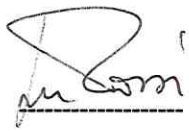
consulfin

INFORMATION SECURITY POLICY

Rev.	Data	Motivo della revisione	Infrastructure & Security	Responsabile Compliance	Approvazione Amm.re
00	04/01/2024	Prima emissione	F. Roberto	S. Mastrofini	L. Rossi
					

consulfin

INDICE

consulfin

1. Premessa, scopo e ambito di applicazione

Il patrimonio informativo rappresenta una componente fondamentale per raggiungere gli obiettivi di Business.

La salvaguardia del patrimonio informativo assume, pertanto, un'importanza strategica per le aziende in generale e per Consulfin srl in particolare.

I temi connessi alla protezione e gestione "sicura" delle informazioni sono peraltro presi in considerazione da una normativa sempre più vasta che richiede, anche dal punto di vista organizzativo, comportamenti, sistemi di controllo e interventi rivolti alla protezione delle informazioni personali.

Ne deriva la necessità di presidiare adeguatamente le tematiche di sicurezza con modelli organizzativi per il governo del patrimonio informativo che presentino un approccio ampio e strutturato.

La sicurezza deve essere quindi garantita, in coerenza con un processo continuativo, in coerenza con normative, standard e best practices internazionali.

Il presente documento ha lo scopo di definire l'Information Security Policy adottata da Consulfin srl che devono essere di riferimento nello svolgimento delle attività aziendali per la salvaguardia del patrimonio informativo aziendale.

Il documento è rivolto a tutto il personale di Consulfin srl.

2. Riferimenti normativi

Regolamento (UE) 2016/679 – Regolamento generale sulla protezione dei dati (di seguito GDPR);

D. Lgs. 196/2003, come modificato dal D. Lgs. 101/18 – Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito Codice Privacy);

Norma UNI EN ISO 9001 – Sistema di qualità

3. Politica di Sicurezza Informatica

Il patrimonio informativo è costituito dall'insieme dei dati e delle informazioni trattate e rappresenta una componente fondamentale per raggiungere gli obiettivi di Business.

consulfin

Come espresso nella Politica per la Qualità e la Sicurezza delle informazioni del Sistema di Gestione Integrato, la tutela del patrimonio informativo di Consulfin srl si raggiunge con la realizzazione di una serie di misure di protezione e verifica di tipo organizzativo, normativo e tecnologico, finalizzate al rispetto dei tre requisiti fondamentali per la sicurezza delle informazioni:

• riservatezza – le informazioni devono essere accessibili ai soli soggetti autorizzati;

• integrità – le informazioni devono essere aggiornate in modo accurato e completo secondo le modalità previste;

• disponibilità – le informazioni devono essere accessibili ed utilizzabili nei tempi e nei modi definiti.

Il Sistema di Gestione della Sicurezza delle Informazioni di Consulfin srl si basa sui seguenti principi:

• Le misure di protezione devono essere commisurate alla criticità delle informazioni gestite. Questo consente di coniugare l'esigenza di tutela del "valore" delle informazioni con la necessità di assicurare efficienza dei processi amministrativi, gestionali e di business.

• Gli interventi di controllo e verifica devono essere predisposti con modalità continuative e replicabili. Questo consente una valutazione continua di congruenza delle contromisure adottate rispetto ai mutamenti di scenario intervenuti.

• I compiti e le responsabilità nell'ambito del SGSI (Sistema Gestione Sicurezza Informazioni) devono essere assegnati alle strutture organizzative coinvolte seguendo un approccio coordinato e unitario. Questo consente di preservare la sicurezza del patrimonio informativo in modo sinergico, con economie di scala.

• La "cultura della sicurezza" deve essere diffusa e mantenuta in azienda. Questo consente una presa di coscienza da parte del personale relativamente ai rischi connessi con la sicurezza e alle proprie responsabilità, favorendo comportamenti vigili e coerenti.

• Il processo di miglioramento deve essere attuato con continuità seguendo il ciclo PDCA (Plan, Do, Check, Act). Questo consente di promuovere una cultura della qualità e conseguentemente della sicurezza, tesa al miglioramento continuo dei processi e all'utilizzo ottimale delle risorse.

