POLITICA PER IL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Indice

1. Obiettivo del documento

In considerazione del ruolo centrale assunto dalle informazioni nel contesto aziendale, Esaote S.p.A (di seguito: "Esaote") ed EBIT S.r.l. (di seguito: "EBIT") hanno predisposto la presente Politica che detta le linee guida al fine di garantire un'adeguata protezione delle informazioni e del sistema informativo nel suo complesso, attraverso l'adozione di un approccio unico, consistente e standardizzato.

Il mancato perseguimento degli obiettivi di protezione del patrimonio informativo potrebbe, infatti, comportare per Esaote ed EBIT forti impatti sul business e sull'operatività aziendale, derivanti dai rischi cui il patrimonio informativo aziendale è esposto (es. perdite economiche, danni di immagine, perdita di competitività sul mercato, sanzioni relative al mancato rispetto delle normative vigenti, ecc.).

L'obiettivo del documento è quello di definire i principi e le indicazioni della Direzione per approcciare e gestire la sicurezza delle informazioni all'interno di Esaote, con riferimento al contesto delle informazioni aziendali, inclusi i dati personali, sia per l'ambito interno che esterno all'Organizzazione.

2. Campo di applicazione

La presente Politica si applica a tutte le risorse (sistemi tecnologici, procedure organizzative, attività, ecc.) coinvolte nella gestione delle informazioni.

Restano al di fuori dell'ambito di applicazione della presente Politica gli aspetti riguardanti la sicurezza sul luogo di lavoro, la tutela della salute delle persone, la tutela ambientale e, in generale, la protezione dei beni materiali ed immateriali non afferenti al patrimonio informativo di Esaote ed EBIT.

3. Criteri di gestione del documento

3.1. Monitoraggio e revisione

Il presente documento deve essere rivisto e, se necessario aggiornato, ogni volta che si verifichi un cambiamento importante che potrebbe influire sul contenuto dello stesso e, in ogni caso, almeno una volta all'anno.

3.2. Distribuzione della politica

La presente Politica è comunicata a tutti i dipendenti ed in via generale, a tutti coloro che, in virtù di un rapporto di lavoro subordinato, parasubordinato o in qualsiasi forma costituito, o di un rapporto di fornitura (dipendenti, collaboratori, fornitori, business partner, stagisti, personale somministrato ed altro), sia coinvolto nella gestione di componenti del sistema informativo e nel trattamento di informazioni di proprietà di Esaote ed EBIT.
Esaote ed EBIT riconoscono la formazione e l'informazione dei dipendenti come strumenti chiave per il riconoscimento e l'attuazione di questa Politica.

4. Normative e documenti di riferimento

La conformità ai requisiti di sicurezza definiti dalla normativa vigente, dagli Standard e dalle Best Practice di maggiore diffusione a livello internazionale, risulta imprescindibile nell'ambito del raggiungimento degli obiettivi individuati nella presente Politica.

4.1. Riferimenti esterni

Requisiti Cogenti:

- **Regolamento Europeo 2016/679 (GDPR):** Regolamento generale per la protezione dei dati personali.
- **Direttiva (UE) 2022/2555 (NIS2)**: Direttiva sulla sicurezza delle reti e dei sistemi informativi che aggiorna e amplia le misure previste dalla Direttiva NIS (2016/1148), imponendo obblighi di sicurezza più rigorosi per le imprese e le organizzazioni di settori critici per l'economia e la società.
- **D. Lgs. 231/2001:** il Decreto Legislativo 8 giugno 2001, n. 231 che introduce e disciplina la responsabilità "amministrativa" degli enti, nell'ipotesi di commissione, da parte di soggetti apicali o sottoposti, dei reati espressamente indicati nel Decreto medesimo, dai quali l'ente ha tratto un interesse o un vantaggio.
- **Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001 o Modello 231:** documento adottato dalla Società, ai sensi degli articoli 6 e 7 del D. Lgs. 231/2001, al fine di prevenire la realizzazione dei reati ivi indicati da parte del personale apicale o subordinato, così come descritto nello stesso Modello 231 e nei relativi allegati.

Standard e Best Practice:

- **ISO/IEC 27001:2022 (Tecnologie Informatiche – Tecniche di sicurezza - Sistemi di gestione della Sicurezza dell'Informazione - Requisiti):** Standard internazionale che definisce i requisiti per pianificare, attuare, operare, monitorare, riesaminare, mantenere e migliorare il Sistema di Gestione per la Sicurezza delle Informazioni delle Aziende.
- **ISO/IEC 27017:2021 (Tecniche di sicurezza – Codice di pratica per i controlli di sicurezza delle informazioni per i servizi cloud)**: Linee guida per l'implementazione dei controlli di sicurezza in ambienti cloud, con indicazioni per clienti e fornitori.
- **ISO/IEC 27018:2020 (Protezione dei dati personali nei servizi cloud pubblici)**: Standard internazionale per la tutela delle informazioni personali in ambienti cloud.
- **NIST CSF (National Institute of Standards and Technology - Cybersecurity Framework):** standard internazionale che fornisce alle organizzazioni una guida su come prevenire, rilevare e rispondere agli attacchi Cyber e gestire i relativi rischi.
- **UNI EN ISO 9001:2015 (Sistemi di gestione per la qualità – Requisiti):** Standard internazionale che definisce i requisiti per pianificare, attuare, operare, monitorare, riesaminare, mantenere e migliorare il Sistema di Gestione per la Qualità.

