktop in uso vengono copiati su un dispositivo NAS di rete con doppia unità disco in configurazione RAID 1 giornalmente da una apposita procedura di backup configurata nel sistema operativo.

Le politiche di backup prevedono quanto segue: ogni ciclo di backup è composto da un salvataggio completo effettuato nel fine settimana tra il venerdì sera e la domenica mattina, e salvataggi incrementali settimanali, ad esso logicamente collegati. I salvataggi completi vengono mantenuti sul NAS per un periodo di 6 mesi. Qualora le dimensioni dei backup superino la dimensione del disco di backup si provvederà a segnalare la necessità di aggiungere ulteriori unità di backup o a rimuovere in automatico quelli meno recenti fino alla liberazione dello spazio necessario per i nuovi backup da salvare.

4.4.2 Firewall

Al fine di prevenire intrusioni dall'esterno è attivato il servizio firewall nativo del router WiFi fibra TIM, e i firewall integrati nei sistemi operativi delle 3 psotazioni di lavoro presenti.

4.4.3 Antivirus

Il sistema informatico dell'Ente e i dati personali da esso custoditi sono protetti contro il rischio di intrusione e contro l'azione di programmi di cui all'Articolo 615-*quinquies* del Codice Penale ("*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*"), mediante l'antivirus Kaspersky, acquistato con licenza a rinnovo annuale, installato sulle 2 postazioni desktop e sulla postazione mobile notebook, con aggiornamenti automatici configurati.

4.4.4 Aggiornamenti software

I sistemi operativi delle postazioni sono periodicamente aggiornati automaticamente mediante la procedura di aggiornamento automatico di Windows.

Gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti sono stati correttamente installati. I programmi sono stati impostati in modo da scaricare e aggiornare automaticamente le loro funzionalità garantendone quindi sempre la massima efficacia di funzionamento.

4.4.5 Sistema di autenticazione

Le postazioni di lavoro sono protette da credenziali di autenticazione associate a una parola chiave riservata e conosciuta solamente dai diretti incaricati. La parola chiave è composta da almeno 8 caratteri (consistenti in numeri e lettere) e non contiene riferimenti agevolmente riconducibili all'incaricato o al dipendente, il quale provvederà a modificarla periodicamente e a custodirla segretamente. Ad integrare la protezione sul sistema informativo, i software dell'Ente e gli applicativi web sono dotati di apposite procedure di accesso tramite username e password.

La rete LAN cablata ha attivo un servizio DHCP per l'assegnazione degli indirizzi IP ai

dispositivi che ne fanno richiesta, è configurato nel router un filtraggio a livello di Mac Address che consente solo ai dispositivi registrati dall'Amministratore di Sistema di accedere alla LAN. L'accesso via WiFi alla LAN avviene tramite autenticazione con password di rete WPA2. La comunicazione di tale password a nuovi utenti deve essere registrata e comunicata al Responsabile della Sicurezza Informatica.

L'accesso alla rete WiFi di tipo "guest" avviene tramite autenticazione con password di rete WPA2 a disposizione degli ospiti dell'Ordine degli Ingegneri che ne fanno richiesta. Tale rete viene utilizzata per fornire connettività durante corsi e riunioni aperti a iscritti all'Ordine ed esterni. Il traffico di tale rete è separato dalla LAN dell'Ordine.

4.5 Disaster Recovery e Continuità Operativa

Il Responsabile del Servizio di Gestione Documentale cura che le funzionalità del sistema, in caso di guasto o anomalia, siano ripristinate entro 72 ore dal blocco delle attività e, comunque, nel più breve tempo possibile. A seguito degli accorgimenti tecnologici sopra descritti, il Responsabile della Sicurezza Informatica garantisce un ripristino dei dati entro un tempo massimo di sette giorni.