4. Funzioni organizzative coinvolte

Di seguito sono riportate le principali figure organizzative coinvolte nel Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di Consulfin srl

consulfin

• IL RESPONSABILE COMPLIANCE:

- approva ed emana il presente documento di Information Security Policy;

- approva il Sistema di Gestione della Sicurezza delle Informazioni (SGSI);

- approva interventi per la mitigazione di rischi di sicurezza elevati;

- riceve aggiornamenti periodici sullo stato del SGSI e sulle situazioni di rischio presenti.

• L'HEAD OF INFRASTRUCTURE & SECURITY:

- definisce, attua e mantiene il Sistema di Gestione della Sicurezza delle Informazioni (SGSI);

- assicura che il SGSI sia conforme ai requisiti del presente documento di *Information Security Policy;*

- riferisce almeno con cadenza semestrale al Group CEO sullo stato del SGSI e sulle situazioni di rischio presenti.

• Il MANAGEMENT DIREZIONALE:

- assicura un adeguato supporto alle iniziative di sicurezza, verificandone l'esecuzione nei tempi previsti;

- concorda gli interventi di sicurezza, garantendo adeguata copertura di budget.

• I RESPONSABILI DELLE UNITA' ORGANIZZATIVE:

- supportano l'Head of Infrastructure & Security nella realizzazione e nel mantenimento del Sistema di Gestione della Sicurezza delle Informazioni (SGSI);

- assicurano che le attività vengano svolte nel rispetto delle Procedure definite;

- favoriscono la consapevolezza dei contenuti del presente documento di Information Security Policy da parte del personale loro assegnato.

5. Linee Guida di Sicurezza Informatica

Di seguito le Linee Guida di Sicurezza Informatica che indirizzano le diverse Procedure

5.1 Valutazione e gestione dei rischi informatici

Il livello dei rischi informatici aziendali deve essere conosciuto, devono essere condivise le strategie per contenerli e devono essere accettati i rischi residui. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

consulfin

• valutazione del rischio: devono essere individuate le minacce cui sono esposte le risorse informatiche in termini di riservatezza, integrità e disponibilità e valutato il relativo rischio, in termini di probabilità che si verifichi una minaccia e di impatto che tale evento produrrebbe sul Business Aziendale;

• trattamento del rischio: devono essere individuate le misure di attenuazione, di tipo tecnico od organizzativo, idonee a contenere il rischio potenziale ad un livello aziendalmente accettabile e deve essere definito e Approvato il piano di realizzazione di tali misure.

5.2 Protezione fisica del patrimonio informativo

Il patrimonio informativo deve essere protetto mediante la predisposizione e il mantenimento di contromisure di natura fisica. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

• sicurezza delle aree fisiche: devono essere predisposti e protetti appositi perimetri e aree dedicate, in particolare per il Data Center, definendo opportune modalità di controllo degli accessi per scongiurare accessi non autorizzati che potrebbero portare ad alterazione o sottrazione degli asset informatici;

• sicurezza delle apparecchiature informatiche: le apparecchiature informatiche devono essere installate e gestite in modo tale da garantire nel tempo la loro integrità e disponibilità; ed attrezzate con appropriati apparati di supporto atti a garantirne la continuità;

• sicurezza delle apparecchiature in dotazione o in uso: le apparecchiature informatiche in dotazione, nonché i dispositivi utilizzati quali fax, fotocopiatrici, telefoni, ecc., devono essere protetti anche attraverso opportune norme che ne disciplinino la conservazione e la protezione, compresi i periodi di assenza temporanea o permanente dell'utente.

5.3 Gestione degli accessi logici

Le informazioni devono essere protette mediante opportune contromisure al fine di garantire che solo le persone autorizzate possano accedervi. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

• requisiti di sicurezza per il controllo degli accessi: l'accesso al patrimonio informativo deve essere definito sulla base delle esigenze connesse con le attività operative svolte dagli utenti (principio della conoscenza minima o need to know);

• autenticazione: l'accesso al sistema informativo (Rete, Sistemi e Applicazioni) deve essere controllato da appositi meccanismi di autenticazione (ad es. credenziali di autenticazione) al fine di consentire l'accesso ai soli utenti autorizzati;

consulfin

• gestione delle credenziali: devono essere stabilite modalità per la definizione, gestione nel tempo e cancellazione delle credenziali di autenticazione degli utenti; gli utenti devono essere informati delle proprie responsabilità in merito;

• monitoraggio degli accessi al Sistema Informativo: l'accesso e l'utilizzo del Sistema Informativo deve essere soggetto a registrazione e successiva analisi delle attività effettuate. In particolare, in ottemperanza a normative di legge (ad es. Amministratori di Sistema).

