Titolo documento:

Politica di cybersecurity e protezione dei dati personali

Politica di cybersecurity e protezione dei dati personali

Rif documento	ISMS-DOC-A05-1
Versione	2
Data	20 January 2026
Autore	Net Patrol Italia
Proprietario del documento	Interlaced

Titolo documento:

Politica di cybersecurity e protezione dei dati personali

Revisioni

VERSIONE	DATA	AUTORE REVISIONE	RIEPILOGO DELLE MODIFICHE
1	02/12/2024	Claudio Basso – Net Patrol	Prima emissione
2	20/01/2026	Irene Benedetti – Net Patrol	Revisione e miglioramento

Distribuzione

NOME	TITOLO

Approvazione

NOME	RUOLO	FIRMA	DATA

Titolo documento:

Politica di cybersecurity e protezione dei dati personali

Sommario

Titolo documento:

Politica di cybersecurity e protezione dei dati personali

1. Introduzione

La presente Politica è stata sviluppata in conformità con lo standard ISO/IEC 27001:2022, al Regolamento UE 2016/679 (GDPR) e nel rispetto degli obiettivi stabiliti dalla Direttiva 2022/2555 (NIS2) e rappresenta il quadro di riferimento dei principi, delle linee guida e delle regole adottate da *Interlaced S.r.l.* per la sicurezza delle informazioni e dei sistemi informativi.

La Politica fornisce una guida a tutto il personale di *Interlaced* ed eventuali terze Parti sulle proprie responsabilità riguardo al trattamento di dati personali, alla gestione e all'utilizzo delle risorse informatiche IT e la responsabilità sulla loro proprietà.

Le finalità specifiche della presente Politica sono:

- Stabilire i principi generali, gli obiettivi e le linee guida che orientano l'approccio dell'organizzazione alla sicurezza informatica;
- Assicurare la tutela dei diritti dei soggetti interessati e garantire il rispetto dei principi applicabili al trattamento dei dati personali;
- Definire i criteri per la gestione dei rischi derivanti dal trattamento di dati personali, nonché per la gestione dei rischi di sicurezza delle informazioni;
- Proteggere dati personali e informazioni sensibili da minacce interne ed esterne, intenzionali o accidentali;
- Fornire un quadro integrato per la gestione del rischio di sicurezza delle informazioni, includendo i requisiti relativi alla definizione, attuazione, aggiornamento e documentazione del piano di gestione dei rischi per la sicurezza informatica, così da garantire un approccio unitario e coerente alla gestione dei rischi in ambito ICT e operativo;

Interlaced si impegna a prendere tutte le misure ragionevoli e appropriate necessarie per proteggere i sistemi informatici che supportano le operazioni aziendali e i dati elaborati, archiviati, o trasmessi da tali sistemi.

1. Gestione del rischio

La gestione del rischio è un processo fondamentale per garantire il rispetto dei diritti e delle libertà dei soggetti interessati, la sicurezza delle informazioni e la resilienza delle infrastrutture critiche.

1.1 Gestione del rischio per i soggetti interessati (privacy)

Interlaced si impegna a sottoporre ogni trattamento che possa presentare un rischio elevato per i diritti e libertà delle persone fisiche a valutazione d'impatto sulla protezione dei dati ("DPIA") ai sensi dell'art. 35 GDPR, specie se il trattamento viene svolto con l'uso di nuove tecnologie.

La valutazione di impatto viene comunque svolta a tutti i casi previsti per legge e in tutti i casi specificatamente definiti con Provv. N. 467/2018 dell'Autorità Garante per la Protezione dei Dati personali, pubblicato in G.U. n. 269 del 19 novembre 2018.

Inoltre, in caso in cui il trasferimento di dati al di fuori dello Spazio Economico Europeo possa dare luogo a rischi elevati per i soggetti interessati, *Interlaced* sottopone lo stesso a una preventiva valutazione d'impatto (Transfer Impact Assessment) al fine di valutare e mitigare tali rischi – applicando le necessarie misure di sicurezza, organizzative e legali.