La procedura per il disaster recovery prevede le seguenti fasi:

- Fase di reazione all'emergenza: si raccolgono le segnalazioni di incidente di cui deve essere immediatamente informato il Responsabile della Sicurezza Informatica. Ciascun evento deve essere analizzato e in caso di gravita' che ne esamina la criticità e ne stima la gravità. Sarà suo compito valutare se l'evento è tale da generare una possibile situazione di emergenza e, quindi coinvolgere il Responsabile del Servizio di Gestione documentale.
- Fase di gestione dell'emergenza e riattivazione dei servizi: il Responsabile della Sicurezza Informatica attua le misure e le procedure necessarie al fine di ripristinare i servizi e salvaguardare l'integrità e la confidenzialità dei dati, coordinandosi con il Responsabile del Servizio di Gestione Documentale che nel contempo valuta se l'incidente richieda la comunicazione verso il personale ed eventuali soggetti terzi coinvolti.
- Fase di ritorno alla normalità: si effettua una analisi dei danni, contestualmente si effettua una verifica dei sistemi interessati dall'incidente, prima di consentirne l'utilizzo dal personale.

5. ANALISI DELLE MINACCE E DELLE VULNERABILITÀ DELL'INFRASTRUTTURA INFORMATICA DI RETE

Si elencano di seguito le principali minacce e rischi cui può essere soggetta l'infrastruttura informatica di rete, indicandone l'impatto:

- Sottrazione di credenziali di autenticazione (Accesso non consentito ai dati, Sottrazione, cancellazione, manomissione, diffusione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: bassa – Rischio: basso.
- Carenza di consapevolezza, disattenzione, incuria (Cancellazione, manomissione e diffusione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: medio – Rischio: medio.
- Comportamenti sleali o fraudolenti (Sottrazione, cancellazione, manomissione, diffusione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: bassa – Rischio: basso.
- Errore materiale (Cancellazione, manomissione e diffusione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: medio – Rischio: medio.
- Malfunzionamenti, indisponibilità o degrado degli strumenti dovuti a comportamenti sleali o fraudolenti (sabotaggio) (Sottrazione, cancellazione, manomissione, diffusione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: bassa – Rischio: basso.
- Malfunzionamenti, indisponibilità o degrado degli strumenti dovuti a guasti dei sistemi complementari (impianto elettrico, apparati) dovuti a degrado/usura dello strumento (Cancellazione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: medio – Rischio: basso.
- Azione di virus informatici o di programmi suscettibili di recare danno (Sottrazione, cancellazione, manomissione, diffusione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: medio – Rischio: medio.
- Accessi esterni non autorizzati con sottrazione di dati (Sottrazione, cancellazione, manomissione, diffusione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: bassa – Rischio: basso.

- Intercettazione di informazioni in rete (Sottrazione, diffusione dei dati) – Impatto: medio – Probabilità della minaccia/vulnerabilità: bassa – Rischio: basso.
- Malfunzionamenti, indisponibilità o degrado degli strumenti dovuti a eventi distruttivi naturali o artificiali (Cancellazione dei dati) – Impatto: medio – Probabilità della minaccia/vulnerabilità: bassa – Rischio: basso.
- Accesso non autorizzato ai locali/reparti ad accesso ristretto (Sottrazione, cancellazione, diffusione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: medio – Rischio: medio.
- Sottrazione di strumenti contenenti dati (Sottrazione, cancellazione, diffusione dei dati) – Impatto: alto – Probabilità della minaccia/vulnerabilità: medio – Rischio: medio.
- Errori umani nella gestione della sicurezza fisica (Cancellazione dei dati) – Impatto: medio – Probabilità della minaccia/vulnerabilità: alta – Rischio: alta.

6. POLITICHE DI SICUREZZA

Gli aspetti fondamentali del sistema di sicurezza sono:

- protezione fisica delle risorse;
- protezione logica delle informazioni;
- norme per il personale.

6.1 Protezione fisica delle risorse

L'obiettivo della protezione fisica delle risorse è quello di proteggere le aree e le componenti del sistema informativo. Generalmente le contromisure di sicurezza fisica possono essere ricondotte a sicurezza dell'area e sicurezza delle apparecchiature.

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi informatici. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle postazioni di lavoro rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

La sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione. Anche la manutenzione dell'hardware rientra in questa area, come anche la protezione da manomissione o furti.

