# POLITICA PER LA GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI

## SCOPO

L'obiettivo di questa politica è quello di garantire che l'impresa reagisca in modo appropriato a qualsiasi tipologia, effettiva o presunta, di incidenti di sicurezza relativamente ai sistemi informativi e ai dati.
L'organizzazione ha la responsabilità di monitorare tutti gli incidenti che si verificano al suo interno che possono violare la sicurezza e/o la riservatezza delle informazioni. Tutti gli incidenti devono essere identificati, segnalati, studiati e monitorati: lo scopo principale di questa politica non è quello di attribuire colpe, ma di contenere i problemi e apprendere dagli errori in ottica di miglioramento continuo.

## CAMPO DI APPLICAZIONE

Questa politica si applica a tutti i dipendenti, collaboratori, consulenti, lavoratori temporanei all'interno dell'organizzazione.

## MODALITÀ OPERATIVE

Partiamo dalla definizione: con "incidenti di sicurezza delle informazioni" s'intende un evento avverso che ha causato o ha il potenziale di causare danni agli assets, alla reputazione e/o al personale dell'organizzazione, attraverso l'intrusione, la compromissione e l'abuso di informazioni e risorse. Quindi è la realizzazione di una delle minacce analizzate nel Risk Assessment dell'organizzazione.

**Tipi di Incidenti**
Le principali categorie di incidente sono:

- Incidenti **CRITICI** devono essere segnalati immediatamente
  *Es.*
  - furto di documenti
  - computer infettato da virus
- Incidenti **SIGNIFICATIVI** devono essere segnalati entro 4 ore
  *Es.*
  - uso di un software privo di licenza
  - accesso e/o uso non autorizzato dei dati di accesso di un altro utente
- Incidenti **MINORI** devono essere segnalati entro 1 giorno
  *Es.*
  - Tentata penetrazione delle difese
  - Spedizioni email non appropriate

**Rischi**
L'organizzazione riconosce che ci sono dei rischi associati all'accesso degli utenti e alla gestione delle informazioni nello svolgimento delle proprie attività, infatti questa politica mira a:

- ✓ Ridurre l'impatto delle violazioni di sicurezza, assicurando che gli incidenti siano seguiti correttamente.
- ✓ Aiutare a identificare le aree di miglioramento per ridurre il rischio e l'impatto di futuri incidenti.
- ✓ Ridurre il numero degli incidenti

Non conformità con questa politica potrebbe avere un impatto significativo sull'efficienza del funzionamento dell'organizzazione e può causare perdite finanziarie, multe e l'impossibilità di fornire i servizi necessari agli interessati del trattamento.

**Procedura da seguire**

*Fase 1* **RILEVAZIONE INCIDENTE**

Un incidente può e deve essere rilevato:

- ✓ Dal personale operativo nello svolgimento delle proprie attività.
- ✓ Dall'avviso automatico dei dispositivi che monitorano le proprie attività di sistema.
- ✓ Dall' utente finale.

*Fase 2* **VALUTAZIONE INCIDENTE**

Lo scopo di questa fase è quello di determinare rapidamente e con precisione se l'incidente è un incidente grave.

- ✓ Raccolta dati del problema iniziale - I dati sono raccolti e viene fatta un'appropriata classificazione dell'Impatto.
- ✓ Valutazione dell'Incidente - l'incidente è valutato e la relativa categoria è confermata dal Responsabile della Sicurezza delle informazioni.
- ✓ Incidente Grave - Se l'incidente è classificato come 'Critico', la valutazione deve essere confermata entro 60 minuti dalla rilevazione.

*Fase 3* **COMUNICAZIONE INCIDENTE**

I processi di comunicazione hanno lo scopo di garantire che tutte le parti siano informate dello stato dell'incidente.

- ✓ I Responsabili di progetto e/o le parti coinvolte devono essere informati dell'incidente e tenuti aggiornati sui relativi progressi per consentire loro di gestire i dati degli interessati.
- ✓ In casi di incidente grave la Direzione deve essere informata e tenuta aggiornata.
- ✓ Qualora la violazione possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare di trattamento notifica al Garante entro 72h dal momento in cui ne è venuto a conoscenza. (Vedi *Modulo Segnalazione Data Breach*).

*Fase 4* **RISOLUZIONE INCIDENTE**

Questa fase comprende tutte le varie indagini tecniche che saranno necessarie per portare l'incidente a risoluzione; può richiedere l'intervento di diverse figure tecniche e non – si prevede che le risorse siano rese disponibili su richiesta.

*Fase 5* **POST-RISOLUZIONE INCIDENTE**

Il processo di post-risoluzione è avviato una volta che l'incidente è stato risolto.

⇒ *Riesame Incidente Critico*: Il Responsabile della Sicurezza delle Informazioni, in occasione di incidente grave, indice una riunione di riesame entro 3 giorni lavorativi dalla data di risoluzione dell'incidente, alla quale partecipa il personale coinvolto.

⇒ *Verbale Incidente Critico*: E' costituito dal verbale della riunione di riesame: riassume gli eventi dell'incidente, l'impatto, le azioni intraprese per risolvere l'incidente e le ulteriori misure adottate per ridurre il rischio di accadimento futuro/impatto.

⇒ *Incidente Non Critico*: E' segnalato tramite la compilazione di un verbale firmato dal Responsabile della Sicurezza; non è necessaria riunione apposita.