[Nome della società]

Cybersecurity Policy

[Sottotitolo del documento]

Cybersecurity Policy

Controllo Documentale

Titolo	Cybersecurity Policy
Tipo Documento	Confidenziale
Contatto SimplyIT	E-mail: michele@simplyit.it Tel: +39 049 099 1394

Lista di Distribuzione

Società	Nome Cognome
SimplyIT	Michele Salvalaggio

Tabella delle Revisioni

Rev	Descrizione	Autori	Verificata	Approvata
[Oggetto]	Released	Michele Salvalaggio		

Sommario

Cybersecurity Policy 1
Controllo Documentale 1
Lista di Distribuzione 1
Tabella delle Revisioni 1
Introduzione 3
Finalità del documento 3
Ruoli e responsabilità 3
Valutazione generale 3
Applicabilità 4
Il Cybersecurity Framework 4
Cyber Risk Management 5
Cybersecurity Awareness 6
Revisioni della Sicurezza delle Informazioni 6
Gestione delle Modifiche (Change Management) 6
Gestione delle informazioni 6
Gestione degli asset 7
Cyber Hygene 7
Sicurezza delle reti 7
Gestione delle vulnerabilità 7
Gestione delle patch 7
Identità e accessi 8
Resilienza e ripristino 8
Sicurezza fisica e visitatori 8
Gestione degli incidenti 8
Monitoraggio continuo 9

Introduzione

L'organizzazione è impegnata a garantire la riservatezza, l'integrità e la disponibilità di tutti i propri beni informativi, fisici ed elettronici, nonché la sicurezza del personale, dei fornitori e di tutte le persone coinvolte nelle proprie attività, assicurando il rispetto dei requisiti normativi, operativi e contrattuali.

Finalità del documento

La cybersecurity rappresenta un tema di fondamentale importanza per tutte le funzioni aziendali, incluse le aree di Information and Communications Technology (ICT).
Essa riguarda la protezione delle informazioni e la tutela degli asset informatici e tecnologici dell'organizzazione.
La presente Cybersecurity Policy ha l'obiettivo di stabilire un Cybersecurity Policy Framework da implementare in modo uniforme in tutta l'organizzazione, comprendendo sia i sistemi ICT che quelli operativi.

Ruoli e responsabilità

Valutazione generale

La NIS2 (art. 20 e 21) rafforza in modo esplicito la responsabilità della direzione e degli organi amministrativi, introducendo responsabilità al Consiglio di amministrazione che svolge un ruolo fondamentale nella governance della sicurezza informatica e della resilienza operativa dell'organizzazione. In conformità alla Direttiva (UE) 2022/2555 (NIS2), il CDA è responsabile della supervisione strategica delle misure di gestione del rischio per la sicurezza delle reti e dei sistemi informativi.

- Approva e supervisiona l'adozione di politiche, standard, procedure e linee guida in materia di sicurezza delle informazioni e cybersecurity.
- Approva le strategie e gli investimenti relativi all'implementazione delle misure di gestione del rischio informatico, assicurandone la coerenza con gli obiettivi aziendali e il profilo di rischio dell'organizzazione.
- Supervisiona l'effettiva attuazione delle misure di sicurezza informatica e ne valuta periodicamente l'adeguatezza ed efficacia.
- Garantisce che siano adottate misure adeguate per la tutela della disponibilità, riservatezza e integrità delle reti, dei sistemi informativi e degli asset informativi rilevanti.
- Assicura la conformità alle politiche interne e agli obblighi normativi applicabili in materia di sicurezza informatica, inclusi quelli derivanti dalla Direttiva NIS2 e dalla normativa nazionale di recepimento.
- Approva e supervisiona i piani di gestione degli incidenti, continuità operativa, disaster recovery e cyber resilienza.

- Promuove una cultura della sicurezza informatica a livello organizzativo, sostenendo iniziative di sensibilizzazione e formazione.
- Partecipa a programmi di formazione periodica in materia di sicurezza informatica e gestione del rischio cyber.
- Assume la responsabilità di supervisione in relazione all'adozione e all'attuazione delle misure di sicurezza informatica.