Le contromisure adottate sono le seguenti:

- l'armadio dove trovano alloggiamento gli apparati di rete e il NAS di salvataggio dei backup è chiuso a chiave.
- le chiavi di accesso alla sede dell'Ente sono distribuite ai soli dipendenti dell'Ente e ai membri dell'Ordine che hanno ricevuto specifico incarico o autorizzazione all'accesso.

6.2 Protezione logica delle informazioni

Gli obiettivi della protezione logica delle informazioni sono:

- il controllo degli accessi alle informazioni
- il mantenimento della loro integrità e riservatezza
- la sicurezza nella trasmissione e nelle comunicazioni all'interno dell'Ente e con l'esterno (Internet, fornitori, altri Enti, ecc...)
- la sicurezza delle postazioni di lavoro e dei personal computer
- la tempestiva rilevazione di eventuali incidenti di sicurezza.

Il campo di applicazione della Sicurezza Logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.

Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.

Le contromisure adottate sono le seguenti:

- uso di sistemi RAID nei dispositivi di archiviazione e backup;
- protezione dei sistemi di accesso e conservazione delle informazioni con assegnazione ad ogni utente di una credenziale riservata di autenticazione tramite username e password;
- cambio delle password con frequenza almeno semestrale;
- sistemi di backup giornalieri (incrementali e/o completi), le copie devono essere sottoposte a test periodici di ripristino.
- firewall perimetrale che protegge la LAN da intrusioni esterne;
- postazioni accessibili dall'esterno solo tramite attivazione all'interno della LAN di software per il controllo remoto;

- software anti-virus su ogni personal computer;
- aggiornamento costante dei software in uso e dei sistemi operativi;
- procedure di Continuità Operativa e Disaster Recovery necessario a garantire la continuità del servizio informatico e la disponibilità delle informazioni, evitando o limitando i danni al patrimonio informativo a fronte di una emergenza.
- devono essere stabilite e attuate regole e limitazioni per l'installazione del software da parte degli utenti.

6.3 Norme per il personale

E' necessario stabilire le regole per proteggere l'Ente da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale.

Sono di proprietà dell'Ente i sistemi di accesso ad Internet, la rete locale LAN ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet.

Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Ente e in rapporto con possibili interlocutori del medesimo.

È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Ente. Le regole sono illustrate per proteggere i dipendenti e i membri dell'Ente con incarichi di accesso all'infrastruttura tecnologica informatica del medesimo..

L'uso non appropriato delle risorse strumentali espone l'Ente al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

Politiche di uso del sistema informatico dell'Ente:

- Gli utenti del sistema informatico devono essere informati che i dati da loro creati sui sistemi dell'Ente e comunque trattati, rimangono di proprietà della medesima.

- Gli utenti del sistema informatico sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete LAN e WiFi non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'Amministratore di Sistema ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.
- Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Ente possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.
- Si deve porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.
- E' necessario mantenere le credenziali di accesso in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informatico sono responsabili dell'uso delle proprie credenziali. Le password devono essere cambiate con regolarità almeno ogni 6 mesi.
- Tutte le postazioni di lavoro (PC desktop e portatili) devono essere rese inaccessibili a terzi privi di credenziali di accesso quando non utilizzate dai titolari.
- Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi devono essere esercitate particolari attenzioni.
- Tutti i sistemi di elaborazione (PC, portatili, ecc…) devono essere dotati di un sistema antivirus approvato dal Responsabile della Sicurezza Informatica ed aggiornato.
- Si deve usare la massima attenzione alla posta elettronica e nell'apertura dei file allegati in quanto potrebbero esporsi a virus, phishing, frodi, ecc...
- Non deve essere permesso a personale non autorizzato o privo di incarico di operare sulla propria postazione di lavoro e/o con le proprie credenziali senza la propria presenza e supervisione.
- Si eviti lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, pen drive USB, dischi esterni, ecc...) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'Ente e, anche in questo caso, verificare prima il supporto con un antivirus.
- È proibita l'installazione e l'uso di qualsiasi software non autorizzato dal Responsabile della Sicurezza Informatica.