4.2. Riferimenti interni

- POL000031 Policy Lavoro Agile
- POL000016 Regolamento Informatico

- Codice Etico: documento, ufficialmente voluto e approvato dal vertice della Società, contenente i principi generali di comportamento - ovvero, raccomandazioni, obblighi e/o divieti - cui i Destinatari devono attenersi nell'esercizio della propria attività e la cui violazione può essere specificamente sanzionata

5. Responsabilità

Il perseguimento degli obiettivi aziendali di sicurezza è conseguito attraverso la definizione di un adeguato modello organizzativo per l'attribuzione di ruoli e responsabilità.
Una governance efficace della Sicurezza delle Informazioni non può prescindere dalla puntuale definizione dei ruoli e delle responsabilità assunte in tale ambito.

Esaote ed EBIT attribuiscono puntualmente ed in modo non ambiguo i ruoli e le responsabilità in materia di Sicurezza delle Informazioni al proprio personale. L'accountability è condizione necessaria per il raggiungimento ed il mantenimento nell'ambito di Esaote ed EBIT degli obiettivi di sicurezza definiti. A tale scopo, Esaote ed EBIT provvedono a verificare nel continuo che l'operato del personale sia conforme con quanto definito.
In ogni caso, per garantire l'applicazione della presente Politica ed il raggiungimento degli obiettivi di sicurezza, tutto il personale è comunque coinvolto e responsabilizzato nell'efficace realizzazione del Sistema di Gestione della Sicurezza delle Informazioni.

Tutte le attività devono essere svolte nel rispetto dei principi di attribuzione di responsabilità e di rappresentanza, di segregazione dei ruoli e dei compiti, di lealtà, correttezza, trasparenza e tracciabilità degli atti.

6. Definizioni

- **Accountability**: L'assegnazione della responsabilità di un'attività o processo aziendale, con il conseguente compito di rispondere delle operazioni svolte e dei risultati conseguiti, a una determinata figura aziendale; in ambito tecnico, si intende la garanzia di poter attribuire ciascuna operazione a soggetti (utenti o applicazioni) univocamente identificabili;
- **Asset**: dati, personale, dispositivi, sistemi e strutture che consentono all'organizzazione di raggiungere gli scopi aziendali.
- **Autenticazione**: fornisce la garanzia che una caratteristica dichiarata di un'entità è corretta.
- **Best practice**: Raccolta organizzata di raccomandazioni derivanti dalla selezione delle pratiche migliori per l'erogazione dei servizi.
- **Dati personali / Informazioni di identificazione personale (PII)**: qualsiasi informazione relativa a una persona fisica identificata o identificabile ("interessato"), o che possa essere utilizzata per stabilire un collegamento con tale persona, direttamente o indirettamente; una persona è considerata identificabile quando può essere identificata, direttamente o indirettamente, mediante riferimento a identificatori quali un nome, un numero di identificazione, dati relativi alla posizione, un identificatore online, oppure a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale.
- **Information & Cyber Security**: l'Information & Cyber Security garantisce la protezione delle informazioni archiviate, elaborate e trasmesse, in tutte le forme, preservando le seguenti caratteristiche:
    - **Riservatezza**: garantire che le informazioni siano disponibili solo per gli utenti autorizzati
    - **Integrità**: garantire che le informazioni siano protette da modifiche non autorizzate per garantirne l'affidabilità e la correttezza

  - **Disponibilità**: garantire che le informazioni siano disponibili quando e dove sono necessarie
- **Informazione**: conoscenza o insieme di dati che hanno valore per un individuo o un'organizzazione. (ISO/IEC 27000). Possono esistere in molte forme:
  - Stampate o scritte su supporto cartaceo
  - Memorizzate elettronicamente
  - Trasmesse via posta o mezzi elettronici
  - Registrate su video
  - Trasmesse verbalmente.
- **Minacce alla sicurezza**: potenziale causa di un incidente indesiderato, che potrebbe danneggiare un sistema o un'organizzazione.
- **Misure di sicurezza**: salvaguardie o contromisure prescritte per un sistema informativo o un'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità del sistema e delle sue informazioni.
- **Modifiche al sistema informativo**: l'aggiunta, la modifica o la rimozione di qualsiasi cosa che possa influenzare il sistema informativo.
- **Outsourcing**: Affidamento a società esterne della gestione di funzioni/servizi. Può riguardare i sistemi informatici (gestione sistemi elaborativi e reti, help desk, fornitura apparati), le infrastrutture (manutenzione impianti, sorveglianza), la formazione, ecc.
- **Privilegio minimo (Least Privilege)**: Il principio che stabilisce che a ciascun utente o amministratore di sistema siano assegnate le abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati.
- **Rischio informatico**: Il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato, in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (Information and Communication Technology – ICT).
- **Risorse informatiche**: tutte le risorse ICT e fattori abilitanti che supportano il sistema informativo, ad esempio sistemi informatici, di rete, di comunicazione, applicativi e di telecomunicazione, infrastruttura, hardware, software, dati, database, personale, procedure, strutture fisiche, fornitori basati su cloud, fornitori di Software as a Service (SaaS) e qualsiasi materiale e servizio correlato.
- **Security & Privacy by Design**: i principi di privacy e sicurezza sono integrati nelle attività di elaborazione e nelle pratiche commerciali, dalla fase di progettazione fino all'intero ciclo di vita (ex art. 25 GDPR).
- **Segregazione dei compiti (Segregation of Duties)**: il principio che stabilisce che l'esecuzione di operazioni di particolare criticità sia svolta attraverso la cooperazione di più utenti o amministratori di sistema con responsabilità formalmente ripartite;
- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)**: il complesso di sistemi di processo, documenti, tecnologie e persone che aiutano un'azienda a gestire, monitorare, controllare e migliorare la Sicurezza delle Informazioni.
- **Sistema informativo**: insieme di applicazioni, servizi, risorse di tecnologia dell'informazione o altri componenti per la gestione delle informazioni.
- **Vulnerabilità**: condizione che consente il verificarsi di una minaccia.

