

POL Politica di sicurezza delle informazioni

Nome della società	NettunoPA
Data di entrata in vigore	10/08/2024

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	10/08/2024	-- N / D --	Daniele Rapillo	Davide Dossena

Scopo

Lo scopo della presente politica è dichiarare e comunicare l'impegno del Top Management verso la protezione degli asset informativi dell'organizzazione. Questo documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e di supportare gli obiettivi strategici aziendali.

Indice

- 1. Campo di Applicazione
- 2. Riferimenti Normativi
- 3. Termini e Definizioni
- 4. Ruoli e Responsabilità
- 5. Obiettivi di sicurezza delle informazioni
- 6. Principi fondamentali di sicurezza delle informazioni
 - 6.1. Impegno del Top Management e Organizzazione
 - 6.2. Approccio Basato sul Rischio
 - 6.3. Sicurezza delle Risorse Umane
 - 6.4. Uso Accettabile delle Risorse e Protezione degli Asset
 - 6.5. Gestione degli Incidenti e Continuità Operativa
 - 6.6. Framework delle Politiche Specifiche
 - 6.7. Principi per i Servizi Cloud
 - 6.8. Revisione e Miglioramento Continuo
 - 6.9. Comunicazione
- 7. Archiviazione e Aggiornamenti
- 8. Documenti di Riferimento

1. Campo di Applicazione

La presente politica stabilisce i principi e gli obiettivi strategici per la gestione della sicurezza delle informazioni all'interno di NettunoPA. Il suo scopo è proteggere gli asset informativi aziendali e dei clienti, garantendo la continuità del business e minimizzando i rischi. Questo documento si applica a tutto il personale, ai processi, ai dati e alle tecnologie che rientrano nel perimetro del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), in conformità con i requisiti della norma ISO/IEC 27001 e della Direttiva NIS2.

2. Riferimenti Normativi

- ISO/IEC 27001:2022 - Sicurezza delle informazioni, cybersecurity e protezione della privacy — Sistemi di gestione della sicurezza delle informazioni — Requisiti
- ISO/IEC 27017:2015 - Tecnologie informatiche — Tecniche di sicurezza — Codice di buone pratiche per i controlli di sicurezza delle informazioni basati su ISO/IEC 27002 per i servizi cloud
- ISO/IEC 27018:2019 - Tecnologie informatiche — Tecniche di sicurezza — Codice di buone pratiche per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici che agiscono come responsabili del trattamento delle PII
- Direttiva (UE) 2022/2555 (Direttiva NIS2)

3. Termini e Definizioni

- **Riservatezza:** La proprietà che le informazioni non siano rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità:** La proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità:** La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.

4. Ruoli e Responsabilità

- **Top Management:** Definisce e approva le politiche di sicurezza, assicura la disponibilità delle risorse necessarie per il SGSI, promuove la cultura della sicurezza e supervisiona l'efficacia del sistema attraverso riesami periodici.
- **Presidente C.d.A.:** Guida l'impegno del Top Management nel sostenere e promuovere attivamente il Sistema di Gestione della Sicurezza delle Informazioni.
- **Resp. Sistema Gestione:** Ha la responsabilità generale dell'implementazione, del mantenimento e del monitoraggio del SGSI, supervisiona il processo di gestione del rischio e riferisce le prestazioni al Top Management.
- **C.F.O.:** Agisce come punto di contatto designato per le questioni relative alla sicurezza informatica.
- **Resp. Risorse Umane:** Assicura che vengano effettuate adeguate valutazioni del personale prima di concedere l'accesso a informazioni e sistemi sensibili, come previsto dalle procedure interne.

5. Obiettivi di sicurezza delle informazioni

NettunoPA si impegna a proteggere i propri asset informativi e quelli dei suoi clienti per garantire la continuità del business e minimizzare i rischi. Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) è stabilito in conformità ai requisiti della norma ISO/IEC 27001:2022 e alle direttive applicabili, inclusa la Direttiva NIS2.

Gli obiettivi strategici del SGSI sono:

- **Riservatezza:** Assicurare che le informazioni siano accessibili solo al personale autorizzato. NettunoPA si impegna a proteggere i dati personali e le informazioni proprietarie da accessi, divulgazioni o modifiche non autorizzate, in conformità con la "POL Politica di protezione delle PII" e la "POL Politica di classificazione ed etichettatura delle informazioni".
- **Integrità:** Salvaguardare l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione. Ogni modifica a dati o software deve avvenire in modo controllato e autorizzato, come definito nella "PRO Procedura di sviluppo sicuro" e nella "PRO Procedura di gestione del cambiamento".
- **Disponibilità:** Garantire che il personale autorizzato abbia accesso alle informazioni e agli asset associati quando necessario, in linea con gli obiettivi definiti nella "PRO Procedura di continuità operativa e di ripristino di emergenza".