5.4 Gestione operativa di sistemi e telecomunicazioni

I sistemi, le reti e gli apparati mediante i quali viene gestito il patrimonio informativo, devono essere tutelati al fine di preservare la riservatezza, l'integrità e la disponibilità delle informazioni attraverso una gestione operativa efficace, efficiente e controllata. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

• procedure operative e responsabilità: deve essere assicurata la separazione dell'ambiente di Produzione dagli altri ambienti (Sviluppo, Test, Quality); devono essere definiti piani e procedure per la corretta pianificazione e gestione dei salvataggi dei dati e dei sistemi;

• pianificazione e accettazione dei sistemi: occorre pianificare in anticipo la capacità dei sistemi, oltre che dell'impiantistica a supporto del loro funzionamento, in modo da assicurare che la capacità elaborativa degli stessi sia sufficiente per evitare malfunzionamenti in seguito a sovraccarichi; devono, inoltre, essere stabiliti criteri di accettazione per i nuovi sistemi nonché per gli aggiornamenti degli stessi;

• protezione dai software dannosi: è necessario predisporre opportune misure per prevenire l'ingresso di software dannoso attraverso la predisposizione di sistemi antivirus; devono essere effettuate verifiche periodiche di vulnerabilità sui sistemi e sulle applicazioni al fine di individuare e rimuovere eventuali debolezze sfruttabili dai malware;

• protezione della rete: è necessario adottare le opportune contromisure per rendere sicura la rete attraverso adeguate configurazioni degli apparati e controllandone il traffico per garantire la corretta e sicura circolazione delle informazioni;

• gestione dei supporti di memorizzazione: devono essere definite le modalità di custodia, riutilizzo, riproduzione e distruzione dei supporti rimuovibili di memorizzazione delle informazioni, al fine di proteggerli da danneggiamenti, furti o accessi non autorizzati, anche nel caso di gestione da parte di terzi;

consulfin

• strumenti per lo scambio di informazioni: gli strumenti utilizzati per lo scambio di informazioni, quali posta elettronica (e-mail), siti web (sia per effettuare operazioni elettroniche che per divulgare informazioni), file transfer, telefoni, fax, ecc., devono essere protetti in base alla tipologia di utilizzo definito e delle informazioni veicolate; occorre inoltre stabilire accordi formali con altre aziende o organizzazioni per lo scambio sicuro di informazioni e procedere a verificarli periodicamente.

5.5 Sviluppo e manutenzione delle applicazioni

Le applicazioni, mediante le quali viene gestito il patrimonio informativo, devono essere sviluppate e manutenute nel tempo al fine di preservare la riservatezza, l'integrità e la disponibilità delle informazioni.

• requisiti di sicurezza delle applicazioni: la sicurezza delle applicazioni deve essere presa in considerazione fin dalla fase di progettazione di nuove applicazioni e di modifica delle stesse. In particolare, deve essere assicurata l'aderenza alle disposizioni normative e di legge;

• processo di sviluppo delle applicazioni: il processo di sviluppo e rilascio in produzione deve essere definito e gestito in modo controllato e verificabile; le applicazioni sviluppate internamente o esternamente devono essere verificate, controllandone l'adeguatezza delle funzionalità implementate, anche rispetto ai requisiti di sicurezza definiti e documentati.

5.6 Classificazione e controllo degli asset informatici

Gli asset del patrimonio informativo devono essere inventariati; deve essere inoltre attribuito loro un valore attraverso la classificazione delle informazioni in relazione al livello di riservatezza, integrità e disponibilità. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

• gestione dell'inventario degli asset informatici: occorre definire il processo di gestione e manutenzione dell'inventario degli asset informatici;

• classificazione delle informazioni: le informazioni, indipendentemente dal tipo, dal formato, dai supporti di memorizzazione su cui sono registrate o dagli strumenti utilizzati per il loro scambio, devono essere classificate in termini di riservatezza, integrità e disponibilità, per individuarne il livello di protezione adeguato. Devono inoltre essere identificate e classificate le informazioni contenenti dati personali.