7. Principi generali di Sicurezza delle Informazioni

Esaote ed EBIT hanno definito i seguenti principi generali di sicurezza da adottare nell'ambito di tutti i processi e delle attività svolte dal personale interno ed esterno. Ciò costituisce un quadro di riferimento per ottenere un adeguato livello di protezione del patrimonio informativo aziendale, mediante il continuo miglioramento dei processi organizzativi e la ricerca di soluzioni tecnologiche innovative in relazione alle evoluzioni della tecnologia, delle minacce e degli strumenti di difesa.

7.1. Security by Design e by Default

Le funzioni aziendali, coinvolte nelle attività di progettazione dei servizi in ambito, devono considerare la Sicurezza delle Informazioni quale contesto essenziale per la loro gestione, dal punto di vista di Riservatezza, Integrità e Disponibilità delle informazioni. Nella gestione delle informazioni, l'Organizzazione si ispira ai seguenti principi chiave:

- **Security by Design:** l'Organizzazione deve prevedere, per ogni iniziativa che sottende la gestione di informazioni, adeguate misure tecniche ed organizzative volte a garantire la sicurezza di tali informazioni, a partire dalle fasi iniziali della progettazione e durante tutto il ciclo di vita dell'iniziativa stessa.

- **Security by Default:** l'Organizzazione deve applicare ai sistemi di elaborazione delle informazioni misure tecniche ed organizzative adeguate, in modo che sia garantito per impostazione predefinita il livello più alto possibile di sicurezza.

7.2. Privacy by Design e by Default

Esaote ed EBIT considerano la tutela della privacy un diritto fondamentale degli interessati. Nella gestione del dato personale, l'Organizzazione si ispira ai seguenti principi chiave:

- **Privacy by Design:** il principio prevede che in funzione dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso, siano in essere misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare e tutelare i diritti degli interessati.

- **Privacy by Default:** il principio prevede che siano messe in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

7.3. Need to know

La Società definisce le logiche di accesso ai dati e alle informazioni, caratterizzanti il patrimonio informativo, nel rispetto del principio del "privilegio minimo", ovvero in relazione alla loro criticità intrinseca e in funzione della pertinenza del ruolo ricoperto dal richiedente.

7.4. Segregazione dei compiti

Esaote ed EBIT implementano apposite misure organizzative, procedurali e tecniche affinché le responsabilità siano definite e debitamente distribuite evitando sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto (persona fisica o giuridica, unità organizzativa, ruolo o funzione aziendale).

8. Sistema di Gestione per la Sicurezza delle Informazioni

Per dare attuazione ai principi di sicurezza contenuti nella presente politica, Esaote ed EBIT hanno definito e implementato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) costituito da principi, regole, requisiti, metodologie, controlli e misure di sicurezza. Esso ha lo scopo di preservare la Sicurezza delle Informazioni e dei beni aziendali e di garantire per ciascuna risorsa informatica:

- protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e responsabilità, appropriata e coerente lungo l'intero ciclo di vita;
- adeguati criteri, modalità di gestione ed utilizzo conformi alle norme di legge e a regolamenti interni ed esterni;
- riduzione dei rischi IT mediante adeguate misure di prevenzione e di mitigazione dei danni degli incidenti, in linea con la propensione al rischio informatico definito a livello aziendale.

Dal punto di vista strategico, un SGSI efficiente consente inoltre di sfruttare le opportunità offerte dalla tecnologia, migliorando prodotti e servizi offerti alla clientela e riducendone i costi.

La gestione della Sicurezza delle Informazioni è finalizzata non solo all'incremento dell'efficacia di processi e controlli, ma anche alla loro maturità, attraverso la produzione di informazioni documentate, cartacee e digitalizzate, di politiche, procedure, processi e registrazioni.

La Sicurezza delle Informazioni è garantita attraverso l'impegno della Direzione ad allocare le risorse, umane e finanziarie, necessarie a garantirne il continuo accrescimento di competenze e consapevolezza in termini di sicurezza delle informazioni.

La Sicurezza delle Informazioni è costantemente monitorata attraverso opportuni strumenti di monitoraggio e controllo volti a valutarne le prestazioni in termini di efficacia ed efficienza. Gli strumenti sono volti anche a identificare le aree di debolezza al fine di comprenderne le cause e poter intervenire con opportune azioni correttive finalizzate al miglioramento continuo.

8.1. Strategia di sicurezza

La strategia per la Sicurezza delle Informazioni della Società si articola nei seguenti punti:

- raggiungimento degli obiettivi di sicurezza in tutti gli ambiti tramite misure ed interventi omogenei e coerenti;
- utilizzo delle valutazioni del rischio per stabilire l'intensità e l'efficacia dei controlli di sicurezza;

- attribuzione di priorità ai controlli di sicurezza che hanno come scopo la prevenzione delle minacce, rispetto a quelli con finalità di mitigazione degli impatti derivanti dagli incidenti;
- distribuzione delle misure di sicurezza su diversi livelli, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva ("difesa in profondità");
- garanzia che l'implementazione di ogni controllo di sicurezza includa le modalità ed i meccanismi adeguati a verificarne l'efficacia e la corretta attuazione nel tempo.

Il perseguimento degli obiettivi aziendali di sicurezza è conseguito attraverso la definizione, l'implementazione e l'aggiornamento periodico di processi facenti parte del Sistema di Gestione per la Sicurezza delle Informazioni.

8.2. **Gestione del rischio**

Questo approccio permette di valorizzare le informazioni, valutare le minacce e i loro impatti sulle informazioni e identificare le misure di sicurezza tecniche-organizzative (o controlli) adeguate finalizzate a proteggere le informazioni, minimizzando il rischio in maniera efficace ed efficiente, attraverso una pianificazione strategica strutturata.