Per specifici dettagli in merito ai criteri, ruoli e responsabilità per lo svolgimento di valutazioni d'impatto sulla protezione dei dati si rimanda al documento "Politica DPIA".

1.2 Gestione del rischio di cybersecurity

In conformità allo standard internazionale ISO/IEC 27001:2022 e altri standard e linee guida internazionali, la gestione del rischio include una serie di attività strutturate e continuative volte a identificare, valutare, mitigare e monitorare i rischi associati alle operazioni e ai sistemi informativi:

1. Identificazione dei rischi: il primo passo prevede la raccolta e l'analisi delle informazioni per individuare potenziali minacce e vulnerabilità. Vengono considerati sia i rischi interni, che quelli esterni, inclusi attacchi informatici, guasti tecnici, errori umani e disastri naturali;
2. Analisi e valutazione dei rischi: una volta identificati i rischi viene valutato l'impatto e la probabilità di occorrenza;
3. Piano di trattamento: la mitigazione dei rischi implica l'implementazione di misure di trattamento e controllo per ridurne la probabilità e l'impatto;
4. Monitoraggio e revisione: la gestione del rischio è un processo dinamico che richiede un monitoraggio continuo e una revisione periodica. È importante valutare l'efficacia delle misure di mitigazione e apportare modifiche in base ai cambiamenti del panorama delle minacce e nelle esigenze organizzative.
5. Comunicazione: tutti i livelli dell'organizzazione sono periodicamente coinvolti e aggiornati relativamente al sistema di gestione per la sicurezza delle informazioni e sul Piano di Trattamento.

Attraverso un approccio sistematico e proattivo, *Interlaced* identifica e definisce misure di mitigazione dei rischi.

2. Ruoli e Responsabilità

Estratto (riferimento documentale riservato): La gestione della sicurezza delle informazioni è supportata da una struttura organizzativa che definisce responsabilità e autorità specifiche, assicurando coordinamento tra funzioni aziendali, processi operativi e gestione del rischio.

2.1 Affidabilità delle risorse umane

I dipendenti di *Interlaced* devono attenersi a specifiche norme di comportamento al fine di assicurare un livello omogeneo di sicurezza, riducendo i rischi connessi a errori umani, in ottemperanza delle procedure aziendali.

Per avere adeguate garanzie che il personale abbia chiare le proprie responsabilità, che sia stato selezionato ed incaricato in modo conforme al ruolo affidatogli e che abbia le competenze necessarie per lo svolgimento delle mansioni assegnategli, *Interlaced* predispone appropriate misure di sicurezza organizzative durante tutto il ciclo di vita aziendale del personale. In particolare:

- All'atto di selezione vengono effettuati controlli sui candidati, in proporzione all'inquadramento e del ruolo aziendale, nel rispetto delle leggi e dei regolamenti pertinenti;
- Almeno per i sistemi informativi e di rete rilevanti, il personale autorizzato ad accedervi è individuato previa valutazione dell'esperienza, capacità e affidabilità e fornisce idonea garanzia del pieno rispetto della normativa in materia di sicurezza delle informazioni e protezione dei dati personali, anche attraverso atti di autorizzazione formale;
- Sono definiti e comunicati al dipendente gli obblighi di riservatezza;
- Si mantiene una gestione continua delle autenticazioni, delle identità digitali e degli accessi, garantendo che solo personale autorizzato e qualificato possa accedere ai sistemi e alle informazioni aziendali.

2.2 Ruoli e Responsabilità di Terze Parti

L'attività svolta da *Interlaced* comporta la possibilità di accesso diretto da parte di terzi ai sistemi informativi aziendali. È dunque fondamentale stabilire i requisiti di sicurezza che devono essere rispettati per la gestione dei rapporti con Terze parti.

Gli accordi con Terzi devono contenere requisiti riguardanti la protezione dei dati. In particolare, i soggetti terzi devono essere disponibili a presentare, su richiesta, il loro piano di sicurezza, le misure di sicurezza implementate e consentire controlli di sicurezza informatica da parte di *Interlaced*.

