Logikamente | Decision Making Software | hello@logikamente.it | REA FE-211931 | P.IVA 01942790385

Headquarter
Via Giovanni Calvino, 38a
44122 Ferrara FE - Italy
T. 0532 206288 - 0532 214802

POL_N.5.2 POLITICA GENERALE PER LA SICUREZZA DELLE INFORMAZIONI

Headquarter
Via Giovanni Calvino, 38a
44122 Ferrara FE - Italy
T. 0532 206288 - 0532 214802

PREMESSA

LOGIKAMENTE offre servizi informatici ai propri clienti attuali e futuri, pertanto, l'obiettivo della sicurezza delle informazioni risulta primario. Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni che l'azienda ha fatto propri al fine di realizzare, mantenere e migliorare costantemente un efficiente Sistema di Gestione della Sicurezza delle Informazioni.

La sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e degli elementi del sistema informativo responsabile della loro gestione.
In particolare, perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere le seguenti proprietà delle stesse:

- **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati
- **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate
- **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta

La mancanza di adeguati livelli di sicurezza, in termini di Riservatezza, Disponibilità, Integrità, può comportare, nell'ambito di una qualsiasi attività aziendale, il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economico/finanziaria.

La sicurezza delle informazioni è, quindi, un requisito fondamentale per garantire l'affidabilità delle informazioni trattate, nonché l'efficacia ed efficienza dei servizi erogati da LOGIKAMENTE; di conseguenza, è essenziale per la società identificare le esigenze di sicurezza attraverso le seguenti attività:

- analisi e trattamento dei rischi, che consente all'azienda di acquisire la consapevolezza e la visibilità sul livello di esposizione al rischio del proprio sistema informativo.
- applicazione della normativa cogente, volontaria e delle clausole contrattuali in tema di sicurezza delle informazioni.

PERIMETRO ORGANIZZATIVO

La presente Politica, emessa dalla Direzione, si rivolge a tutto il personale dipendente ed ai collaboratori di LOGIKAMENTE, nonché a tutte le parti interessate esterne coinvolte nella gestione delle informazioni trattate dalla società.

IDENTIFICAZIONE, CLASSIFICAZIONE E GESTIONE DEGLI ASSET

Obiettivo: *garantire la piena conoscenza delle informazioni gestite in LOGIKAMENTE e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.*

- Esiste e viene periodicamente aggiornato un sistema di censimento di tutti i beni materiali ed immateriali da tutelare (informazioni, hardware, software, documentazioni cartacee e supporti di memorizzazione)
- Ogni risorsa (bene materiale/immateriale) è direttamente associabile ad un responsabile
- Le informazioni sono classificate in base al loro livello di criticità, in modo da essere gestite con

Headquarter
Via Giovanni Calvino, 38a
44122 Ferrara FE - Italy
T. 0532 206288 - 0532 214802

livelli di riservatezza ed integrità coerenti ed appropriati. La criticità delle informazioni deve essere valutata in maniera quanto più oggettiva possibile, attraverso l'utilizzo di adeguate metodologie di lavoro
- Le modalità di gestione ed i sistemi di protezione per le informazioni e gli asset su cui risiedono devono essere coerenti con il livello di criticità identificato

GESTIONE SICURA DEGLI ACCESSI

Obiettivo: *garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti che non hanno i necessari diritti.*

- L'accesso alle informazioni da parte di ogni singolo utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti. La comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio
- L'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinato al superamento di una procedura di identificazione ed autenticazione degli stessi
- Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione e gestite attraverso credenziali
- I sistemi che costituiscono l'infrastruttura ICT devono essere opportunamente protetti e segregati, in modo da minimizzare la possibilità degli accessi non autorizzati

NORME COMPORTAMENTALI PER LA GESTIONE SICURA DELLE RISORSE AZIENDALI

Obiettivo: *garantire che i dipendenti e collaboratori di LOGIKAMENTE adottino modelli di comportamento volti a garantire adeguati livelli di sicurezza delle informazioni.*