Il Processo di Gestione del Rischio Informatico rappresenta lo strumento mediante il quale la Società assicura l'efficacia delle misure di sicurezza poste a protezione del sistema informativo. Tale processo consente, inoltre, la gradazione delle misure di mitigazione in funzione del profilo di rischio dell'asset IT definito dalle funzioni preposte della Società.

Il Processo di Gestione del Rischio interessa:

- Tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo (*Security by Design*);
- Le procedure in esercizio, per le quali non è stata svolta un'analisi del rischio in fase di sviluppo (ovvero realizzate antecedentemente all'entrata in vigore della presente Policy).

Esso viene eseguito con una periodicità adeguata alla tipologia degli asset IT, in presenza di situazioni che possono influenzare il complessivo livello di esposizione al rischio informatico del sistema informativo e comunque almeno annualmente sugli asset IT classificati come critici.

Tra le situazioni che possono richiedere una esecuzione straordinaria dell'analisi del rischio si evidenziano:

- Il verificarsi di gravi incidenti di sicurezza informatica;
- La rilevazione di carenze nei controlli di sicurezza;
- La diffusione di notizie su nuove vulnerabilità o minacce di sicurezza informatica.

8.3. **Integrazione della Sicurezza delle Informazioni nelle attività operative**

La Sicurezza delle Informazioni è implementata all'interno delle attività operative attraverso la definizione di opportune procedure. L'approccio agli interventi è basato sul concetto di rischio operativo legato a specifici ambiti di controllo per la sicurezza. Esaote ed EBIT definiscono le misure di sicurezza da adottare a tutela degli asset IT caratterizzanti il proprio patrimonio

informativo, tramite l'emanazione di politiche, procedure e linee guida in materia di Sicurezza delle Informazioni.

8.3.1. Comunicazione

La Sicurezza delle Informazioni è garantita attraverso adeguati canali di comunicazione, in funzione delle specifiche esigenze. Tali canali comprendono la pubblicazione di politiche e procedure di sicurezza, la condivisione di principi e requisiti all'interno di offerte e contratti e sui canali istituzionali di comunicazione (sito web, canali social, etc.).

8.3.2. Formazione e awareness (personale e sicurezza)

Il personale, sia esso dipendente che di terze parti, rappresenta un fattore critico per la sicurezza delle informazioni in quanto è spesso la componente più esposta a minacce esterne o interne.

Affinché possa essere garantito un livello adeguato di Information Security è necessario promuovere informazione, formazione, e accrescimento della consapevolezza delle risorse umane:

- Informazione, intesa come il complesso di attività dirette a fornire conoscenze utili alla identificazione e riduzione dei rischi per la gestione della Sicurezza delle Informazioni;
- Formazione, intesa come il processo educativo attraverso il quale trasferire a dipendenti e collaboratori e altri soggetti le conoscenze e le procedure utili all'acquisizione di competenze per lo svolgimento sicuro dei rispettivi compiti nella gestione delle informazioni (sviluppatori, tecnici ICT, amministrazione, gestione del personale, etc.);
- Consapevolezza, inteso come il complesso di attività dirette a sensibilizzare personale e collaboratori sui potenziali rischi di sicurezza associati a specifici comportamenti e fenomeni (social engineering, phishing, etc.).

In aggiunta a quanto sopra, nel contesto specifico della fornitura di servizi cloud ed in conformità alle linee guida ISO/IEC 27017, EBIT valuta regolarmente la necessità di prevedere sessioni formative specifiche in materia di sicurezza informatica nel contesto cloud.

8.3.3. Classificazione e gestione degli asset IT

Tutte le risorse materiali e immateriali caratterizzanti il patrimonio informativo della Società hanno per essa un valore strategico e, pertanto, devono essere adeguatamente protette.

La messa in sicurezza del patrimonio informativo ha inizio con l'identificazione degli asset IT e delle informazioni che lo caratterizzano, le quali devono essere classificate secondo metriche coerenti con la politica di classificazione delle informazioni definita dalla Società e che ne evidenzino la criticità in termini di sicurezza per facilitare la corretta implementazione di misure di protezione adeguate.

Le principali attività da eseguire per una corretta gestione degli asset IT aziendali sono le seguenti:

- Asset Inventory: costituire e mantenere aggiornato, nel corso del tempo, un inventario degli asset IT al fine di assegnare la responsabilità di tutela degli stessi e monitorarli per

l'intero ciclo di vita. Affinché sia garantito un corretto livello di protezione dei dati e delle informazioni, tutti gli asset IT correlati al sistema informativo aziendale, devono essere opportunamente tracciati, nel rispetto delle seguenti regole:

- ciascun asset deve essere assegnato ad un referente aziendale identificabile, che li classifichi in termini di confidenzialità, integrità e disponibilità e ne stabilisca i requisiti di sicurezza;
- le attività di tracciamento devono essere effettuate in maniera sistematica e per le diverse fasi del ciclo di vita degli asset;

- Classificazione degli asset: l'Organizzazione, con il supporto della funzione IT, deve definire una metodologia per la classificazione degli asset sulla base dei criteri di confidenzialità, integrità e disponibilità, al fine di identificare, con gli owner delle informazioni, il livello di criticità in termini di sicurezza e definire adeguate misure di protezione. Tale classificazione deve essere realizzata in coerenza con la policy di classificazione delle informazioni definita dalla Società e deve essere periodicamente aggiornata.

8.3.4.Sicurezza dei dispositivi aziendali

La riservatezza delle informazioni deve essere rispettata anche attraverso la scrupolosa osservanza delle disposizioni contenute nelle Politiche aziendali di Esaote ed EBIT e nel Codice Etico che le Società adottano per una corretta gestione degli strumenti elettronici dati in dotazione al Personale, delle banche dati organizzate da Esaote ed EBIT e per tutti gli ulteriori specifici adempimenti connessi.

