golemmed
a GOLEM SOFTWARE Company

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

REV.	DATA	NOTA DI REVISIONE
0	02/09/2020	Prima emissione

Emesso da	**RSI**	Approvata da	**DA**

1 INTRODUZIONE

1.1 PREMESSA

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni che GOLEM MED ha fatto propri al fine di realizzare e mantenere un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.
Tali principi sono concretizzati nelle Policy per la sicurezza delle informazioni (nonché sintetizzati all'interno del "Manuale di Gestione Integrato"), la quale rispecchia le reali esigenze derivanti dalla tipologia di attività svolte da GOLEM MED.
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;
- Autenticità: garantire la provenienza dell'informazione;
- Non ripudio: assicurare che l'informazione sia protetta da falsa negazione di ricezione, trasmissione, creazione, trasporto e consegna.

La mancanza di adeguati livelli di sicurezza, in termini di Riservatezza, Disponibilità, Integrità, Autenticità e Non Ripudio, 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 economica e 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 Informatica Trentina. Di conseguenza, è essenziale per la società identificare le esigenze di sicurezza sia di natura esterna che derivanti dal cogente. Tale attività viene realizzata attingendo a diverse fonti:

- Analisi dei rischi: consente all'azienda di acquisire la consapevolezza e la visibilità sul livello di esposizione al rischio del proprio sistema informativo. Sulla base di tale livello sono individuate le misure di sicurezza idonee.

La valutazione del rischio consiste nella sistematica considerazione dei seguenti elementi:

- danno che può derivare dalla mancata applicazione di misure di sicurezza al sistema informativo, considerando le potenziali conseguenze derivanti dalla perdita di riservatezza, integrità, disponibilità, autenticità e non ripudio delle informazioni;
- realistica probabilità di come sia possibile perpetrare un attacco alla luce delle minacce individuate.

I risultati della valutazione aiutano a determinare quali siano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee rispetto ai propri obiettivi , in base alla definizione del livello di rischio residuo che l'azienda decide di accettare, da implementare successivamente.

- Principi ispiratori: sono indicati nel Capitolo 2 intitolato "Policy". Rappresentano il sistema dei valori in cui l'azienda crede con riferimento alla gestione della sicurezza del proprio sistema informativo. Si tratta delle idee di fondo che l'azienda ha maturato nei riguardi della sicurezza delle informazioni, ovvero che cosa sia giusto fare, o meno, per disporre di un sistema di gestione della sicurezza efficiente, efficace e adeguato alle proprie necessità. Il riferimento primario dei principi generali di sicurezza è lo standard ISO/IEC 27002.
- Leggi e contratti: nell'ambito del contesto normativo esistente, vengono fornite indicazioni su come affrontare le problematiche della sicurezza e su come gestire l'utilizzo dei sistemi informativi. Il rispetto della legislazione italiana relativa alla sicurezza serve, oltre che per limitare i rischi di un coinvolgimento dell'azienda, anche per garantire un livello minimo di sicurezza del sistema informativo da proteggere.

La presente policy, nel rispetto delle principali norme e degli standard in materia:

- sottolinea l'importanza di garantire la sicurezza delle informazioni e degli strumenti atti al trattamento delle stesse;
- è coerente con la volontà espressa dalla società di garantire la protezione del patrimonio informativo;
- ha come oggetto aspetti fisici, logici ed organizzativi del Sistema di Gestione della Sicurezza delle Informazioni.

1.2 PERIMETRO ORGANIZZATIVO

La presente policy si applica a tutto il personale dipendente di GOLEM MED e a tutti i soggetti che collaborano con Informatica Trentina.
La policy si applica inoltre a tutti i processi più in generale a tutte le risorse coinvolte nella gestione delle informazioni trattate dalla società.

1.3 TERMINI E DEFINIZIONI

Asset o Bene – Qualsiasi risorsa che abbia un valore per l'organizzazione, sia essa materiale o immateriale (es. beni fisici, software, informazioni e dati,..).
Autenticità – Proprietà per la quale è garantito che l'identità di un soggetto o di una risorsa è quella dichiarata; l'autenticità si applica ad entità quali utenti, processi, sistemi ed informazioni (ISO/IEC 13335-1).
Disponibilità – Proprietà per la quale le informazioni sono rese accessibili ed utilizzabili su richiesta di un entità autorizzata (ISO/IEC 13335-1).
Integrità – Proprietà per la quale l'accuratezza e la completezza degli asset è salvaguardata (ISO/IEC 13335-1).
Non ripudio – Capacità di dimostrare che un'azione o un evento hanno avuto luogo, in modo che questo evento od azione non possano essere ripudiati successivamente (ISO/IEC 13335-1).
Riservatezza – Proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati (ISO/IEC 13335-1).
Hardening – Insieme di azioni atte ad analizzare le funzionalità di un sistema operativo/applicazione al fine di individuare la configurazione ottima che permetta di innalzare il livello di sicurezza e ridurre il rischio residuo connesso alle debolezze dei sistemi.