Il Top Management si impegna a perseguire il miglioramento continuo dell'efficacia del SGSI, riesaminando periodicamente gli obiettivi e i risultati raggiunti. Gli obiettivi specifici e misurabili sono definiti e monitorati tramite la procedura "PRO Obiettivi e pianificazione per il loro raggiungimento".

6. Principi fondamentali di sicurezza delle informazioni

6.1. Impegno del Top Management e Organizzazione

Il Top Management di NettunoPA, guidato dal Presidente C.d.A., dimostra un impegno attivo nel sostenere e promuovere il SGSI. Tale impegno si concretizza attraverso:

- L'approvazione della presente politica e delle politiche specifiche ad essa collegate.
- L'integrazione dei requisiti di sicurezza delle informazioni nei processi di business aziendali.

La fornitura delle risorse necessarie per l'implementazione, il mantenimento e il miglioramento del SGSI.

La promozione di una cultura della sicurezza a tutti i livelli dell'organizzazione.

La struttura organizzativa per la sicurezza, con ruoli e responsabilità, è formalizzata nella "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni". Il Resp. Sistema Gestione ha la responsabilità generale di implementare e mantenere il SGSI e di riferire le sue prestazioni al Top Management. Il ruolo di punto di contatto per la sicurezza informatica è assegnato al C.F.O.

6.2. Approccio Basato sul Rischio

NettunoPA adotta un approccio alla gestione della sicurezza delle informazioni basato sul rischio, in accordo con la "PRO Procedura di gestione dei rischi" e la "PRO Valutazione

rischi per la sicurezza delle informazioni". Questo approccio garantisce che le misure di sicurezza implementate siano proporzionate ai rischi identificati per gli asset informativi. Il Resp. Sistema Gestione ha la responsabilità di supervisionare il processo di valutazione del rischio, mentre il Top Management ha il compito di approvare il piano di trattamento dei rischi.

6.3. Sicurezza delle Risorse Umane

La sicurezza è una responsabilità condivisa e parte integrante del ciclo di vita di ogni dipendente, come definito nella "PRO Procedura di gestione delle risorse umane".

- Il Resp. Risorse Umane deve assicurare che, per il personale autorizzato ad accedere a sistemi e informazioni rilevanti, venga effettuata una valutazione di esperienza, capacità e affidabilità.
- Tutti i dipendenti e collaboratori devono sottoscrivere un accordo di riservatezza, come il "MOD Accordo interno di non divulgazione (NDA)", all'inizio del rapporto di lavoro.
- Gli obblighi di riservatezza, definiti contrattualmente, rimangono validi anche dopo la cessazione del rapporto di lavoro.

6.4. Uso Accettabile delle Risorse e Protezione degli Asset

L'uso delle informazioni e degli asset aziendali deve essere conforme a quanto stabilito nel "Codice di condotta" e nella "POL Politica di sicurezza operativa".

- **Scrivania e Schermo Puliti:** Il personale deve assicurare che le informazioni sensibili, sia in formato cartaceo che su supporti rimovibili, siano protette quando non utilizzate. Le postazioni di lavoro devono essere bloccate se incustodite e deve essere richiesta una password per riattivare la sessione dopo un periodo di inattività.
- **Dispositivi Mobili e Telelavoro:** L'uso di dispositivi mobili e il lavoro da remoto sono permessi a condizione che vengano adottate le misure di sicurezza definite nella "POL Politica di sicurezza operativa" per proteggere le informazioni aziendali. Gli asset utilizzati fuori sede devono essere protetti da furto, perdita o accesso non autorizzato.

6.5. Gestione degli Incidenti e Continuità Operativa

- Tutto il personale ha la responsabilità di segnalare tempestivamente qualsiasi evento o debolezza di sicurezza osservata o sospetta, seguendo i canali definiti nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".
- NettunoPA si impegna a garantire la continuità delle proprie attività critiche e a ripristinare i servizi a seguito di un'interruzione, secondo le strategie definite nella "PRO Procedura di continuità operativa e di ripristino di emergenza".