La diffusione di nuove tecnologie informatiche espone Esaote ed EBIT e gli utenti a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di leggi, creando problemi alla sicurezza e all'immagine dell'azienda stessa. Pertanto, l'utilizzo di risorse informatiche digitali (device e software) deve ispirarsi ai principi di correttezza e diligenza. Gli strumenti informatici, in particolare, devono essere custoditi con cura, evitando ogni possibile forma di danneggiamento. Per ulteriori dettagli, si rimanda al documento "*POL000016 - Regolamento Informatico*".

La Società deve garantire l'adozione di adeguate misure di sicurezza per prevenire problemi di protezione causati dall'errata configurazione, gestione ed utilizzo delle postazioni di lavoro e dei dispositivi mobili quali PC portatili, Smartphone, tablet e memorie rimovibili. Al fine di garantire il raggiungimento di tali obiettivi, è necessario che siano definite e rispettate delle norme comportamentali per l'utilizzo dei dispositivi aziendali assegnati, nonché misure di sicurezza specifiche con particolare attenzione verso i dispositivi mobili (es. remote lock, remote wipe).

8.3.5.Cancellazione dei dati

La cancellazione sicura dei dati contenuti all'interno degli asset aziendali è assicurata mediante l'adozione di appositi tool e in generale secondo le modalità prescritte dai Clienti con apposite clausole contrattuali.
La distruzione dei documenti cartacei contenenti dati personali, il cui trattamento non trova più legittimazione, è assicurato tramite strumenti di tritatura documenti.

8.3.6. Gestione degli accessi logici

L'accesso alle informazioni e agli asset IT deve essere adeguatamente gestito al fine di garantirne il rispetto della confidenzialità e dell'integrità delle informazioni da essi gestite.
La gestione sicura degli accessi logici agli asset IT componenti il sistema informativo aziendale deve essere basata sulle seguenti regole:

- deve essere formalizzato un processo di approvazione e gestione delle autorizzazioni all'accesso;
- i profili di accesso devono essere definiti in modo da permettere all'utente di accedere alle informazioni strettamente necessarie per lo svolgimento dei compiti assegnati, nel rispetto del principio del "need to know" e del privilegio minimo;
- la gestione e il controllo deve riguardare l'intero ciclo di vita dei profili di accesso degli utenti (assegnazione, creazione, aggiornamento, disattivazione e revoca);
- deve essere verificato, in modo strutturato e scadenzato, la validità delle credenziali di accesso e dei profili di accesso conformemente alle norme vigenti e in relazione al ruolo aziendale assegnato all'utente;
- devono essere definiti meccanismi di protezione adeguati all'autenticazione del personale nel caso di accesso da remoto alla rete aziendale;
- devono essere implementati dei meccanismi di controllo e tracciatura degli accessi conformemente alle norme vigenti e alle politiche aziendali.

Nel contesto specifico della fornitura di servizi cloud, ed in conformità alle linee guida ISO/IEC 27017, EBIT definisce procedure per la creazione, modifica e revoca degli account dei clienti cloud, garantendo la protezione delle credenziali e la tracciabilità delle operazioni lungo l'intero ciclo di vita. L'accesso agli asset dei clienti da parte del personale di EBIT è consentito solo in base a procedure formalizzate, con autorizzazioni tracciate e limitate al principio del privilegio minimo. Ogni accesso è monitorato e soggetto a verifica periodica.

8.3.7. Crittografia

Al fine di proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni Esaote ed EBIT prevedono l'utilizzo di idonei controlli crittografici. Laddove ritenuto necessario, in riferimento all'analisi dei rischi cui sono esposti gli asset contenenti informazioni riservate, sono adottati metodi di crittografia.

La robustezza dell'algoritmo di crittografia deve essere selezionata in funzione della riservatezza dei dati, su qualsiasi supporto esse si trovino.
Nella scelta devono essere valutati i rischi di impossibilità di ispezione di dati cifrati e il livello di accuratezza necessario per la gestione delle chiavi crittografiche lungo il loro intero ciclo di vita e le puntuali modalità di generazione delle chiavi, da adottare in caso di danneggiamento o perdita delle chiavi di decifratura. Nel caso in cui tali attività siano affidate a provider esterni, deve essere valutata l'adeguatezza delle procedure adottate in questo ambito dal fornitore.

In generale per tutti i dati personali trattati è richiesta la valutazione circa l'adozione di controlli crittografici, in linea con le prescrizioni del GDPR. Inoltre, deve essere garantita la crittografia nella trasmissione dei dati su reti pubbliche attraverso l'uso del protocollo HTTPS per la comunicazione sicura.

Particolare attenzione deve essere prestata ai log degli Amministratori di Sistema e alle password associate ad utenze per l'accesso a sistemi aziendali critici dal momento che devono anch'essi essere adeguatamente protetti attraverso meccanismi di crittografia.

8.3.8. Gestione dei Cambiamenti

Esaote ed EBIT tengono in considerazione tutti gli aspetti di sicurezza nell'ambito della gestione dei cambiamenti degli asset IT. In particolare, si richiede di valutare gli impatti e i rischi connessi alle richieste di cambiamento inerenti alla modifica o allo sviluppo degli asset IT, identificando gli opportuni requisiti di sicurezza da adottare (Security by Design), oltre che di svolgere opportuni test di sicurezza (es. Vulnerability Assessment e Penetration Test) prima del rilascio in produzione dei suddetti cambiamenti.

Nel contesto specifico della fornitura di servizi cloud, ed in conformità alle linee guida ISO/IEC 27017, EBIT si impegna a comunicare tempestivamente ai clienti cloud eventuali modifiche rilevanti ai servizi che possano impattare la sicurezza o la disponibilità, fornendo indicazioni sui rischi e sulle misure di mitigazione adottate.

