Akeron & Akeron Lab

Politica per la Gestione degli Incidenti di Sicurezza delle Informazioni

Release date: 30 Aprile 2024
Protection level: Public

Identification: AK 20

Data	Descrizione delle modifiche	Rev. n°
30/04/2024	Prima emissione per ISO 27001:2022	00
		01
		02
		03

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

Il Sistema di Gestione degli Incidenti di Sicurezza delle Informazioni include tutti prodotti ed i servizi offerti da Akeron e ha come scopo:

- 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.)

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

PROGETTAZIONE, SVILUPPO, VENDITA, CONFIGURAZIONE E SUPPORTO DI SOLUZIONI SOFTWARE GESTIONALI E DI PERFORMANCE MANAGEMENT IN MANAGED MODE O IN AMBIENTI SAAS (SOFTWARE AS A SERVICE) IN CONFORMITÀ CON LE LINEE GUIDA ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27035

La Politica si applica al personale di Akeron 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.
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.

L'importanza della gestione degli incidenti di sicurezza delle informazioni per l'organizzazione è connessa alla 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 sopra.

L'impegno diretto dei responsabili aziendali è reso evidente dal coinvolgimento nelle fasi critiche del processo e con l'assegnazione di risorse idonee al raggiungimento degli obiettivi dichiarati.

L'azienda ha redatto un piano di gestione degli incidenti, a cui si aggiungono altre informazioni documentate quali procedure e istruzioni di lavoro interne afferenti al Sistema di Gestione per la Sicurezza delle Informazioni.
Il processo di gestione degli incidenti di sicurezza adottato da Akeron prevede i seguenti sotto-processi, descritti nei paragrafi successivi:

- **Rilevazione degli eventi di sicurezza**: attività finalizzata al monitoraggio, all'analisi, al tracciamento ed alla classificazione degli eventi di sicurezza;
- **Gestione degli eventi di sicurezza**: attività finalizzata a contrastare le violazioni di sicurezza riferite ad un determinato allarme o un determinato incidente di sicurezza, ivi comprese le attività di accertamento danni e ripristino alle condizioni standard antecedenti all'incidente stesso. In

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

funzione della classificazione dell'evento (allarme, incidente o falso positivo) si procede alla relativa modalità di gestione;

- **Analisi post-incidente**: attività finalizzata all'analisi delle condizioni che hanno determinato l'incidente in modo da formulare un piano di miglioramento che tenda a contenere i rischi di nuovi incidenti di simile natura;
- **Lesson learnt e miglioramento continuativo**: attività finalizzata al miglioramento continuativo dell'intero processo di Gestione Incidenti

Definizioni	Descrizione
Agente malevolo	Soggetto che, sfruttando le vulnerabilità insite in un sistema ICT ovvero sfruttando le proprie conoscenze derivanti dal ruolo organizzativo rivestito, causa, volontariamente o accidentalmente, una violazione delle politiche di sicurezza applicate ad un determinato asset ICT.
Analisi post-incidente	Insieme di attività finalizzate alla raccolta ed alla analisi delle evidenze utili a stabilire le cause, il contesto e le modalità di attuazione di una violazione della sicurezza configurabile come incidente di sicurezza.
Criticità	Insieme di circostanze avverse, derivanti dalla concomitanza di eventi che costituiscono una minaccia per la sicurezza di un determinato contesto.
Disponibilità	Proprietà dell'informazione di essere accessibile e utilizzabile dal personale autorizzato, nei tempi, nei luoghi e nelle modalità adeguate alle necessità operative dell'azienda.
Evento di sicurezza	Qualsiasi occorrenza o evento significativo che si verifica nell'ambito di un determinato asset informatico o del patrimonio informativo dell'azienda, rilevata mediante strumenti automatizzati o non automatizzati, che, per il suo impatto potenziale sul patrimonio informativo dell'azienda, richiede un'azione immediata o una risposta per garantire la protezione, l'integrità e la disponibilità delle informazioni critiche per l'organizzazione.
Incidente di sicurezza	Qualsiasi evento o insieme di eventi che sottintendono una violazione delle politiche di sicurezza fonte di danno per il patrimonio informativo dell'azienda.
Integrità	Proprietà dell'informazione di essere presente, corretta e valida.
Monitoraggio degli eventi di sicurezza	Insieme di attività continuative, organizzate, controllate e documentate, finalizzate al rilevamento degli eventi di sicurezza, anche con l'ausilio di strumenti automatici.
Minacce	Insieme di eventi malevoli che possono agevolare una violazione delle politiche di sicurezza ed un danno al patrimonio informativo dell'azienda.