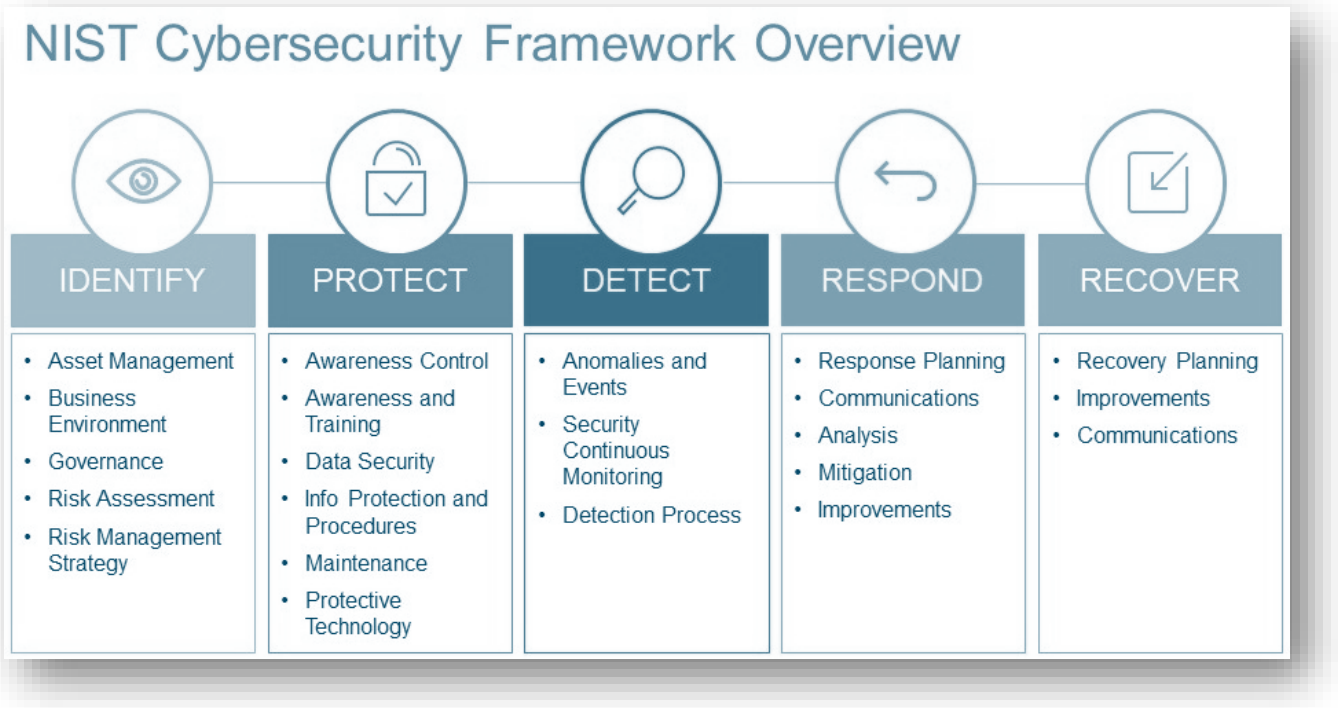
Applicabilità

La presente policy si applica a tutto il personale dell'organizzazione, inclusi dipendenti. Tutti i soggetti rientranti nel perimetro di applicazione sono tenuti a conoscere, rispettare e applicare le linee guida e le misure previste in materia di sicurezza delle informazioni e cybersecurity.

Il Cybersecurity Framework

Gli argomenti trattati nel presente documento sono coerenti con i principi del NIST Cybersecurity Framework (CSF) 2.0, pur senza stabilire una corrispondenza diretta punto per punto. Le attività di sicurezza descritte nel framework possono essere raggruppate in sei funzioni principali, che rappresentano l'approccio complessivo alla gestione della sicurezza informatica:

- Govern (Governare): mantenere un quadro strategico che assicuri la definizione e l'attuazione di ruoli, responsabilità, politiche e strategie per la gestione del rischio informatico.
- Identify (Identificare): sviluppare una comprensione organizzativa che consenta di gestire il rischio informatico relativo a sistemi, persone, asset, dati e capacità operative.
- Protect (Proteggere): sviluppare e implementare misure di salvaguardia adeguate per garantire la sicurezza e la continuità dei servizi critici.
- Detect (Rilevare): sviluppare e implementare attività efficaci per identificare tempestivamente il verificarsi di eventi di sicurezza.
- Respond (Rispondere): sviluppare e implementare azioni appropriate per gestire e mitigare gli incidenti informatici rilevati.
- Recover (Ripristinare): sviluppare e implementare misure per ristabilire le capacità o i servizi compromessi a seguito di un incidente informatico.