5.7 Business Continuity (Continuità Operativa)

Deve essere garantita la disponibilità dei servizi a supporto dei processi di Business e il loro ripristino a seguito di eventi che ne interrompano l'erogazione. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

consulfin

• identificazione delle necessità di Business: devono essere identificate le necessità di continuità operativa dei servizi di Business.;

• pianificazione e gestione della continuità aziendale: la continuità dei servizi di Business deve essere garantita anche a seguito di eventi imprevisti che, con diversi gradi di rilevanza, impattano sulla loro erogazione, attraverso la definizione di appropriati piani di intervento che consentano il ripristino dei servizi entro tempi stabiliti.

• soluzione di Disaster Recovery: devono essere definiti gli scenari per cui predisporre le soluzioni di Disaster Recovery. Tali soluzioni devono prevedere sia procedure per la gestione della crisi sia il piano per il ripristino dell'operatività.

5.8 Selezione, gestione e formazione del personale

Il personale deve essere selezionato e informato anche relativamente agli aspetti di sicurezza, formalizzandone le specifiche responsabilità. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

• selezione del personale e attribuzione degli ambiti operativi e delle relative responsabilità: il personale, in quanto parte attiva del processo di tutela del patrimonio informativo, deve essere opportunamente selezionato e informato dei propri ambiti operativi e delle responsabilità in tema di sicurezza delle informazioni;

• valutazione del personale autorizzato ad operazioni critiche sui sistemi: il personale autorizzato ad effettuare operazioni critiche sui sistemi, quali ad esempio amministratori di sistema e utenti privilegiati, deve essere soggetto a valutazione sulle competenze e sull'affidabilità e a controlli sull'attività svolta.

• formazione: occorre sensibilizzare il personale tramite appositi piani di formazione e/o comunicazione in funzione dei ruoli e delle responsabilità ad esso attribuiti, per il rispetto e l'applicazione delle norme.

5.9 Gestione dei rapporti con i Fornitori di Servizi

La tutela del patrimonio informativo deve essere garantita nei rapporti con terze parti fornitori di servizi IT. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

• accordi di riservatezza: nei rapporti con terzi, fornitori di servizi IT, è necessario prevedere la loro responsabilizzazione mediante la sottoscrizione di appositi accordi di riservatezza (non disclosure agreement);

consulfin

- clausole contrattuali: a fronte di attività che richiedano l'accesso al Sistema Informativo è necessario procedere alla valutazione dei rischi connessi e alla predisposizione di clausole contrattuali affiancate da opportuni accordi di servizio.

5.10 Monitoraggio delle misure di Sicurezza

Le misure di Sicurezza devono essere monitorate per verificare il loro corretto funzionamento e per rilevare i tentativi di forzatura. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

- verifiche delle misure di sicurezza: devono essere eseguite in maniera efficace, sistematica e ripetibile, verifiche volte a valutare il livello di sicurezza implementato sulle infrastrutture e sulle applicazioni.

- monitoraggio delle segnalazioni: devono essere rilevate e valutate in modo continuativo le segnalazioni di potenziali tentativi di forzatura delle misure di sicurezza implementate. L'esito deve attivare un processo di miglioramento continuo delle misure in essere e della capacità di rispondere a tali tentativi.

5.11 Compliance

La tutela del patrimonio informativo deve essere conforme alle normative di Legge e alle disposizioni regolamentari in materia di sicurezza delle informazioni. Tale obiettivo si persegue indirizzando, per gli aspetti di seguito indicati, i relativi interventi:

- conformità ai requisiti di legge: deve essere assicurata, verificata e garantita nel tempo la conformità delle contromisure definite alla normativa di Legge e alle disposizioni regolamentari. Deve inoltre essere assicurato l'adempimento delle normative di legge in materia di sicurezza delle informazioni;

- conformità alle norme aziendali: devono essere previsti controlli per verificare la coerenza delle misure di sicurezza con le normative interne identificando le eventuali non conformità.

6. Verifica, Applicazione e Aggiornamento

È compito dell'Head of Infrastructure & Security:

- verificare che le disposizioni contenute nel presente documento siano rispettate;

- raccogliere osservazioni o segnalazioni sulle necessità di revisione delle disposizioni;

- proporre gli aggiornamenti alle disposizioni che valuta necessari.