- Le collaborazioni con Terze parti devono includere l'accettazione da parte del contraente delle norme vigenti, delle modalità operative e delle normative vigenti;
- Devono essere sottoscritti accordi di riservatezza o di non divulgazione validi prima, durante e dopo l'ingaggio in base alla criticità delle informazioni e dei servizi coinvolti;

3. Gestione del rischio della supply chain

Interlaced riconosce che la sicurezza delle informazioni non dipende esclusivamente dalla misure tecniche e organizzative adottate internamente, ma anche dal livello di protezione garantito dai propri fornitori, partner commerciali e soggetti terzi coinvolti nei processi aziendali.

A tal fine, l'organizzazione definisce e implementa un processo di gestione del rischio legato alla supply chain che comprende, in primo luogo, la valutazione preliminare dei fornitori e dei partner strategici prima dell'avvio di qualsiasi collaborazione. Tale valutazione include l'analisi del loro livello di maturità in ambito cybersecurity, delle certificazioni possedute (ad esempio ISO/IEC 27001, ISO 22301, o equivalenti) e delle politiche di sicurezza applicate, nonché la verifica delle misure tecniche e organizzative adottate per la protezione delle informazioni e dei servizi critici.

L'organizzazione adotta inoltre un monitoraggio continuo dei fornitori durante l'intero ciclo di vita del rapporto commerciale, al fine di individuare tempestivamente variazioni nel livello di sicurezza o nuovi rischi emergenti. Questo processo di monitoraggio si basa su verifiche periodiche, aggiornamenti di documentazione e, se necessario, rivalutazioni del rischio.

4. Gestione degli asset

Per "asset" si intendono tutte le risorse tecnologiche, informative e infrastrutturali che contribuiscono al funzionamento dei processi aziendali e al raggiungimento degli obiettivi strategici dell'organizzazione.

Interlaced adotta un approccio sistematico e centralizzato alla gestione degli asset, finalizzato a garantire una visibilità completa sul patrimonio tecnologico e informativo, a minimizzare i rischi legati a utilizzi non autorizzati o non controllati e a supportare le attività di monitoraggio, protezione e risposta agli incidenti.

A tal fine, l'organizzazione mantiene un inventario aggiornato e accurato di tutti gli asset rilevanti, costantemente revisionato e aggiornato in occasione di acquisizioni, modifiche infrastrutturali, dismissioni o cambiamenti significativi nel contesto operativo. In particolare, *Interlaced* mantiene inventari aggiornati di:

- Apparati fisici (hardware) che compongono i sistemi informativi, ivi inclusi dispositivi IT, IoT e mobili;
- Servizi, sistemi e applicazioni software che compongono i sistemi informativi e di rete;
- Servizi informatici erogati da fornitori, ivi inclusi servizi Cloud

Viene inoltre mantenuto un censimento delle apparecchiature e dei dispositivi assegnati agli utenti.

5. Classificazione delle informazioni

Le informazioni possono assumere varie forme, tra cui: dati cartacei conservati su carta, dati archiviati elettronicamente in sistemi informatici e comunicazioni inviate tramite posta. L'organizzazione ha la responsabilità di proteggere le informazioni che detiene ed elabora, utilizzando controlli proporzionati alla sensibilità e alla criticità delle informazioni coinvolte.

Al fine di proteggere tali informazioni, è stato definito un modello di classificazione delle informazioni, così strutturato:

Livello 0	***CLEAR**:* pubblico o non soggetto a classificazione
Livello 1	**GREEN**: Riservato ai membri di una community
Livello 2	**AMBER**: riservato all'organizzazione ed ai suoi clienti
Livello 3	**AMBER+STRICT**: riservato solo all'organizzazione
Livello 4	**RED**: Confidenziale, riservato ai singoli soggetti elencati

Al momento della creazione, tutte le risorse informative devono essere valutate e classificate dal proprietario in base al loro contenuto. La classificazione determinerà come il documento deve essere protetto e a chi deve essere consentito l'accesso. Qualsiasi sistema che consenta successivamente l'accesso a queste informazioni deve indicare chiaramente la classificazione.