8.3.9. Sviluppo Sicuro del software

Esaote ed EBIT adottano metodologie e tecniche per lo sviluppo sicuro del software che consentano di prevenire eventuali problematiche di sicurezza nel software e, allo stesso tempo, costituiscano uno strumento utile per individuare possibili vulnerabilità presenti nel codice sorgente e le relative contromisure da applicare.

8.3.10. Gestione delle vulnerabilità

Esaote ed EBIT devono garantire l'aggiornamento continuo degli asset IT, hardware e software, della Società al fine di prevenire e correggere eventuali malfunzionamenti e di eliminare eventuali vulnerabilità di sicurezza presenti.

La Società deve garantire che le eventuali vulnerabilità tecniche presenti sugli asset IT devono essere opportunamente monitorate e gestite, mediante l'attuazione delle seguenti regole:

- attribuzione della specifica responsabilità di gestione e mantenimento degli asset IT in merito agli aspetti di vulnerabilità di sistema (patch management di sicurezza, hardening, ecc.);
- monitoraggio delle informazioni tecniche che periodicamente sono emesse dai soggetti preposti (vendor, centri istituzionali di sicurezza, ecc.);
- garanzia che le vulnerabilità tecniche rilevate siano analizzate e gestite, previa una loro valutazione e successiva adozione dei necessari interventi correttivi (es. opportune attività di patching);
- esecuzione di periodiche verifiche di sicurezza sugli asset IT gestiti (es. Vulnerability Assessment, Penetration Test, Security Audit) attraverso la predisposizione di un piano di verifica periodico che tenga conto della criticità degli asset IT, nonché di eventi occorsi nel periodo di riferimento (es. cambiamenti delle piattaforme tecnologiche, change rilevanti, incidenti gravi).

8.3.11. Gestione dei Backup

Specifiche Politiche di Backup devono essere definite a livello aziendale in funzione della criticità dei dati elaborati dagli asset IT, al fine di garantire gli aspetti di disponibilità dei dati e delle informazioni della Società mediante una serie di misure di salvataggio e ripristino periodico degli stessi.

Strutture di backup adeguate sono state previste al fine di garantire il recupero di tutte le informazioni e i software essenziali in seguito a un incidente, a un guasto o alla perdita dei supporti di memorizzazione. Pertanto, sono stati sviluppati e implementati piani per il backup delle informazioni, del software e dei sistemi dell'organizzazione.

I piani per il backup prevedono la produzione di registrazioni accurate e complete delle copie di backup e delle procedure di ripristino documentate. Esse riflettono i requisiti aziendali dell'organizzazione, i requisiti di sicurezza delle informazioni coinvolte e la criticità delle informazioni per il funzionamento continuo dell'organizzazione e nella frequenza dei backup.

I backup vengono custoditi in un luogo remoto e sicuro, a una distanza sufficiente per evitare i danni di un eventuale disastro nel sito principale, garantendo un livello adeguato di protezione fisica e ambientale, in linea con gli standard applicati al sito principale. Inoltre, mediante crittografia, viene garantita una protezione da rischi relativi alle informazioni la cui confidenzialità è importante.

I supporti di backup vengono testati regolarmente in modo da garantire che si possa fare affidamento su di essi in caso di emergenza. Inoltre, le misure di backup vengono testate regolarmente per garantire che soddisfino gli obiettivi dei piani di risposta agli incidenti e di continuità operativa, con relativo controllo delle procedure di ripristino.
Per i servizi cloud vengono effettuate copie di backup delle informazioni, delle applicazioni e dei sistemi dell'organizzazione nell'ambiente del servizio cloud.

8.3.12. Network Security

Deve essere garantita la protezione perimetrale dei dati e delle informazioni da accessi esterni ed interni non autorizzati, mediante la definizione di opportune misure di sicurezza perimetrale (firewall, IDS, etc.) della rete aziendale. Tali misure di protezione dovranno essere periodicamente testate al fine di verificarne il corretto funzionamento ed il loro mantenimento nel tempo.
In particolare:

- l'accesso agli apparati di rete (firewall, router, ecc.) deve essere consentito solo al personale tecnico competente ed autorizzato per le necessarie attività di gestione ed amministrazione;
- deve essere prevista la segmentazione delle reti di telecomunicazione, con controllo dei flussi scambiati;
- devono essere previsti adeguati meccanismi per la protezione della riservatezza delle informazioni in transito sulla rete aziendale (fissa e wireless) e attraverso reti pubbliche oppure di terze parti, basati su algoritmi e protocolli sicuri (p.e. cifratura delle comunicazioni).

Nel contesto della fornitura di servizi cloud, EBIT si impegna a garantire la sicurezza delle informazioni mediante la definizione di responsabilità chiare tra la Società e i fornitori di servizi cloud selezionati. Nel rispetto del modello di responsabilità condivisa e delle clausole contrattuali definite con i fornitori di servizi cloud selezionati, i seguenti controlli e misure di sicurezza, conformi alle linee guida ISO/IEC 27017, vengono concordati e regolamentati con i fornitori stessi; la loro effettiva adozione e implementazione è demandata ai fornitori secondo gli obblighi tecnici e organizzativi previsti dagli accordi di servizio (es. contratto, SLA e allegati di sicurezza):

- isolamento logico e fisico delle risorse dei clienti, mediante controlli di segregazione e configurazioni sicure per ambienti multi-tenant, al fine di prevenire commistioni di dati e accessi non autorizzati tra tenant;
- protezione degli ambienti virtualizzati, includendo hardening delle piattaforme, gestione e remediation delle vulnerabilità e monitoraggio delle configurazioni, al fine di prevenire attacchi che possano compromettere l'isolamento tra clienti;
- verifica e mantenimento della coerenza tra le configurazioni delle reti virtuali e le controparti fisiche/sottostanti, al fine di prevenire vulnerabilità di rete e garantire la sicurezza dei servizi cloud.

