PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE
WEB TECHNOLOGY FOR A REAL INNOVATION

POLITICA AZIENDALE PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA DELLE INFORMAZIONI

Revisione 03 del 01/08/2024

	EMESSO	APPROVATO
Funzione	**Responsabile Gestione Sicurezza delle Informazioni**	**Amministratore Delegato**
Data	01/08/2024	01/08/2024
Firma		

INDICE

1. GENERALITÀ

1.1 Scopo e Obiettivi

Scopo della presente Politica Aziendale è descrivere la Gestione degli Incidenti di Sicurezza delle Informazioni della società PA DIGITALE S.p.A. Obiettivi della presente Politica Aziendale sono:

- Garantire il rispetto dei requisiti della norma ISO/IEC 27035-2:2023
- Garantire il rispetto dei requisiti cogenti
- Ridurre i danni fisici e/o monetari
- Ridurre eventuali danni alle persone
- Ridurre altri impatti aziendali (impatto legale e normativo, impatto sull'erogazione dei servizi, danni alla reputazione dell'azienda, ecc.)

1.2 Campo di Applicazione e Ambito

La Politica Aziendale per la Gestione degli Incidenti di Sicurezza delle Informazioni rientra nell'ambito del Sistema di Gestione Integrato, che ha ad oggetto:

Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale e per il Mercato Privato, erogati in modalità SaaS oppure erogati con installazione in locale (on premise). Erogazione dei servizi professionali connessi ai prodotti software. Erogazione dei servizi SaaS in cloud per la Conservazione Digitale di documenti informatici a Norma e relativo servizio di assistenza.

La Politica si applica al personale di PA Digitale che opera nella preparazione e pianificazione, nel rilevamento, nella segnalazione, nella valutazione e decisione, nella risposta e nelle lezioni appresene da incidenti di Sicurezza delle Informazioni. La presente Politica ha revisione annuale o in occasione di particolari cambiamenti che influiscono sulla Politica stessa.

2. RIFERIMENTI

La presente politica segue la norma ISO 27035-2:2023, estensione applicata al Sistema di Gestione della Sicurezza delle Informazioni in conformità alla Norma ISO/IEC 27001:2022.

3. GESTIONE DEGLI INCIDENTI

3.1 Importanza della gestione degli incidenti di sicurezza delle informazioni per l'organizzazione

Importanza della gestione degli incidenti di sicurezza delle informazioni per l'organizzazione è connessa con la creazione di un ambiente consapevole dell'importanza della sicurezza e

dei rischi relativi, attraverso l'impegno diretto dei responsabili aziendali a garantire il raggiungimento degli obiettivi definiti nel paragrafo 1.1.

3.2 Impegno del top management

L'impegno diretto dei responsabili aziendali è reso evidente dalla partecipazione ai Comitati aziendali di Gestione (IMT) e Risposta (IRT) degli Incidenti di Sicurezza delle Informazioni.

3.3 Documentazione di piano

L'azienda ha redatto un apposito piano di gestione degli incidenti, a cui si collegano altre informazioni documentate quali procedure e istruzioni di lavoro interne afferenti al Sistema di Gestione per la Sicurezza delle Informazioni. Inoltre, ha redatto uno specifico piano di risposta agli incidenti medesimi.

4. DEFINIZIONI

Evento relativo alla sicurezza delle informazioni: accadimento che indica una possibile violazione relativa alla sicurezza delle informazioni o il malfunzionamento di uno o più controlli.
Incidente relativo alla sicurezza delle informazioni: uno o più eventi relativi alla sicurezza delle informazioni correlati e identificati che possono danneggiare gli asset di un'organizzazione o comprometterne l'operatività.
Violazione relativa alla sicurezza delle informazioni: compromissione della sicurezza delle informazioni che porta alla distruzione, alla perdita, alla modifica, alla divulgazione o all'accesso indesiderato a informazioni protette trasmesse, memorizzate o altrimenti elaborate.