Il Cybersecurity Policy Framework definisce la struttura complessiva delle politiche, procedure e linee guida necessarie per garantire un approccio coerente e integrato alla sicurezza informatica in tutta l'organizzazione.
L'obiettivo principale del framework è assicurare che tutti gli aspetti della cybersecurity dalla gestione del rischio alla risposta agli incidenti siano affrontati in modo sistematico, basato su standard riconosciuti a livello internazionale e in conformità con le normative vigenti.

Cyber Risk Management

I rischi associati all'uso delle risorse informatiche in particolare i rischi di natura cyber devono essere inclusi nel processo generale di gestione del rischio dell'organizzazione.
L'approccio alla cybersecurity si basa sull'analisi e valutazione dei rischi informatici e sulla conseguente definizione di misure di protezione proporzionate. Il processo di gestione del rischio informatico deve:

- produrre documentazione formale e prove coerenti e confrontabili;
- essere condotto regolarmente e ogni volta che si verificano modifiche significative ;

In linea con l'articolo 21 della Direttiva NIS2, l'organizzazione deve adottare misure tecniche, operative e organizzative adeguate e proporzionate per:

- gestire i rischi legati alla sicurezza delle informazioni;
- garantire la continuità operativa;
- tutelare la sicurezza della catena di fornitura;
- conformarsi agli standard e alle migliori pratiche internazionali.

Cybersecurity Awareness

La formazione e la consapevolezza in materia di cybersecurity sono obbligatorie per tutto il personale. I programmi di training e sensibilizzazione devono garantire che ciascun ruolo aziendale disponga delle conoscenze, competenze e capacità necessarie per sostenere gli sforzi di sicurezza e mitigare i rischi informatici.
In conformità con gli articoli 20 e 21 della Direttiva NIS2, la dirigenza e gli amministratori di sistema devono partecipare regolarmente a corsi di formazione per mantenere le competenze necessarie alla difesa dell'organizzazione dalle minacce informatiche.
Tali programmi di formazione devono essere aggiornati periodicamente per riflettere:

- l'evoluzione delle pratiche di igiene informatica;
- i nuovi scenari di minaccia;
- le specifiche esigenze dei diversi ruoli aziendali.

Revisioni della Sicurezza delle Informazioni

L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni incluse le politiche, gli standard e i controlli di sicurezza deve essere riesaminato a intervalli pianificati o in occasione di cambiamenti significativi.
Tali revisioni devono essere condotte da personale indipendente rispetto all'area oggetto di verifica, ad esempio tramite la funzione di audit interno o da un ente esterno specializzato.
Le persone incaricate delle revisioni devono possedere competenze ed esperienza adeguate in materia di sicurezza informatica.
I risultati delle revisioni indipendenti devono essere documentati e comunicati alla direzione, e i relativi registri devono essere conservati in conformità con le procedure aziendali.

Gestione delle Modifiche (Change Management)

Gli utenti coinvolti nelle attività di amministrazione, sviluppo o erogazione di risorse tecnologiche devono seguire procedure di gestione delle modifiche appropriate, in modo da garantire che i cambiamenti ai sistemi vengano implementati in modo tempestivo, controllato ed efficace, riducendo al minimo gli errori connessi.

Gestione delle informazioni

La gestione della sicurezza delle informazioni richiede una struttura organizzativa chiaramente definita, con ruoli e responsabilità stabiliti a supporto del quadro di sicurezza complessivo.
Ciò deve garantire:

- Definizioni coerenti delle politiche di sicurezza, applicabili in tutte le situazioni e a tutti i livelli dell'organizzazione;
- Linee di riporto chiare, che assicurino percorsi di escalation efficaci per la gestione e la risposta agli incidenti di sicurezza;

- Ruoli e responsabilità ben definiti per tutto il personale, in relazione al mantenimento dell'integrità e dell'efficacia continua del sistema di sicurezza delle informazioni.

Gestione degli asset

Un asset è definito come qualsiasi piattaforma, sistema o dispositivo coinvolto nell'elaborazione delle informazioni, inclusi hardware, software e dati. Tutti gli asset devono essere identificati e mantenuti in un inventario aggiornato, al fine di garantire una gestione corretta e la mitigazione dei rischi.