- Gli ambienti di lavoro e le risorse aziendali devono essere utilizzati in modo congruo con le finalità per le quali sono state rese disponibili e garantendo la sicurezza delle informazioni trattate
- Devono essere definite delle procedure per la gestione ed utilizzo delle informazioni sia su supporto digitale che su supporto cartaceo
- I sistemi informatici aziendali devono essere impiegati da dipendenti e dai collaboratori secondo procedure approvate

PERSONALE E SICUREZZA

Obiettivo: *garantire che il personale che opera per conto di LOGIKAMENTE (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni.*

- Nelle fasi di selezione ed inserimento del personale in LOGIKAMENTE devono essere valutati i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza aziendale in funzione delle attività che dovranno essere svolte
- Durante la permanenza in LOGIKAMENTE il personale deve ricevere un'adeguata e continuativa formazione inerente alle tematiche di sicurezza dei dati
- In apposita procedura sono previste le misure di sicurezza attinenti telelavoro e utilizzo di dispositivi portatili e quelle relative all'ottimizzazione dell'area di lavoro
- Le modalità di chiusura del rapporto di lavoro con LOGIKAMENTE dovranno essere coerenti

Headquarter
Via Giovanni Calvino, 38a
44122 Ferrara FE - Italy
T. 0532 206288 - 0532 214802

con gli obiettivi di sicurezza aziendale

La direzione garantisce che i dipendenti abbiano le conoscenze pertinenti in materia di sicurezza delle informazioni e dei sistemi che sviluppano o mantengono. Il personale coinvolto nel ciclo di vita dello sviluppo dei sistemi informativi è consapevole delle proprie responsabilità in materia di sicurezza dei sistemi e delle informazioni.

GESTIONE DEGLI EVENTI ANOMALI E DEGLI INCIDENTI

Obiettivo: *garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.*

- Tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare, a chi di competenza e secondo adeguate procedure, eventuali problematiche legate alla sicurezza delle informazioni
- Gli incidenti che possono avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e no, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure, coinvolgenti anche la relazione con determinati fornitori

GESTIONE DELLA SICUREZZA FISICA

Obiettivo: *prevenire l'accesso non autorizzato alle sedi ed ai singoli locali aziendali e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni.*

- Deve essere garantita la gestione della sicurezza delle aree e dei locali tramite la definizione dei livelli adeguati di protezione
- Deve essere garantita la sicurezza delle apparecchiature tramite:
    1. la definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni
    2. la messa a disposizione delle risorse necessarie al loro funzionamento
    3. la predisposizione di un adeguato livello di manutenzione

ASPETTI CONTRATTUALI CONNESSI ALLA SICUREZZA DELLE INFORMAZIONI

Obiettivo: *assicurare la conformità dei contratti con le terze parti ai requisiti legali ed ai principi legati alla sicurezza delle informazioni, in accordo con le caratteristiche specifiche della relazione che LOGIKAMENTE deve instaurare con le terze parti stesse.*

- Gli accordi con le terze parti (clienti e fornitori) che accedono alle informazioni e/o agli strumenti che le elaborano, devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza
- Gli accordi con terze parti, ove necessario, devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali

GESTIONE DELLA BUSINESS CONTINUITY

Obiettivo: *garantire la continuità dell'attività di LOGIKAMENTE e l'eventuale ripristino tempestivo dei servizi erogati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze sia all'interno che all'esterno del contesto aziendale.*

- Devono essere attentamente identificati e valutati, in termini di probabilità di accadimento e

Headquarter
Via Giovanni Calvino, 38a
44122 Ferrara FE - Italy
T. 0532 206288 - 0532 214802

possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità del business
- Devono essere definiti le tempistiche delle attività di ripristino ed i relativi costi e le modalità più idonee a permettere all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto, in modo tale da consentire la riduzione delle conseguenze negative sull'azienda