8.3.13. Monitoring

Devono essere predisposte adeguate misure di monitoraggio degli asset IT (produzione di log), nel rispetto delle normative sulla privacy ed il trattamento dei dati, mediante il tracciamento degli accessi e delle attività effettuate dagli utenti e di tutti gli eventi considerati significativi per il monitoraggio della sicurezza degli asset IT (es. Access log, Activity log, System log, Security log).

8.3.14. Gestione delle terze parti

La gestione della sicurezza del sistema informativo richiede che sia garantito un adeguato livello di sicurezza delle risorse accedute e utilizzate da soggetti terzi (fornitori, consulenti, partner).

In tale ottica, la Società si impegna a:

- identificare i rischi connessi all'attività di outsourcing e a definire adeguate misure di sicurezza (Rischio delle Terze Parti);
- prevedere l'inserimento di opportuni impegni/obblighi contrattuali a carico delle terze parti.

Nel contesto della fornitura di servizi cloud, EBIT estende i principi di sicurezza definiti nel presente documento anche ai fornitori di servizi cloud e SaaS (Software as a Service), assicurandosi che essi operino in conformità alle linee guida ISO/IEC 27017 per garantire la sicurezza delle informazioni e la corretta gestione delle responsabilità contrattuali.

8.3.15. Gestione della sicurezza fisica

La protezione del patrimonio informativo della Società richiede che venga posta particolare attenzione agli aspetti di sicurezza fisica, al fine di prevenire l'accesso non autorizzato ai locali

aziendali ed un eventuale rischio di sottrazione, manomissione e/o danneggiamento degli asset.
Al fine di garantire la sicurezza fisica, la Società deve individuare adeguate misure tecniche, organizzative e procedurali da adottare relativamente alla:

- gestione delle aree fisiche (intese come sedi, aree e locali): adottare adeguate misure di sicurezza e di protezione in funzione della criticità delle risorse informative trattate e conservate;
- gestione sicura degli asset: posizionare e proteggere gli asset in funzione del livello di classificazione delle informazioni;
- gestione degli accessi: garantire che l'accesso ai locali sia controllato e consentito esclusivamente al personale previamente identificato ed autorizzato.

L'accesso ai locali aziendali è consentito solo a persone autorizzate. L'accesso dei dipendenti agli uffici è autorizzato e subordinato all'utilizzo del badge sul sistema automatico di controllo. Tutti i visitatori devono essere identificati da parte del personale Esaote ed EBIT prima di consentirne l'accesso. Chiunque riceva un visitatore si assume la responsabilità sul suo operato e la sua condotta. I visitatori devono essere sempre accompagnati, in ingresso ed in uscita dalla sede. All'ingresso è depositato un Registro per tracciare gli ingressi dei visitatori.
Le aree di consegna, carico/scarico merci e corrispondenza sono situate in aree sicure, che ne garantisce il controllo e la protezione degli accessi da persone non autorizzate.

8.3.16. Gestione degli incidenti inerenti alla Sicurezza delle Informazioni

La gestione degli incidenti di sicurezza informatica ha l'obiettivo di minimizzare l'impatto di eventi avversi e di garantire il tempestivo ripristino del regolare funzionamento degli asset IT coinvolti.

Pertanto, la Società adotta un processo di gestione degli incidenti di sicurezza, conforme alle normative vigenti (es. GDPR) ed alle best practice di settore, volto alla mitigazione ed al contrasto tempestivo di qualsiasi evento che possa compromettere la riservatezza, l'integrità o la disponibilità dei dati e dei sistemi aziendali.

8.3.17. Gestione degli aspetti di Business Continuity

La Società deve garantire adeguati livelli di continuità operativa, a fronte di un eventuale evento imprevisto, di qualsiasi natura, che possa comportare blocchi nell'erogazione dei servizi.
Pertanto, anche al fine di salvaguardare gli interessi dei suoi stakeholder, la Società adotta un processo strutturato per la gestione della Business Continuity, in grado di garantire il ripristino tempestivo delle funzionalità dei servizi critici e di mitigare i principali rischi operativi ad essi connessi.

Il processo, in particolare, deve prevedere:

- l'elaborazione di piani di continuità operativa basati sulle reali esigenze del business aziendale nonché sull'adeguata analisi degli impatti relativi al fermo dei principali processi della Società;
- la definizione e svolgimento di esercitazioni periodiche che permettano di convalidare il funzionamento delle soluzioni di Business Continuity identificate;

- la revisione periodica e l'aggiornamento tempestivo dei piani di continuità operativa in funzione delle nuove minacce alla continuità dei servizi della Società;
- la richiesta di garanzie in termini di Business Continuity, all'inizio di ogni progetto e in ciascun contratto, ai "fornitori di servizi considerati critici", al fine di favorire la prevenzione sui rischi dovuti ad attività esternalizzate.

