POLITICA PER LA QUALITA' E LA SICUREZZA DELLE INFORMAZIONI

Rev. 3.2

13/09/2021

1 Introduzione

Enigma Defense identifica la propria *mission* nel portare sul mercato soluzioni innovative, sicure, di alto profilo ingegneristico, con competenze certificate su temi riguardanti sicurezza, pianificazione strategica e corporate governance, continuità del business, sviluppo e realizzazione di architetture complesse.

Allo scopo di perseguire la propria *mission*, Enigma Defense ha deciso di adottare due sistemi di gestione - il Sistema di Gestione per la Qualità (SGQ) e il Sistema di Gestione per la Sicurezza delle informazioni (ISMS) - conformi ai requisiti delle norme UNI EN ISO 9001:2015 e ISO/IEC 27001:2017 ed integrati nel Sistema di Gestione Integrato (da qui SGI o anche semplicemente il Sistema) con l'intento di perseguire il miglioramento continuo e la sicurezza relativamente ai servizi forniti e le soluzioni offerte.

È stata definita una Politica per la qualità e la sicurezza delle informazioni (il presente documento, da qui anche riferito semplicemente come Politica) che rappresenta il quadro di riferimento degli obiettivi di qualità e sicurezza delle informazioni che, coerentemente con la *mission* aziendale, l'Azienda deve perseguire. Tale politica è sostenuta da specifiche procedure che guidano l'attuazione operativa degli obiettivi di controllo della qualità e della sicurezza delle informazioni e che sono state realizzate per rispondere e trattare puntuali esigenze e/o argomenti.

1.1 Ente Emittente

La presente Politica è definita, validata, emessa e diffusa dalla Direzione.

La Politica è stata definita assicurando che sia:

- appropriata alla mission dell'Azienda e ai suoi indirizzi strategici;
- adeguata rispetto alle esigenze dei Clienti e di tutte le parti interessate nel rispetto e conformità della normativa cogente e volontaria ed in particolare alle norme di riferimento;
- esplicativa degli obiettivi di qualità e sicurezza che ci si prefigge;
- garante dell'impegno al soddisfacimento dei requisiti di qualità e sicurezza delle informazioni applicabili nonché il miglioramento continuo del SGI attraverso l'attuazione dei piani di miglioramento.

La Politica è opportunamente comunicata e divulgata a tutte le parti interessate che a vario titolo influenzano il Sistema. In particolare, la–Enigma Defense si impegna affinché la presente Politica sia utilizzata come riferimento nello svolgimento delle proprie mansioni da tutto il personale coinvolto e sia conosciuta, condivisa ed applicata a tutti i livelli della stessa.

Per garantire la diffusione a tutti i livelli della Politica la Direzione, attraverso il RSGI, si attiva affinché siano create occasioni di crescita professionale ed attività informative e formative al fine di rendere consapevole ogni lavoratore dell'importanza del proprio comportamento.

1.2 Finalità

La presente Politica descrive i principi generali che ispirano la Enigma Defense nella definizione e gestione degli aspetti di qualità e sicurezza delle informazioni in ogni loro forma e/o declinazione, conformemente alle disposizioni della Direzione Aziendale, e a quanto richiesto dalle norme di riferimento. Come citato, la Politica per la Qualità e la Sicurezza delle Informazioni rappresenta il quadro di riferimento degli obiettivi di qualità e sicurezza delle informazioni che, coerentemente con la mission aziendale, l'Azienda deve perseguire.

1.3 Conformità

La conformità alla Politica è obbligatoria per tutte le figure professionali coinvolte nel SGI e ivi operanti a qualsiasi titolo, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale.

Ogni violazione ai principi espressi dal presente documento si connota come violazione ai principi della qualità e della sicurezza delle informazioni e deve essere opportunamente valutata da parte della Direzione, la quale, se del caso, intraprende tutte le azioni necessarie atte a minimizzare la situazione di rischio venutasi a creare, oltre che definire le misure idonee a prevenire future simili circostanze.

1.4 Gestione delle modifiche e deroghe

La presente Politica viene riesaminata dalla Direzione e dal RSGI almeno una volta l'anno in occasione del Riesame di Direzione.