1.4 RIFERIMENTI

Norme di legge
DLGs 196 del 30/06/2003 "Codice in materia di protezione dei dati personali"
REGOLAMENTO 2016/679/UE "Regolamento europeo in materia di protezione dei dati personali"
Standard di Riferimento
UNI CEI ISO/IEC 27001 – "Tecnologia per l'Informazione – Tecniche per la Sicurezza – SGSI - Requisiti"
ISO/IEC 27002 - "Information technology – Security techniques – Code of practice for information security management"
ISO/IEC 13335-1 - "Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management"
A documenti del Sistema Sicurezza

2 POLICY

2.1 PRINCIPI GENERALI

I principi generali cui GOLEM MED si ispira nella gestione della sicurezza delle informazioni sono articolati nelle seguenti tematiche:

- Identificazione, classificazione e gestione delle risorse

- Gestione sicura degli accessi logici
- Norme comportamentali per la gestione sicura delle risorse aziendali
- Personale e Sicurezza
- Gestione degli eventi anomali e degli incidenti
- Gestione della sicurezza fisica
- Aspetti contrattuali connessi alla sicurezza delle informazioni
- Gestione della Business Continuity
- Monitoraggio, tracciamento e verifiche tecniche
- Ciclo di vita dei sistemi e dei servizi
- Rispetto della normativa

Di seguito, si riporta, per ciascuna tematica, l'obiettivo e le linee guida definite da Informatica Trentina.

2.2 IDENTIFICAZIONE, CLASSIFICAZIONE E GESTIONE DELLE RISORSE

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

- Deve esistere ed essere mantenuto aggiornato, nel corso del tempo, 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) deve essere direttamente associabile ad un responsabile.
- Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con 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.

2.3 GESTIONE SICURA DEGLI ACCESSI LOGICI

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 (c.d. principio del "need-to-know"). 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 subordinata 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' necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso.
- I sistemi che costituiscono l'infrastruttura ICT devono essere opportunamente protetti e segregati, in modo da minimizzare la possibilità degli accessi non autorizzati.

2.4 NORME COMPORTAMENTALI PER LA GESTIONE SICURA DELLE RISORSE AZIENDALI

Obiettivo: garantire che i dipendenti e collaboratori di GOLEM MED 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.

2.5 PERSONALE E SICUREZZA

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

▪ Nelle fasi di selezione ed inserimento del personale in GOLEM MED 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 GOLEM MED il personale deve ricevere un'adeguata e continuativa formazione inerente le tematiche di sicurezza dei dati.

▪ Le modalità di chiusura del rapporto di lavoro con GOLEM MED dovranno essere coerenti con gli obiettivi di sicurezza aziendale.

2.6 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 non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure.

▪ Deve esistere un sistema di registrazione e classificazione degli incidenti e degli eventi anomali per effettuare analisi volte al miglioramento dei livelli di sicurezza coerentemente con le reali problematiche riscontrate.

2.7 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:

• l'individuazione delle aree e la classificazione dei locali in base alla criticità delle informazioni elaborate;

• la definizione dei livelli adeguati di protezione.

▪ Deve essere garantita la sicurezza delle apparecchiature tramite:

• la definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni;

• la messa a disposizione delle risorse necessarie al loro funzionamento;

• la predisposizione di un adeguato livello di manutenzione.

2.8 ASPETTI CONTRATTUALI CONNESSI ALLA SICUREZZA DELLE INFORMAZIONI

Obiettivo: assicurare la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti, in accordo con le caratteristiche specifiche della relazione che GOLEM MED deve instaurare con le terze parti stesse.

▪ Gli accordi con le terze parti e con gli outsourcer 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 e con gli outsourcer, ove necessario, devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali ("normativa privacy").

2.9 GESTIONE DELLA BUSINESS CONTINUITY

Obiettivo: garantire la continuità dell'attività di GOLEM MED 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 possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità del business.

▪ Deve essere predisposto un piano di continuità che permetta all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che consentano la riduzione delle conseguenze negative sulla missione aziendale.

▪ Devono essere preparate, validate e opportunamente divulgate tutte le procedure operative ed organizzative necessarie per assicurare l'implementazione del piano di continuità.

▪ Devono essere periodicamente effettuati i test per tutti i componenti del piano di continuità.

▪ Deve essere assicurato il mantenimento e l'aggiornamento dei piani e delle procedure di cui ai punti precedenti al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi/tecnologici.

2.10 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.

2.11 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.

▪ Nella fase di progettazione e sviluppo devono essere opportunamente considerati gli aspetti di sicurezza. In particolare devono essere indirizzate 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 con impiego di procedure formali di accettazione nel passaggio fra ambienti.

▪ Nella fase di esercizio devono essere opportunamente considerati gli aspetti di sicurezza. In particolare devono essere indirizzate le seguenti tematiche:

• capacity management dell'infrastruttura tecnologica;
• securizzazione dei sistemi e dei dati (configuration management, hardening, installazione di sistemi anti-malware, crittografia);
• utilizzo di procedure di change management;
• adozione di procedure di backup e restore;
• adozione di procedure di dismissione controllata dei sistemi (per esempio cancellazione sicura dei dischi);
• network security: segregazione delle reti, monitoraggio dei gateway (firewall).

▪ Nella gestione dei servizi devono essere opportunamente considerati gli aspetti di sicurezza. In particolare devono essere indirizzate le seguenti tematiche:

• monitoraggio dei sistemi e servizi;

• gestione utenze;
• performance monitoring.

2.12 RISPETTO DELLA NORMATIVA

Obiettivo: garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la 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.

3 DEFINIZIONE DEI RUOLI E DELLE RESPONSABILITÀ

3.1 STRUTTURA RESPONSABILE DELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

La struttura responsabile del sistema di gestione della sicurezza delle informazioni dovrà farsi promotrice, 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.

Palmi, lì 02/09/2020

LA DIREZIONE

_____