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

Patrimonio informativo	Insieme di beni strumentali, materiali ed immateriali, che assumono un valore significativo per il compimento della missione dell'azienda. Il patrimonio informativo è costituito dalle seguenti tipologie di risorse: • Risorse tecnologiche: sistemi, apparati, infrastrutture hardware e software utilizzati come strumenti di supporto allo svolgimento dei processi dell'azienda; • Informazioni: insieme composto da un'aggregazione di dati elementari, o da altre informazioni logicamente correlate tra di loro, funzionali allo svolgimento dei processi dell'azienda; • Risorse umane: soggetti interni od esterni all'organizzazione che, attraverso il proprio patrimonio cognitivo e professionale, contribuiscono allo svolgimento dei processi dell'azienda in un ambito di competenze e responsabilità predefinito; • Innovazioni, frutto dell'ingegno, copyright e brevetti: qualsiasi elemento ascrivibile all'ambito di proprietà dell'organizzazione che costituisce fonte di vantaggio per lo svolgimento della missione di impresa e dei processi ad essa correlati.
Riservatezza	Caratteristica dell'informazione di essere conoscibile solo ad alcuni soggetti autorizzati.
Violazione di sicurezza	Azione o insieme di azioni intenzionali o accidentali, intraprese da un agente malevolo che comportano una elusione o inibizione delle politiche di sicurezza applicate ad un determinato asset ICT.
Vulnerabilità	Elemento caratteristico di un determinato asset ICT, che potrebbe essere sfruttato da agenti malevoli per apportare una violazione alle politiche di sicurezza e/o per danneggiare il patrimonio informativo dell'azienda.

Per i dettagli dei vari tipi di incidenti di sicurezza e le modalità di segnalazione si fa riferimento alla procedura dedicata GDIM 11 Procedura di incident management.
Come descritto nel dettaglio nell'apposita procedura GDIM11, 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

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.

Nel processo di gestione degli incidenti di sicurezza delle informazioni e delle attività correlate, sono chiamati in causa il Team di gestione degli incidenti (di seguito IRT) ed eventuali consulenti esterni con

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

competenze ed esperienze specifiche nel monitoraggio e nell'analisi degli eventi di sicurezza, che erogano il servizio per conto dell'azienda.

Come dichiarato 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), Akeron ha individuato un collaboratore (consulente esterno), 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.

Il Team di gestione degli incidenti (IRT) è il gruppo responsabile della capacità di gestione degli incidenti per l'organizzazione, coordinato dal Responsabile del Team di Gestione Incidenti (di seguito Responsabile IRT).

- L'**IRT** con la responsabilità di:
  - Monitorare gli eventi di sicurezza (in orario di lavoro standard) garantendo le attività di analisi e di classificazione degli eventi;
  - Raccogliere e valutare tutte le comunicazioni, verbali o scritte;
  - Tracciare in una scheda evento le informazioni raccolte nel corso delle attività di monitoraggio degli eventi;
  - Supportare il Responsabile IRT nella definizione del piano di trattamento degli eventi non precodificati;
  - Applicare le azioni di trattamento per gli eventi precodificati, secondo quanto riportato nelle relative istruzioni operative approvate dal Responsabile IRT e attivando, ove necessario, le Funzioni Coinvolte responsabili della gestione dei sistemi;
  - Garantire un adeguato grado di efficacia/efficienza dei sistemi preposti al rilevamento, al tracciamento ed alla segnalazione degli eventi di sicurezza;
  - Valutare e applicare le azioni di tuning alle piattaforme di propria competenza per il trattamento dei falsi positivi;
  - Definire sotto il coordinamento del Responsabile IRT le azioni di contrasto/contenimento per il trattamento degli eventi classificati come evento o incidente;
  - Raccogliere sotto il coordinamento del Responsabile IRT le evidenze e/o i logfile ed applicare le modifiche alle piattaforme di propria competenza, coinvolgendo se necessario le Funzioni Coinvolte;
  - Trattare gli eventi classificati come incidenti avendo cura di inviare al Responsabile IRT il report incidente contenente tutte le informazioni utili alla gestione degli stessi;
  - Supportare il Responsabile IRT per le attività di analisi post-incidente, nella raccolta delle evidenze utili alla definizione delle cause, delle modalità di attuazione e dei danni subiti dalle infrastrutture ICT;
  - Coinvolgere e/o coordinare le Funzioni Coinvolte nell'attuazione delle misure di contrasto/ contenimento per il trattamento degli allarmi e degli incidenti di sicurezza;
  - A seguito di incidenti di sicurezza, eseguire, sotto il coordinamento e la supervisione del Responsabile IRT, le seguenti attività:

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

- Valutazione dei possibili danni subiti al patrimonio informativo e/o asset ICT interessato dall'incidente;
- Rilevamento dei danni, coinvolgendo se necessario le Funzioni Coinvolte nella gestione dei sistemi ICT interessati dall'incidente;
- Redazione del rapporto incidente;
- Redazione del piano di trattamento e ripristino degli incidenti.