Le definizioni delle classi di informazioni sono descritte più in dettaglio nel documento: (*ISMS-A05-12 Procedura di classificazione delle informazioni-v1*).

5.1 Dati personali

È da considerarsi "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile ("soggetto interessato").

Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, attraverso identificativi come il nome, un numero univoco, informazioni relative all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Nel caso in cui un documento, sia cartaceo che digitale, contenga più tipologie d'informazione (dati personali e non personali), troverà comunque applicazione il livello di classificazione e protezione relativo ai dati personali.

5.2 Uso, conservazione e cancellazione dei dati personali

Le finalità, i mezzi e le modalità di conservazione dei dati personali devono essere consistenti con gli obiettivi e criteri delineati nella presente Politica. *Interlaced* mantiene delle politiche interne per determinare il periodo di conservazione massimo e le modalità di cancellazione o distruzione dei dati personali trattati. Il dipartimento legale è incaricato di supervisionare l'implementazione e il rispetto degli obiettivi e dei criteri di uso, conservazione e cancellazione dei dati personali definiti nella presente politica e altre politiche interne.

Le modalità di utilizzo e conservazione di dati personali da parte di *Interlaced* , sia in qualità di Titolare del trattamento che di Responsabile del trattamento sono descritte nel Registro delle attività di trattamento ai sensi dell'art.30 GDPR.

Per le specifiche modalità di conservazione e cancellazione dei dati, nonché per la mappatura dei processi di trattamento dati e per le modalità di aggiornamento periodico del Registro si rimanda ai documenti: *Politica Data Retention* e *Politica di gestione del Registro Trattamento Dati*.

5.3 Trasparenza del trattamento di dati personali

Interlaced assicura che tutte le informazioni rilevanti in relazione al trattamento dei dati personali siano fornite ai soggetti interessati nel momento in cui i dati sono acquisiti. Ove ciò non sia possibile, è assicurata la pubblicazione delle informazioni su apposita sezione del sito web, o nelle modalità che verranno ritenute più opportune in base al contesto, in un formato accessibile e con linguaggio chiaro, conciso e facilmente comprensibile dal pubblico di riferimento.

L'organizzazione garantisce la gestione tempestiva e completa de reclami e delle segnalazioni relative al trattamento di dati personali, nonché alle richieste di esercizio dei diritti previsti dagli artt. 15-22 del GDPR.

Per il dettaglio della gestione delle richieste ai sensi degli artt. 15-22 del GDPR si rimanda al relativo documento: *Procedura gestione Data Rights.*

6. Sicurezza fisica

Interlaced ha definito, mediante opportuna analisi del rischio e con il supporto delle strutture aziendali preposte, criteri e requisiti di sicurezza fisica e ambientale al fine di impedire e/o limitare perdite di dati e di risorse critiche dovute a vulnerabilità nell'ambito del dominio fisico.

L'accesso ai locali ove risiedono strumenti di elaborazione e agli archivi cartacei deve essere consentito solo al personale preposto e autorizzato.

L'accesso alle sedi aziendali deve essere consentito solo previa identificazione della persona che necessita di entrare.

Le aree che ospitano i sistemi di maggiore criticità devono essere localizzate in zone sicure e protette al fine di minimizzare il rischio di perdite o danneggiamenti e utilizzi impropri e non consentiti. I locali che ospitano elaboratori elettronici devono disporre di dispositivi che consentono di:

- Segregare e tracciare gli accessi effettuati dal personale autorizzato;
- Monitorare i tentativi di accesso non autorizzato e di effrazione nei locali.

7. Continuità operativa e ripristino

In un contesto tecnologico e normativo in continua evoluzione, e in considerazione delle potenziali minacce informatiche, tecniche o fisiche, l'organizzazione adotta un approccio strutturato e proattivo alla business continuity e al disaster recovery, finalizzato a prevenire, mitigare e gestire gli eventi che potrebbero compromettere la disponibilità dei sistemi informativi, dei dati e dei servizi essenziali.