5. TIPI DI INCIDENTE DI SICUREZZA

Nella tabella seguente è indicata una descrizione del tipo di incidenti suddivisi per categorie di sicurezza.

Categoria	Descrizione
Calamità naturale	Disastri naturali al di fuori del controllo umano
Disordini sociali	Instabilità della società civile
Danno fisico	Azioni fisiche deliberate o accidentali
Guasto dell'infrastruttura	Guasti dei sistemi e dei servizi di base che supportano il funzionamento dei sistemi informativi
Disturbo da radiazioni	Disturbo dovuto alle radiazioni
Guasto tecnico	Guasti nei sistemi di informazione o nelle relative strutture non tecniche, nonché da problemi non intenzionali causati dall'uomo, con conseguente indisponibilità o distruzione dei sistemi informativi
Malware	Programmi dannosi creati e diffusi deliberatamente. Un programma dannoso viene inserito nei sistemi di informazione per danneggiare la riservatezza, l'integrità o la disponibilità di dati, applicazioni o sistemi operativi e/o compromettere il normale funzionamento dei sistemi informativi

Attacco tecnico	Informazioni di attacco ai sistemi attraverso reti o altri mezzi tecnici, sfruttando le vulnerabilità dei sistemi di informazione in configurazioni, protocolli o programmi, o con la forza, che si traduce in uno stato anomalo dei sistemi di informazione o in un potenziale danno alle attuali operazioni del sistema
Violazione delle regole	Violazione delle regole deliberatamente o accidentalmente
Compromissione delle funzioni	Compromissione deliberata o accidentale delle funzioni dei sistemi informativi in termini di sicurezza
Compromissione delle informazioni	Compromissione deliberata o accidentale della sicurezza delle informazioni come riservatezza, integrità, disponibilità, ecc.
Contenuti dannosi	Diffusione di contenuti indesiderati attraverso le reti di informazione, che mette in pericolo la sicurezza nazionale, la stabilità sociale e/o la sicurezza pubblica e i benefici

6. MODALITÀ DI SEGNALAZIONE DEGLI INCIDENTI

Le modalità di segnalazione degli incidenti (classificati secondo una puntuale scala di gravità), compresi elementi da segnalare, meccanismi utilizzati per la segnalazione, luoghi e invii di una segnalazione sono definite da apposite procedure aziendali interne.

7. FLUSSO DI GESTIONE DEGLI INCIDENTI

Come descritto in maniera dettagliata nelle apposite procedure aziendali interne, il flusso del processo di gestione degli incidenti comprende:

- la pianificazione e la preparazione
- il rilevamento
- la segnalazione
- la valutazione e la decisione
- la risposta
- le lezioni apprese

8. RISOLUZIONE DEGLI INCIDENTI

La risoluzione degli incidenti non si limita solo al ripristino delle corrette funzionalità, ma è rivolta alla rimozione delle cause, approfondendo il contenuto delle lezioni apprese nell'ottica del miglioramento continuo del processo di gestione degli incidenti di sicurezza delle informazioni.

9. RUOLI E RESPONSABILITÀ

Nel processo di gestione degli incidenti di sicurezza delle informazioni e delle attività correlate, sono chiamati in causa il Team di gestione degli incidenti (Incident Management Team, IMT) e il Team di risposta agli incidenti (Incident Response Team, IRT).
Il Team di gestione degli incidenti (IMT) è il gruppo responsabile della capacità di gestione degli incidenti per l'organizzazione, coordinato dall'Incident Manager.
Il Team di risposta agli incidenti (IRT) è un gruppo di membri dell'organizzazione adeguatamente qualificati che gestisce i singoli incidenti durante il loro ciclo di vita.

