POLITICA DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI DEL GRUPPO PRESENT

Premessa

In considerazione della natura delle proprie attività, Present giudica la sicurezza delle informazioni un fattore irrinunciabile per l'importanza del proprio business, oltre a rappresentare un elemento di valenza strategica ed un vantaggio competitivo rilevante nel panorama di riferimento del mercato delle aziende di servizi ICT.

A tale scopo Present ha definito e mantiene attivo un Sistema di Gestione della Sicurezza delle informazioni (SGSI) conforme a quanto espresso nella Norma ISO/IEC 27001:2022, inserito all'interno di un più ampio Sistema di Gestione Integrato (SGI).

La Politica del SGSI del Gruppo Present è orientata ad assicurare la condotta dell'azienda a tutela dell'integrità, della riservatezza e della disponibilità del patrimonio informativo proprio e dei propri Clienti, trattato nell'ambito del business di erogazione dei servizi, attraverso il miglioramento continuo delle capacità organizzative e tecniche, in ottemperanza ai requisiti dello Standard internazionale di riferimento e agli obblighi cogenti del quadro normativo di riferimento.
Per valorizzare il patrimonio del proprio Sistema di Gestione delle Sicurezza delle Informazioni a supporto delle attività di pianificazione, progettazione, implementazione e gestione di infrastrutture ICT, nonché di progettazione, installazione e manutenzione di sistemi informativi, Present definisce, attua e comunica le Politiche articolate nei seguenti due livelli:

- **Politica generale**: è descritta nel presente documento e definisce "gli orientamenti e gli indirizzi generali come formalmente espressi dalla Direzione" (ISO 27000, 2.28).
- Politiche specifiche o più comunemente "**Linee guida**": estendono e dettagliano la Politica generale, declinandola agli ambiti operativi e/o ai contesti organizzativi di Present, sulla base del recepimento dei singoli obblighi derivanti da normative di legge o da specifiche contrattuali, nonché dai requisiti fissati dagli Standard internazionali in materia di sicurezza delle informazioni. Le Linee Guida sono da intendersi a tutti gli effetti parte integrante della presente Politica e come tali devono essere riesaminate regolarmente e poste all'attuazione di modifiche al variare dei fattori che le influenzano, per garantire che rimangano nel tempo idonee alle finalità dell'Organizzazione di Present e alle aspettative di tutte le parti interessate.

La Direzione di Present ha espresso in modo formale gli indirizzi generali della Politica del proprio SGSI, riassunti nei principi, obiettivi e impegni.

Present ha inoltre definito, attraverso Politica del proprio SGSI, le responsabilità e il governo della sicurezza delle informazioni, consapevole dell'importanza del processo culturale e organizzativo che quest'ultima sottende. Come tale è richiesto il coinvolgimento a tutti i livelli e in modo pervasivo nell'operatività individuale di tutte le risorse umane, con particolare riferimento alle unità aziendali che operano, direttamente e/o indirettamente, all'interno del perimetro di certificazione.

Present S.p.A.
Cap. Sociale: € 2.000.000 - CF e P.IVA 06696370961 - REA n. 1909017 Milano - www.it-present.com - info@it-present.com

MILANO
Sede legale e operativa
Via Cechov 48
20151 Milano
tel. +39 02 30012 1

ROMA
Sede operativa
Via Maglianella 65/H
00166 Roma
tel. +39 06 59012.1

TORINO
Sede operativa
Strada della Cebrosa 86
10156 Torino
tel. +39 011 0460.201

BOLOGNA
Sede operativa
Via di Corticella 89
40128 Bologna
tel. +39 02 30012 1

PADOVA
Sede operativa
Via delle Croce Rossa, 8
35129 Padova
tel. +39 02 30012 1

NAPOLI
Sede operativa
Via G. Luraghi
80038 Pomigliano D'arco NA
tel. +39 02 30012 1

Principi

La cultura della sicurezza

Il SGSI di Present si basa sul principio primario della diffusione della cultura della sicurezza del patrimonio informativo gestito dei propri Clienti, costituito da qualunque tipo di aggregazione di dati a prescindere dalla forma e dalla tecnologia utilizzata per il loro trattamento e conservazione.

In particolare, promuove a tutti i livelli l'attenzione e la sensibilità alla tutela delle informazioni, che deve avvenire in misura proporzionale alla sua importanza a livello di business e consiste nel prevedere ed implementare contromisure di sicurezza adeguate alle diverse forme ed alle differenti modalità di interazione utilizzate.

Il rispetto delle regole della sicurezza

Il SGSI di Present definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base, che devono essere rispettate a tutti i livelli aziendali:

- ***riservatezza***, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- ***integrità***, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- ***disponibilità***, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi;
- ***autenticità***, ovvero la garanzia che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che l'ha trasmessa.