L'obiettivo principale delle politiche di continuità di *Interlaced* è garantire che i servizi critici possano proseguire o essere ripristinati in tempi accettabili a seguito di eventi imprevisti, minimizzando l'impatto operativo, economico, reputazionale e normativo.

7.1 Business Continuity Plan

Il Business Continuity Plan (BCP) rappresenta lo strumento attraverso cui *Interlaced* assicura la continuità dei propri servizi essenziali. Il piano definisce:

- L'elenco dei servizi critici e le relative priorità di ripristino;
- I livelli di servizio attesi e gli obiettivi di tempo di ripristino (RTO) e punto di ripristino dei dati (RPO);
- Le misure organizzative e tecniche da attuare per mantenere operativi i servizi o ristabilirli in tempi compatibili con le esigenze aziendali;
- Le responsabilità delle diverse funzioni coinvolte nella gestione dell'emergenza.

Il BCP è soggetto a revisioni periodiche e aggiornamenti ogniqualvolta si verifichino modifiche rilevanti al contesto tecnologico, organizzativo o normativo. Simulazioni e test regolari sono condotti al fine di validare l'efficacia del piano e di garantire la prontezza del personale coinvolto. Si rimanda a*: ISMS-DOC-A05-30-1-Business Impact Analysis Process*", "*ISMS-DOC-A05-30-3-ICT Continuity Incident Response Procedure*", "*ISMS-DOC-A05-30-4-ICT Continuity Plan List*".

7.2 Disaster Recovery Plan

Interlaced ha, in parallelo, adottato un Disaster Recovery Plan (DRP), con l'obiettivo di ripristinare l'operatività dei sistemi informativi e delle infrastrutture digitali a seguito di eventi catastrofici, quali attacchi informatici gravi, incidenti fisici, guasti tecnici critici o disastri naturali. Il DRP definisce:

- le procedure di attivazione del piano e di escalation verso i referenti aziendali;
- le attività necessarie per il ripristino graduale o completo dei sistemi;
- i canali di comunicazione interna ed esterna in situazioni di emergenza.

Il piano viene testato con regolarità per verificarne l'efficacia, individuare eventuali criticità e migliorare le procedure operative.

8. Gestione degli incidenti

Al fine di prevenire qualsiasi evento dannoso derivante da violazioni di dati e incidenti di sicurezza, *Interlaced* adotta procedure e protocolli di gestione per tali eventi.

Al sensi della NIS2, per "incidente" si intende un evento che comprometterebbe la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete accessibili attraverso di essi.

8.1 Piano di Incident Management

Il piano di gestione delle violazioni di dati personali e degli incidenti di *Interlaced* prevede i seguenti elementi, ulteriormente dettagliati anche in specifiche politiche e procedure:

- Pianificazione: definizione di politiche e procedure, formazione del personale, creazione di un team di risposta agli incidenti e l'acquisizione degli strumenti necessari.
- Rilevamento e segnalazione: identificazione tempestiva degli incidenti di sicurezza. Utilizzando strumenti di monitoraggio e rilevamento delle minacce, l'organizzazione deve essere in grado di individuare attività sospette o anomale.
- Contenimento, eradicazione e ripristino: Dopo aver identificato un incidente, è necessario contenerlo per prevenire ulteriori danni. Questo può includere l'isolamento dei sistemi compromessi, la disconnessione delle reti infette e l'applicazione di patch di sicurezza.
- Comunicazione e notifica: La comunicazione efficace durante un incidente è cruciale. È necessario informare tempestivamente tutte le parti interessate, sia interne che esterne. In particolare, è obbligatorio notificare violazioni di dati personali e incidenti alle Autorità competenti, nonché eventualmente ai soggetti interessati, entro i termini di legge previsti da GDPR e NIS2. La trasparenza e la chiarezza nella comunicazione aiutano a mantenere la fiducia e a coordinare le azioni di risposta.
- Post-incidente e miglioramento continuo: Dopo la gestione di un incidente, è importante condurre una revisione post-incidente per valutare l'efficacia della risposta e identificare le aree di miglioramento. Questo include la registrazione della violazione di dati nell'apposito registro interno, l'aggiornamento delle politiche di sicurezza, la revisione dei piani di risposta agli incidenti e la formazione aggiuntiva del personale. L'obiettivo è imparare dagli incidenti per prevenire future occorrenze e migliorare continuamente la postura di sicurezza dell'organizzazione.