Come detto anche nella Politica Aziendale per la Sicurezza delle Informazioni, per rispondere ai crescenti requisiti normativi, in particolar modo legati alla necessità di definire e rendere noti i ruoli e le responsabilità inerenti alla cybersecurity per tutto il personale e per le terze parti rilevanti (es. fornitori, clienti, partner), PA Digitale ha nominato:

- un incaricato (e il suo sostituto), con il compito di gestire l'attuazione delle disposizioni normative in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico dell'azienda e assicura l'efficace implementazione delle misure di sicurezza
- un referente tecnico (e il suo sostituto), in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia ai fini della gestione degli incidenti aventi impatto sull'infrastruttura.

Tale struttura è di seguito declinata:

Incaricato	***Direttore Cybersecurity e IT Buffetti S.p.A.***
Sostituto	Responsabile per la Gestione della Sicurezza delle Informazioni PA Digitale S.p.A.
Referente Tecnico	Responsabile Sicurezza Informatica PA Digitale S.p.A.
Sostituto	Responsabile dello Sviluppo del Sistema di Conservazione PA Digitale S.p.A.

10. TEAM DI GESTIONE DEGLI INCIDENTI - IMT

Come anticipato al paragrafo precedente, il Team di gestione degli incidenti (IMT) è il gruppo responsabile della capacità di gestione degli incidenti per l'organizzazione. Coincide con il Comitato di Sicurezza Informatica aziendale definito nella Politica della Sicurezza delle Informazioni. L'IMT fa a capo all'Incident Manager, che coincide con il Presidente del Comitato di Sicurezza Informatica aziendale, ovvero l'Amministratore Delegato. Una panoramica dell'IMT (che comprende struttura organizzativa dell'IMT, ruoli chiave, responsabilità, autorità e un riepilogo dei compiti inclusi) è specificata nel piano di gestione degli incidenti aziendale.
Nel caso di incidenti di natura catastrofica, ai componenti interni dell'IMT si aggiungono i membri del CyberSecTeam - Struttura di Cybersecurity di Gruppo.

11. TEAM DI RISPOSTA DEGLI INCIDENTI - IRT

Secondo la categoria di incidente, nel processo di gestione degli incidenti di sicurezza delle informazioni sono coinvolti uno o più IRT, che sono costituiti all'occorrenza e sono sciolti alla chiusura di ciascun incidente. Gli IRT rispondono a incidenti specifici che hanno ambiti e competenze diversi a seconda dell'incidente. L'IRT fa a capo a un coordinatore degli incidenti, di volta in volta designato secondo la categoria di incidente. Una panoramica degli IRT è specificata nel piano di gestione degli incidenti aziendale.
Nel caso di incidenti di natura catastrofica, ai componenti interni dell'IRT si aggiungono i membri del CyberSecTeam - Struttura di Cybersecurity di Gruppo, all'interno del quale può essere nominato (all'occorrenza) il coordinatore degli incidenti di natura catastrofica.

12. COLLABORAZIONE

Il personale dell'azienda contribuisce a rilevare, analizzare e rispondere agli incidenti di sicurezza delle informazioni.

13. SORVEGLIANZA

La sorveglianza sul processo di gestione degli incidenti di sicurezza delle informazioni è garantita dai monitoraggi definiti dalle apposite procedure aziendali interne, oltre ai monitoraggi periodici dell'IMT.

14. COLLEGAMENTI ESTERNI

Secondo la categoria di incidente, l'azienda può usufruire della collaborazione di fornitori qualificati che possono cooperare con gli IRT per la risoluzione degli incidenti di sicurezza delle informazioni. In caso di necessità, dunque, l'azienda può rivolgersi eventualmente ad altre organizzazioni in grado di fornire supporto esterno specifico, quali ad esempio come team forensi, consulenti legali, ecc.

15. REQUISITI COGENTI

Una sintesi dei requisiti o dei mandati di conformità legale e normativa associati alle attività di gestione degli incidenti di sicurezza delle informazioni è espressa nella normativa di settore emessa dalle autorità competenti (es. AgID, ACN, ecc.).