Obiettivi

Inoltre con la presente Politica Present intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- proteggere al meglio il patrimonio informativo gestito dei propri Clienti in conformità agli accordi contrattuali stabiliti (definiti all'interno di apposite linee guida della sicurezza);
- preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- adottare le misure atte a garantire la formazione e la consapevolezza del personale, mantenendo nel tempo adeguati livelli di conoscenza e competenza;
- rispondere a precise esigenze di sicurezza e organizzazione del lavoro sulla base delle indicazioni delle normative vigenti e cogenti, ed in particolare a:
  - Data Privacy: principali riferimenti normativi, in ambito italiano ed internazionale, sul tema della tutela della riservatezza e della protezione dei dati personali;
  - Disciplina della responsabilità amministrativa d'impresa: principali riferimenti normativi ai reati riconducibili alla frode informatica in danno dello stato o di altro ente pubblico, ai delitti informatici e trattamento illecito di dati;
- adottare, quando applicabile, ulteriori soluzioni di sicurezza delle informazioni rese disponibili dall'innovazione tecnologica.

Il continuo miglioramento

Il raggiungimento dei risultati deve avvenire attraverso un processo di miglioramento continuo del SGSI al quale contribuiscono tutte le parti interessate tra le quali giocano un ruolo fondamentale:

- **la Direzione** che ha il compito di definire la Politica e gli obiettivi, il contesto e l'ambito, i ruoli e le responsabilità del Personale;
- **il Personale** che utilizza il SGSI e mette in atto le politiche ed i requisiti di sicurezza per raggiungere gli obiettivi prefissati;
- **i Clienti** che usufruiscono dei servizi e che devono essere garantiti per le loro esigenze di sicurezza, in misura conforme agli impegni assunti da Present;
- **i Fornitori** che contribuiscono al raggiungimento degli obiettivi dell'organizzazione e che accettano ed operano in conformità alle politiche di sicurezza connesse alla fornitura.

Impegni

Crescita e partecipazione del personale

Chiunque, nell'ambito delle proprie funzioni e responsabilità, è chiamato ad operare con l'obiettivo di offrire ai Clienti servizi ad elevato standard di sicurezza, in conformità a quanto specificato nella presente Politica, senza far venire mai meno il proprio impegno alla crescita di un SGSI efficacie ed efficiente.

Disponibilità di risorse e mezzi

La Direzione si impegna a mettere a favore del SGSI risorse e mezzi adeguati, garantendo la congruità degli investimenti coerentemente alla Politica e alle linee strategiche aziendali definite.

Responsabilità

Il raggiungimento degli obiettivi della sicurezza di Present è possibile solo attraverso il supporto di tutte le strutture aziendali, ciascuna per la parte di propria competenza.

Present, così come previsto dalla Norma ISO/IEC 27001, ha definito nella propria organizzazione un insieme di funzioni e ruoli organizzativi per presidiare e gestire al meglio le tematiche di sicurezza delle informazioni. Ruoli e responsabilità sono illustrati nel relativo documento che costituisce parte integrante dell'impianto descrittivo del sistema di gestione.

In particolare, nella presente Politica si desidera richiamare il ruolo che rivestono:

- ***tutto il personale a qualsiasi titolo:*** il quale collabora con l'azienda ed è responsabile dell'osservanza di questa Politica e della segnalazione di incidenti di sicurezza, anche non formalmente codificati, di cui dovesse venire a conoscenza;
- ***tutti i soggetti esterni (coloro che intrattengono rapporti di collaborazione con Present):*** sono responsabili di garantire la conoscenza, la condivisione ed il rispetto dei principi e dei requisiti di sicurezza esplicitati dalla presente Politica ed inclusi nei corrispondenti contratti di collaborazione.

Governo

I principali criteri su cui Present basa la governance della sicurezza del patrimonio informativo dei propri Clienti sono sintetizzabili in quattro punti fondamentali:

- **metodologie, standard e linee guida:** oltre al rispetto dei numerosi standard tecnici, Present basa la sicurezza delle informazioni su un insieme di principi guida dettati dall'azienda che garantiscono circa la conformità del servizio erogato alle norme di riferimento e agli standard metodologici consolidati;
- **organizzazione:** prevede un insieme di funzioni e ruoli organizzativi per presidiare e gestire le tematiche di Sicurezza delle Informazioni, tra i quali vi sono: Comitato di crisi, Comitato della sicurezza, Chief Security Officer, Technical Information Security Officer, specialisti dei domini di competenza per le varie aree: ICT, HR, Operations, Finance;
- **revisione:** stabilisce gli adeguamenti attraverso le relazioni operative come i "Security Meeting", focalizzati sui temi di maggiore rilievo e che vedono il coinvolgimento dei responsabili delle strutture tecniche e operative dell'azienda;
- **controllo interno e gestione "security incidents":** vengono garantite le attività periodiche di audit atte a verificare la conformità del sistema con la Politica e gli standard di sicurezza adottati dall'azienda. Inoltre, è previsto un processo di gestione degli incidenti relativi alla sicurezza ("security incidents") che prevede di identificare, secondo il framework ITIL v3, i seguenti stadi:
  - preventivo: le misure di sicurezza sono definite con lo scopo di evitare (prevenire) incidenti;
  - riduttivo: le misure di sicurezza sono orientate alla riduzione del danno;
  - investigativo: le misure di sicurezza sono orientate all'identificazione immediata (o a breve termine) dell'incidente;
  - repressivo: le misure di sicurezza sono orientate a contrastare la causa dell'incidente;
  - correttivo: le misure di sicurezza sono orientate alla correzione dei danni provocati;
- **formazione:** tutto il personale riceve regolarmente una formazione sulla sicurezza