6.6. Framework delle Politiche Specifiche

La presente politica è supportata da un insieme di politiche e procedure specifiche che coprono tutti gli ambiti rilevanti per la sicurezza delle informazioni, in conformità con la Direttiva NIS2 e gli standard ISO. Il Top Management approva tutte le politiche del SGSI. Queste includono, ma non si limitano a:

- Gestione del rischio ("PRO Procedura di gestione dei rischi")

- Ruoli e responsabilità ("POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni")
- Sicurezza delle risorse umane ("PRO Procedura di gestione delle risorse umane")
- Conformità e audit ("PRO Gestione audit interni")
- Sicurezza della catena di approvvigionamento ("PRO Procedura di gestione degli acquisti e delle terze parti")
- Gestione degli asset ("PRO Procedura di configurazione, gestione e smaltimento degli asset")
- Gestione delle vulnerabilità e sicurezza operativa ("POL Politica di sicurezza operativa")
- Continuità operativa e gestione delle crisi ("PRO Procedura di continuità operativa e di ripristino di emergenza")
- Controllo degli accessi ("PRO Procedura di gestione e controllo degli accessi logici")
- Sicurezza fisica e ambientale ("PRO Procedura di sicurezza fisica e ambientale")
- Formazione e consapevolezza del personale
- Sicurezza dei dati, crittografia e protezione delle PII ("POL Politica di classificazione ed etichettatura delle informazioni", "PRO Procedura di crittografia e gestione delle chiavi crittografiche", "POL Politica di protezione delle PII", "POL Politica di conservazione e cancellazione delle informazioni")
- Sviluppo e manutenzione dei sistemi ("PRO Procedura di sviluppo sicuro")
- Protezione delle reti ("PRO Procedura di gestione della sicurezza della rete")
- Monitoraggio e risposta agli incidenti ("PRO Procedura di gestione degli incidenti di sicurezza delle informazioni")

6.7. Principi per i Servizi Cloud

In qualità sia di cliente che di fornitore di servizi cloud, NettunoPA adotta principi specifici per la sicurezza nel cloud, in linea con gli standard ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

- **Come cliente di servizi cloud:** NettunoPA valuta i rischi associati ai fornitori di servizi cloud, tenendo conto della localizzazione dei dati, dell'accesso da parte del fornitore e dei modelli di responsabilità condivisa.
- **Come fornitore di servizi cloud:** NettunoPA implementa controlli per garantire l'isolamento dei dati dei clienti, la sicurezza della virtualizzazione, la gestione sicura degli accessi amministrativi e la comunicazione trasparente delle violazioni. I requisiti dettagliati sono definiti nella "POL Politica di sicurezza del cloud" e nella "POL Politica di protezione delle PII".

6.8. Revisione e Miglioramento Continuo

Questa politica e l'intero SGSI sono soggetti a revisione da parte del Top Management a intervalli pianificati, e comunque almeno una volta all'anno o a seguito di cambiamenti significativi, per assicurarne la continua idoneità, adeguatezza ed efficacia. Il processo è formalizzato nella "PRO Gestione riesame della direzione". Le modifiche al SGSI sono

gestite in modo controllato attraverso la "PRO Procedura di gestione del cambiamento". Il Top Management riceve relazioni periodiche sull'efficacia delle misure di gestione del rischio e approva i piani di adeguamento necessari.

6.9. Comunicazione

La presente politica è comunicata a tutto il personale e resa disponibile alle parti interessate rilevanti. Il Resp. Sistema Gestione assicura che la comunicazione avvenga tramite i canali aziendali ufficiali, come e-mail e repository documentali interni. Tutto il personale è tenuto a prendere visione della politica e a confermarne la comprensione.

7. Archiviazione e Aggiornamenti

Questo documento è archiviato nel sistema di gestione documentale aziendale. Viene riesaminato con cadenza almeno annuale, o a seguito di cambiamenti significativi nel contesto organizzativo o normativo, dal Top Management per garantirne la continua idoneità ed efficacia. Ogni aggiornamento è gestito attraverso la procedura di gestione del cambiamento.

8. Documenti di Riferimento

- POL Politica di protezione delle PII
- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di sviluppo sicuro
- PRO Procedura di gestione del cambiamento
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Obiettivi e pianificazione per il loro raggiungimento
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione dei rischi
- PRO Valutazione rischi per la sicurezza delle informazioni
- PRO Procedura di gestione delle risorse umane
- MOD Accordo interno di non divulgazione (NDA)
- Codice di condotta
- POL Politica di sicurezza operativa
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Gestione audit interni
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di sicurezza fisica e ambientale

NettunoPA

Pubblico

- PRO Procedura di crittografia e gestione delle chiavi crittografiche
- POL Politica di conservazione e cancellazione delle informazioni
- PRO Procedura di gestione della sicurezza della rete
- POL Politica di sicurezza del cloud
- PRO Gestione riesame della direzione