È, inoltre, molto importante tenere presente che a livello generale, ai fini di garantire dei livelli più alti in termini di continuità e di sicurezza delle informazioni in caso di interruzione e per una maggior resilienza complessiva, per tutti i servizi in ambito deve sempre essere previsto l'utilizzo di:

- Dispositivi portatili dotati di batteria interna (Tablet, Smartphone, Laptop, ecc.) e gruppi di continuità per tutti gli altri sistemi (Desktop, Server e infrastruttura) al fine di consentire di poter mettere in sicurezza le informazioni a fronte di una interruzione di energia elettrica e proseguire con la propria attività minimizzando la perdita di dati e salvaguardando le informazioni.
- Sistemi per la ridondanza dei dati, dell'hardware, del software e delle componenti infrastrutturali in modo da minimizzare i periodi di disruption su tutti i servi in ambito e le loro componenti.
- Sistemi in grado di prevenire, intercettare ed eliminare eventuale malware, spyware e virus su tutti i propri sistemi.
- Cablaggi e linee di trasmissione dati opportunamente protetti in modo che non siano esposti ad attività finalizzate alla frode o al furto, quali intercettazione e manomissione da parte di persone non autorizzate o eventuale danneggiamento.
  Tecniche e meccanismi di segregazione e di protezione degli accessi per i dati e le informazioni, in modo che questi non siano disponibili a persone non autorizzate in caso di interruzione di uno o più sistemi che ne abbiano accesso per il loro funzionamento.

8.4. **Conformità**

La presente Politica deve essere implementata da Esaote ed EBIT in accordo con le normative applicabili. La Società non intende, infatti, omettere o porsi in contrasto con leggi, norme nazionali e internazionali applicabili, nonché regolamenti definiti specificatamente per l'ambito in cui essa opera.

8.4.1. Protezione dei dati personali

Il Regolamento Generale per la Protezione dei dati Personali (EU) 679/2016 (GDPR) è, dal 25 Maggio 2018, il principale testo normativo di riferimento sulla protezione dei dati personali nell'Unione Europea e rafforza le attuali disposizioni normative (sia nella sostanza che nel contesto), estendendo gli obblighi in materia di sicurezza direttamente anche ai Responsabili del trattamento.

Uno dei principali obblighi per tutte le imprese, e quindi per Esaote ed EBIT, sia che agiscano come Titolare, sia come Responsabile del trattamento, è finalizzato alla sicurezza delle operazioni di trattamento dei dati personali.

La sicurezza nel trattamento dei dati personali, disciplinata in via primaria dall'articolo 32 del GDPR, afferma che il Titolare del trattamento e il Responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato ai rischi connessi ai diritti e alle libertà delle persone fisiche, verificando nel continuo l'efficacia delle misure tecniche e organizzative, al fine di garantire la sicurezza del trattamento.

In linea con quanto stabilito dal GDPR, Esaote ed EBIT hanno come obiettivo primario la sicurezza dei dati personali gestiti, con particolare attenzione alla riservatezza, integrità e disponibilità dei dati attraverso un approccio basato sui rischi (risk-based approach) connessi ai diritti e la libertà degli interessati. Per tale ragione, Esaote ed EBIT adottano un approccio per la protezione dei dati personali che prevede la piena conformità agli adempimenti e ai principi del GDPR in ogni specifico contesto operativo e in ogni processo aziendale dove i dati personali sono trattati.

In aggiunta a quanto sopra, nel contesto specifico della fornitura di servizi cloud, EBIT si impegna a garantire la conformità alle linee guida ISO/IEC 27018 in materia di protezione delle informazioni personali identificabili (PII) trattate nei servizi di cloud pubblico, in linea con le disposizioni normative applicabili in materia di protezione dei dati.

8.4.2. Protezione della Proprietà Intellettuale

La conoscenza sviluppata da Esaote ed EBIT costituisce una risorsa fondamentale da proteggere. I destinatari della presente Policy, anche dopo la cessazione del rapporto di lavoro, non dovranno divulgare a terzi alcuna informazione riguardante l'attività tecnica, tecnologica e commerciale del Gruppo, né alcuna informazione non pubblica riguardante la Società e le sue controparti commerciali (clienti, fornitori, partner, ecc.).

L'unica eccezione è rappresentata dai casi in cui tale divulgazione sia richiesta dalla legge o da altri requisiti normativi, oppure sia espressamente prevista da specifici accordi contrattuali; in questi casi, è necessario informare le funzioni aziendali competenti affinché forniscano una specifica autorizzazione.

In particolare, tutte le idee, i modelli e le altre forme di proprietà intellettuale sviluppate durante l'attività lavorativa devono essere protette e trattate con la necessaria discrezione.

Il Gruppo Esaote si impegna a non realizzare alcun progetto e/o iniziativa che possa comportare una violazione dei diritti di proprietà intellettuale di terzi.

9. Provvedimenti disciplinari

Qualsiasi violazione della presente Politica, o di altre Politiche pertinenti, deve essere tempestivamente e adeguatamente segnalata a Responsabile SGSI.

La violazione delle regole contenute in questo documento potrà comportare l'adozione di provvedimenti disciplinari secondo quanto previsto dal vigente contratto collettivo e in relazione alla portata e alla gravità dell'infrazione commessa.

Esaote ed EBIT, fermo restando l'adozione di provvedimenti disciplinari ritenuti opportuni, si riservano la facoltà di rivalersi nei confronti di coloro che non osservino le disposizioni contenute nel presente documento, per qualsiasi costo che dovesse essere sostenuto, così come per qualsiasi somma che Esaote ed EBIT fossero tenute a corrispondere a terzi a titolo di sanzione amministrativa e/o risarcimento danni in conseguenza della violazione commessa.

La violazione delle regole di questo documento può essere qualificata come inadempimento agli obblighi contrattuali in capo al lavoratore Dipendente. In caso di effettiva violazione degli obblighi contrattuali in capo al Dipendente, Esaote ed EBIT chiedono al lavoratore di cessare immediatamente le sue azioni. Esaote ed EBIT hanno facoltà di intraprendere le dovute azioni disciplinari e le altre misure in conformità alle disposizioni dei regolamenti interni dell'entità, nonché la normativa vigente.

10. Archivio

La copia del presente documento è archiviata, con l'evidenza delle firme di redazione, controllo ed approvazione all'interno del sistema documentale aziendale.