- Chiudere formalmente le schede evento, aggiornando la Knowledge Base di supporto alla gestione incidenti;
- Rendicontare al Responsabile IRT, con cadenza periodica, la gestione degli eventi di sicurezza, avendo cura di fornire i dati relativi ad eventi, allarmi, incidenti e falsi positivi nel periodo di riferimento.

- Il **Responsabile IRT** ha la responsabilità di:
  - Definire le istruzioni operative per il contrasto/contenimento/trattamento degli eventi precodificati, coinvolgendo ove necessario, le Funzioni Coinvolte responsabili della gestione dei sistemi;
  - Approvare la strategia di contrasto e contenimento degli allarmi e incidenti, coordinando l'IRT nelle successive attività di trattamento;
  - Supervisionare e coordinare le attività svolte dall'IRT in caso di incidenti di sicurezza nella definizione del piano di trattamento e ripristino, nell'accertamento dei danni subiti, nella raccolta delle evidenze e nella redazione del rapporto di constatazione incidente;
  - Approvare formalmente il piano di ripristino redatto dall'IRT in caso di incidenti di sicurezza;
  - Valutare il grado di invasività delle azioni di contrasto/contenimento per gli incidenti presi in gestione;
  - Coordinare le Funzioni Coinvolte nella gestione dei sistemi ICT interessati da un incidente di sicurezza nell'attuazione delle attività di ripristino alle condizioni standard (antecedenti ad un incidente di sicurezza), relativamente ai sistemi di propria competenza;
  - Comunicare a tutte le parti coinvolte (interne ed esterne all'IRT) l'esito degli interventi di ripristino;
  - Ricevere le schede incidente inviate dall'IRT;
  - Effettuare l'analisi post-incidente al fine di consentire una corretta attuazione del processo di miglioramento di gestione dei rischi di sicurezza, richiedendo se necessario l'intervento dell'IRT e di specialisti esterni;
  - Ricevere dall'IRT la reportistica sullo stato della sicurezza e sull'avanzamento delle attività di gestione incidenti;
  - Definire e revisionare periodicamente il processo di trattamento degli allarmi e gestione degli incidenti di sicurezza, in maniera tale da garantire un adeguato grado di efficacia ed efficienza del processo stesso, in funzione degli obiettivi di trattamento dei rischi prefissati;
  - Effettuare la revisione periodica della presente Procedura;
  - Produrre ed inviare al Responsabile Sistema Informativo la reportistica relativa al processo di trattamento degli allarmi e di gestione degli incidenti di sicurezza.
  - Approvare il piano di ripristino in caso di incidenti di sicurezza;
  - Gestire la reportistica sullo stato della sicurezza e sull'avanzamento delle attività di gestione incidenti.

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

- Le **Funzioni Coinvolte** hanno la responsabilità di:
  - Garantire, per il proprio ambito di competenza, l'attuazione delle misure di contrasto/contenimento degli eventi e degli incidenti di sicurezza, sulla base delle istruzioni impartite dall'IRT;
  - Garantire, per il proprio ambito di competenza e responsabilità, il corretto svolgimento delle attività necessarie al ripristino delle condizioni standard di servizio, conseguenti ad un incidente di sicurezza, sulla base delle istruzioni impartite dall'IRT;
  - Supportare l'IRT nello svolgimento delle analisi degli allarmi e degli incidenti di sicurezza, attenendosi alle richieste effettuate dal personale preposto a tale compito;
  - Supportare il Responsabile IRT nello svolgimento delle analisi post-incidente, attenendosi alle richieste effettuate dal personale preposto a tale compito.

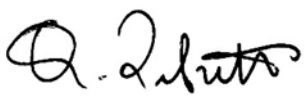
Il personale dell'azienda contribuisce a rilevare, analizzare e rispondere agli incidenti di sicurezza delle informazioni.

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'IRT.

Secondo la categoria di incidente, l'azienda può usufruire della collaborazione di fornitori qualificati che possono cooperare con l'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.

Lucca il 30.04.2024

Firma per riesame ed approvazione:



Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com