MONITORAGGIO, TRACCIAMENTO E VERIFICHE TECNICHE

Obiettivo: *garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni.*

- I sistemi informativi devono essere periodicamente controllati in modo da valutare il corretto funzionamento dei sistemi di sicurezza, hardware e software, implementati, nonché l'eventuale presenza di vulnerabilità non riscontrate o conosciute in passato
- A fronte dei risultati di tutte le attività di monitoraggio, tracciamento e verifica devono essere effettuate periodiche attività di analisi, volte all'identificazione delle aree critiche e delle opportune azioni correttive e migliorative
- Devono essere pianificate attività periodiche di audit del sistema di gestione della sicurezza delle informazioni

CICLO DI VITA DEI SISTEMI E DEI SERVIZI

Obiettivo: *assicurare che gli aspetti di sicurezza siano inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.*

I requisiti di garanzia e di sicurezza sono rispettati all'inizio di ogni progetto di sviluppo per garantire che siano efficaci e che non vi siano ripercussioni negative sul progetto o sul prodotto.
I requisiti di sicurezza non sono in nessun caso considerati separatamente dai requisiti funzionali dei sistemi. Per considerare in modo efficace la sicurezza, occorre pianificarla fin dall'inizio del processo di sviluppo e/o manutenzione per garantire che sia inserita nel contesto del sistema.

- Nella fase di progettazione e sviluppo devono essere gestite le seguenti tematiche:
  - inclusione dei requisiti di sicurezza nelle specifiche funzionali dei servizi e sistemi
  - adozione di best-practice per lo sviluppo e la manutenzione del software
  - gestione controllata della documentazione
  - separazione degli ambienti di sviluppo e test
- Nella fase di erogazione del servizio devono essere gestite le seguenti tematiche:
  - capacity management dell'infrastruttura tecnologica
  - miglioramento della sicurezza dei sistemi e dei dati (configuration management, installazione di sistemi anti-malware)
  - gestione dei cambiamenti
  - adozione di procedure di backup e restore
  - adozione di procedure di dismissione controllata dei sistemi
  - monitoraggio dei sistemi e servizi
  - gestione utenze
  - performance monitoring

RISPETTO DELLA NORMATIVA

Obiettivo: *garantire il rispetto delle disposizioni di legge, di regolamenti o obblighi contrattuali e di*

Headquarter
Via Giovanni Calvino, 38a
44122 Ferrara FE - Italy
T. 0532 206288 - 0532 214802

ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.

- Tutti i requisiti normativi e contrattuali in materia di sicurezza del sistema informativo e aventi impatto sul Sistema di Gestione della Sicurezza delle Informazioni devono essere identificati ed analizzati, al fine di valutarne gli impatti sull'organizzazione e sui sistemi informativi
- I responsabili delle diverse aree devono assicurarsi, ciascuno nell'ambito di propria competenza, che tutte le politiche, le procedure, gli standard e in generale tutta la documentazione relativa alla sicurezza delle informazioni siano applicati e rispettati
- Il mancato rispetto di quanto indicato in questo documento, e in tutti gli altri che da esso discendono, sarà gestito in ottemperanza a quanto previsto nel CCNL oppure, nel caso di inadempienze di terze parti, secondo i rapporti contrattuali in essere

RESPONSABILE DELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Il responsabile del sistema di gestione della sicurezza delle informazioni, supportato dalla Direzione, dovrà farsi promotore, al fine di rendere la politica generale di sicurezza coerente con l'evoluzione del contesto aziendale, delle eventuali azioni da intraprendere a fronte del verificarsi di eventi quali:

- nuove minacce o modifiche a quelle considerate nelle precedenti attività di analisi del rischio
- significativi incidenti di sicurezza
- evoluzione del contesto normativo e legislativo in materia di sicurezza delle informazioni
- risultati di analisi sui costi, impatti, efficacia ed efficienza del sistema di gestione per la sicurezza delle informazioni