Analisi e gestione rischi

Il SGSI di Present si fonda sull'Analisi e Gestione dei Rischi di Sicurezza.

L'Analisi e Gestione dei Rischi di Sicurezza delle Informazioni è il processo attraverso il quale l'Azienda: esegue una valutazione dei rischi che possono avvenire e causare perdite all'organizzazione, procede al trattamento dei rischi individuati in modo proporzionale al valore delle informazioni da proteggere.

La Direzione di Present ritiene adeguato l'utilizzo di una metodologia di valutazione dei rischi di tipo qualitativo basata su quattro livelli (critico, alto, medio, basso), nella convinzione che per meglio comprendere ogni fenomeno di rischio sia preferibile osservarlo, esaminarlo e giudicarlo nel suo contesto, a prescindere da qualunque analisi dei dati fondata su complesse elaborazioni statistiche e/o modelli matematici. L'analisi dei rischi deve tenere principalmente in considerazione i requisiti di sicurezza connessi ai servizi di business, nonché quelli derivanti dalle leggi e dalle normative di settore (ad esempio Data Privacy per la protezione ed il trattamento delle informazioni personali).

Inoltre, il processo di gestione rischi di sicurezza e il SGSI sono allineati al paradigma ciclico (Plan, Do, Check, Act). Questo assicura che tutte le attività del SGSI sono eseguite nel tempo tenendo sempre in considerazione i rischi connessi.

Il processo si fonda su una metodologia che deriva dalle linee guida fornite da ISO/IEC 27005 (Information Security Risk Management) e che permette l'identificazione, la valutazione ed il trattamento dei Rischi di Sicurezza delle Informazioni. In maniera conforme a quanto previsto dalla Norma ISO/IEC 27001, l'insieme dei controlli di sicurezza selezionati a seguito del processo di analisi e gestione dei rischi è incluso nel documento "SoA" (Statement of Applicability). Le azioni di trattamento dei rischi di Sicurezza delle Informazioni sono raccolte e monitorate nel documento "Piano di Trattamento Rischi".

Applicabilità e violazioni

La presente Politica, nei suoi principi generali, si applica indistintamente a tutte le società del Gruppo, a tutti gli enti di staff e alle business unit dell'azienda. La sua attuazione è obbligatoria per tutto il personale del Gruppo Present e si inserisce nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno, quale fornitore e collaboratore che, a qualsiasi titolo, possa venire a conoscenza delle informazioni gestite in azienda in qualsivoglia forma (elettronica, cartacea, verbale, ecc.), sia che siano di proprietà di Present, tenute in custodia per conto dei propri clienti o utilizzate da Present. Present consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole, delle norme cogenti e degli impegni contrattuali.

Le eventuali violazioni a questa Politica possono dar luogo a "sanzioni disciplinari" nel rispetto della procedura descritta al paragrafo di pari oggetto del Regolamento Aziendale.

La Politica del SGSI, redatta dal Chief Security Officer (CSO), è approvata dalla Direzione di Present e in particolare dal Comitato Executive Committee.
La revisione sarà fatta, a cura del Comitato della sicurezza, almeno una volta all'anno o in occasione di significative modifiche organizzative e/o tecnologiche rilevanti per la gestione delle informazioni, verificandone la sua efficacia ed efficienza al fine di garantire un adeguato supporto per l'adozione delle necessarie migliorie e consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali.
La revisione della Politica del SGSI non potrà prescindere dalla verifica e dalla validazione sia delle Linee guida, della quale sono parte integrante, sia dell'analisi del contesto (interno ed esterno) che ne caratterizza ed orienta gli indirizzi.

Gruppo Present

Chief Security Officer

Tipo:	Politica			**Codice:**	SGSI-DG-PA
Classe:	Pubblico	**Rel. / Rev.:**	6.01	**Stato:**	Rilasciato
Redatto da:	Bossina Ermete	**Data:**	29/05/2024	**Firma:**	
Approvato da:	Comitato Executive Committee	**Data:**	20/06/2024	**Firma:**	