Cyber Hygene

Per garantire un ambiente tecnologico sicuro e resiliente, tutti i dipendenti devono attenersi ai seguenti requisiti di cyber hygene. Queste misure sono fondamentali per ridurre i rischi derivanti da un utilizzo improprio dei dispositivi, da una gestione inadeguata delle credenziali o da comportamenti non sicuri nell'uso degli asset aziendali.
Tutti i dispositivi aziendali e personali utilizzati per attività lavorative devono essere configurati in modo sicuro e in linea con gli standard dell'organizzazione.

Sicurezza delle reti

Come indicato nell'articolo 21 della Direttiva NIS2, garantire una sicurezza di rete solida è essenziale per la protezione delle infrastrutture e dei servizi critici. Gli amministratori di rete devono gestire, controllare e segmentare le aree di rete di loro competenza per ridurre il rischio di accessi non autorizzati o di trasferimento improprio di informazioni protette.
Solo gli asset autorizzati, siano essi dispositivi o software, sono ammessi all'interno delle reti aziendali. La difesa dei confini di rete rappresenta l'insieme dei controlli necessari per garantire adeguate misure di protezione all'ingresso della rete aziendale, al fine di proteggerla dalle minacce informatiche.

Gestione delle vulnerabilità

I proprietari e gli amministratori dei sistemi devono garantire che i processi di gestione delle vulnerabilità siano seguiti per correggere le vulnerabilità di sicurezza nelle risorse tecnologiche di cui sono responsabili. Ciò include l'implementazione di controlli per gestire proattivamente le vulnerabilità di rete, sistema e applicazioni.

Gestione delle patch

Tutti i componenti dei sistemi e il software devono essere protetti dalle vulnerabilità note installando patch di sicurezza fornite dai fornitori o controlli compensativi appropriati.
Il patching riguarda il processo di modifica di programmi o applicazioni per aggiornare,

correggere o migliorare le vulnerabilità di sicurezza. Deve essere eseguito secondo le migliori pratiche di settore.

Identità e accessi

L'accesso agli asset informativi e alle risorse tecnologiche che li memorizzano o li elaborano è concesso solo a utenti autorizzati, secondo le esigenze operative. L'identità degli utenti deve essere confermata prima di accedere a dati non pubblici.
I dipendenti sono responsabili della sicurezza dei dati di cui hanno gestione. I dati riservati devono essere protetti contro accessi o utilizzi non autorizzati, applicando crittografia e restrizioni di accesso.

Resilienza e ripristino

Le capacità di resilienza e ripristino dei sistemi tecnologici devono essere regolarmente verificate e i piani aggiornati per minimizzare la perdita di dati o le interruzioni delle operazioni aziendali in caso di incidente. I dati importanti e le configurazioni sono sottoposti a backup e recuperabili secondo i piani.

Sicurezza fisica e visitatori

Devono essere definiti perimetri di sicurezza e/o barriere fisiche con controlli di accesso appropriati per proteggere le aree contenenti informazioni sensibili (ad esempio informazioni segrete o riservate) e per prevenire accessi fisici non autorizzati o rischi derivanti da minacce ambientali (ad esempio furti, incendi, esplosivi).
Devono essere predisposte procedure adeguate per lavorare in aree sicure, al fine di garantire la sicurezza fisica e ambientale. Le apparecchiature devono essere protette da interruzioni di corrente o altri disservizi, e solo il personale di manutenzione autorizzato deve avere accesso alle aree in cui sono collocate. Le apparecchiature, le informazioni o il software possono essere portati fuori sede solo con autorizzazione preventiva. I dipendenti che ospitano visitatori sono responsabili di assicurarsi che gli ospiti siano registrati alla reception, che indossino il badge identificativo in modo visibile e che siano sempre accompagnati.

Gestione degli incidenti

Gli incidenti di sicurezza devono essere identificati e gestiti in modo costante ed efficace in conformità con le linee guida sulla sicurezza, al fine di proteggere le informazioni e ridurre al minimo l'impatto sulle attività operative, la policy di riferimento è la Incident Response Plan.

Monitoraggio continuo

Gli eventi di sistema devono essere registrati e conservati per consentire il monitoraggio, l'analisi e l'investigazione di attività non autorizzate, supportati da soluzioni EDR. Secondo l'Articolo 10 della Direttiva NIS2, il monitoraggio continuo deve rilevare incidenti significativi che potrebbero influenzare servizi essenziali. L'organizzazione deve garantire che i sistemi di monitoraggio forniscano avvisi tempestivi e report alle autorità competenti, con alta disponibilità garantita tramite un LOG Management System.