Per la specifica procedura di gestione e risposta agli incidenti informatici si rimanda al relativo documento: "*DOC-RS.MA-01 Procedura di Incident Management*", "*Data Breach procedure*". Le istruzioni stabilite in quel documento devono essere utilizzate solo come guida quando si risponde a un incidente. La natura esatta di un incidente e il suo impatto non possono essere previsti con un

elevato grado di certezza, e quindi è importante che venga utilizzato un buon livello di buon senso quando si decidono le azioni da intraprendere.

9. Sicurezza dell'infrastruttura IT

L'infrastruttura IT e le sue principali componenti devono essere adeguatamente protette e ne deve essere mantenuta l'efficacia e l'efficienza nel tempo. Pertanto:

- Le procedure operative, le architetture definite, le configurazioni applicate, devono essere documentate e mantenute aggiornate per garantire l'uso corretto e sicuro delle risorse IT;
- Devono essere pianificate e messe in atto le misure necessarie a garantire un adeguato livello di efficienza e di prestazioni dei sistemi IT, la prevenzione del rischio di malfunzionamenti o di degrado delle funzionalità di sicurezza applicate. Inoltre, tali misure devono assicurare:
    - Il mantenimento dell'efficienza dei sistemi e la loro regolare manutenzione, anche in considerazione del livello di criticità delle informazioni che trattano;
    - Che l'accesso ai sistemi ai fini di amministrazione e manutenzione sia consentito solo al personale preposto e autorizzato;
    - Che il software installato sia provvisto di licenza, conforme alle normative di legge applicabili e fornisca il livello di servizio richiesto;
- È stata individuata una politica di prevenzione a livello aziendale contro software malevoli;
- La valutazione di nuovi prodotti, in sostituzione o integrazione del software di base deve comprende le verifiche delle caratteristiche di sicurezza, affidabilità e disponibilità, in ottica di riduzione della probabilità di eventi dannosi e di miglioramento del livello di sicurezza.

9.1 Misure tecniche

Le misure tecniche comprendono tutte le soluzioni e le tecnologie per proteggere le informazioni e i sistemi da accessi non autorizzati, attacchi informatici e altre minacce. Tali misure includono:

- Controllo degli accessi: implementazione di sistemi di autenticazione robusti, come MFA e la gestione dei privilegi degli utenti, per garantire che solo il personale autorizzato possa accedere alle informazioni sensibili;
- Crittografia: utilizzo di protocolli crittografici per proteggere i dati sia a riposo che in transito;
- Backup e ripristino: implementazione di procedure di backup regolari e strategie di ripristino per garantire che i dati possano essere recuperati in caso di perdita o danneggiamento;
- Sicurezza sei sistemi endpoint: protezione dei dispositivi endpoint (computer, server, dispositivi mobili) tramite software antivirus, anti-malware e patch management);

- Monitoraggio e logging: Attivazione dei sistemi di monitoraggio e registrazione delle attività (logging) per garantire la tracciabilità delle informazioni e facilitare l'analisi in caso di incidenti di sicurezza;
- Aggiornamenti e patch: politiche per l'aggiornamento regolare d sistemi e l'applicazione dele patch di sicurezza per ridurre il rischio di vulnerabilità note.

9.2 Misure organizzative

Le misure organizzative si riferiscono alle politiche, alle procedure e alla cultura aziendale necessarie per garantire un ambiente sicuro e includono:

- Sviluppo e implementazione di politiche e procedure chiare e documentate che stabiliscano aspettative e responsabilità in materia di sicurezza delle informazioni;
- Formazione e sensibilizzazione: programmi di formazione regolari per il personale su tematiche di sicurezza informatica, buone pratiche e procedure da seguire in caso di incidente;
- Valutazione e mitigazione dei rischi: processi regolari di valutazione dei rischi per identificare, analizzare e mitigare i rischi per la sicurezza delle informazioni.
- Audit e controllo: esecuzione di audit interni e controlli di conformità per garantire che le misure di sicurezza siano efficaci e che l'organizzazione rispetti le normative e politiche stabilite;
- Gestione dei fornitori: procedure per la valutazione e gestione della sicurezza dei fornitori e dei partner, assicurando che anche le terze parti che accedono ai sistemi e alle informazioni dell'organizzazione rispettino gli standard di sicurezza adeguati;

10. Formazione e consapevolezza

Al fine di garantire un'ottima ed efficace gestione della protezione dei dati personali e della sicurezza informatica, il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity e del trattamento dei dati personali.

Interlaced attua, aggiorna e documenta un piano di formazione in materia di cybersecurity e protezione dei dati personali per tutto il personale, ivi inclusi gli organi di amministrazione e direttivi.

I programmi di formazione sono regolari e aggiornati, includendo simulazioni di attacchi informatici ed esercitazioni pratiche per migliorare le reattività e la preparazione del personale. Inoltre è importante promuovere una cultura della sicurezza attraverso campagne di sensibilizzazione che evidenziano l'importanza della protezione dei dati e della cybersecurity, incoraggiando comportamenti responsabili.

La consapevolezza e la formazione continua sono elementi chiave per ridurre i rischi e garantire una difesa efficace contro le minacce informatiche. Si rimanda a "*ISMS-FORM-A06-03-50-RegistroTraining*".

11. Conformità e Audit di sicurezza

Interlaced riconosce che la conformità normativa e il monitoraggio costante dell'efficacia delle misure di sicurezza informatica rappresentano elementi essenziali per garantire la resilienza organizzativa e la continuità dei servizi erogati. In tale prospettiva, l'azienda adotta un approccio strutturato e sistematico volto ad assicurare che tutti i processi, le tecnologie e le attività operative siano conformi al quadro regolamentare vigente.

Gli audit saranno di natura interna, condotti dal team di sicurezza o da altre funzioni indipendenti, ed esterna, affidati a soggetti qualificati e indipendenti per garantire un livello di oggettività e trasparenza più elevato.

Gli audit interni vengono pianificati con cadenza almeno annuale e comprendono la verifica dei seguenti aspetti principali:

- Conformità delle procedure aziendali alle normative e agli standard di riferimento;
- Adeguatezza delle misure di sicurezza tecniche e organizzative implementate;
- Efficacia dei processi di gestione del rischio e dei controlli interni;

Al termine di ogni audit viene redatto un rapporto di valutazione contenente le evidenze raccolte, le eventuali non conformità riscontrate e le raccomandazioni per il miglioramento continuo. Tali risultati vengono condivisi con il Responsabile IT e il Consiglio di amministrazione, che provvedono a definire e approvare un piano di azione correttivo con tempi, responsabilità e modalità di verifica del loro completamento.

12. Monitoraggio e revisione

La presente politica è soggetta a monitoraggio continuo e revisioni periodiche per garantire che rimanga efficace e conforme alle normative rilevanti (GDPR, NIS2) e ai sistemi di gestione interni. È fondamentale effettuare audit regolari per valutare l'aderenza alle misure di sicurezza e identificare eventuali aree di miglioramento.

Ogni revisione deve considerare i cambiamenti nel panorama delle minacce informatiche, le nuove normative e le tecnologie emergenti. Inoltre, è importante coinvolgere tutte le parti interessate nel processo di revisione per assicurare che la politica risponda alle esigenze operative e di sicurezza dell'organizzazione.

Gli aggiornamenti della politica sono comunicati tempestivamente a tutto il personale.

Titolo documento:

Politica di cybersecurity e protezione dei dati personali