Ogni richiesta di deroga alla Politica deve esprimere i motivi e le necessità per cui è presentata ed i rischi ad essa associati. La richiesta deve essere sottoposta al Responsabile del Sistema Integrato e approvata dalla Direzione.

2 Principi generali

La Direzione sostiene attivamente l'adozione del SGI tramite un chiaro indirizzo, un impegno evidente, incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni. L'impegno della Direzione si attua, tra l'altro, tramite i seguenti principi generali:

- la garanzia che siano identificati tutti gli obiettivi relativi al SGI in uso coerentemente con i requisiti di sicurezza aziendali;
- la disponibilità di risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGI;
- il controllo che il Sistema sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- l'approvazione e il sostenimento di tutte le iniziative volte al miglioramento del sistema;
- l'attivazione di programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni, della qualità dei servizi IT e della qualità in generale, attraverso la corretta comunicazione e divulgazione di politiche e procedure oltre che l'attivazione di programmi di formazione e informazione;
- la verifica periodica e regolare (o in concomitanza di cambiamenti significativi) dell'efficacia e dell'efficienza del Sistema, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della Politica in risposta ai cambiamenti del contesto esterno, dell'ambiente aziendale, del business, delle condizioni legali.

3 Principi e obiettivi per la Qualità

Enigma Defense considera il Sistema di Gestione della Qualità assolutamente strategico, fattore critico di successo del business aziendale, nonché fattore abilitante per la competitività e qualificazione sul mercato. In tal senso, il presente documento rappresenta l'impegno assunto dalla Direzione della Enigma Defense per la definizione, realizzazione, mantenimento e miglioramento continuo del SGI in linea con la norma UNI EN ISO 9001:2015 e con la normativa cogente e volontaria.

Quanto segue costituisce il principale riferimento – in termini di principi ed obiettivi per la qualità - cui deve attenersi tutto il personale della Enigma Defense coinvolto all'interno dell'ambito di applicazione del SGI.

3.1 Principi di riferimento

Principio fondamentale per la qualità è il perseguimento della massima soddisfazione del Cliente nel rispetto di tutte le sue aspettative ed esigenze, ottenuta tramite l'erogazione di servizi di alto livello qualitativo, in un'ottica di miglioramento continuo dei servizi offerti e delle performance aziendali.

A tal fine, l'Organizzazione si impegna a garantire:

- Il miglioramento delle modalità di gestione dei processi per il conseguimento di risultati qualitativamente e quantitativamente sempre migliori, tramite la definizione di specifici indicatori di misura dell'efficienza dei processi;
- L'operato aziendale in termini di contenimento dei costi e di efficienza interna, al fine di mantenere l'equilibrio economico della gestione;
- Il rispetto costante della legislazione cogente e volontaria applicabile;
- L'analisi delle esigenze dei Clienti in fase di progettazione dei servizi ed il controllo, attraverso un monitoraggio continuo ed efficace, del raggiungimento delle loro aspettative;
- Lo sviluppo di servizi il più possibile efficienti ed affidabili, che permettano la riduzione dei disservizi, dei reclami e dei conseguenti costi;
- La ricerca del fattivo contributo di tutte le parti interessate per migliorare le performance aziendali;
- La ricerca dell'ottimizzazione dei processi aziendali al fine di raggiungere il migliore livello possibile di efficacia ed efficienza;
- Il mantenimento della certificazione del proprio Sistema di Gestione Qualità in relazione alle norme UNI EN ISO 9001:2015;
- Il miglioramento del proprio Sistema di Gestione Qualità garantendone la costante uniformità alle correnti norme certificabili;
- Il mantenimento di un ruolo proattivo del RSGI per la promozione del miglioramento continuo nelle materie interessate dal SGI;
- L'impostazione delle fasi di pianificazione, controllo, monitoraggio e riesame per garantire che la politica sia rispettata, in modo da assicurare l'efficacia del SGI;
- Il periodico riesame della Politica e l'applicazione del SGI per valutarne la correttezza e l'efficacia, nell'ottica del miglioramento continuo;
- L'esecuzione di verifiche, ispezioni e audit atti a identificare e a prevenire eventuali situazioni di non conformità con i requisiti del SGI e la promozione di azioni correttive e preventive;
- La valorizzazione di tutte le risorse professionali tramite investimenti costanti in aggiornamento professionale, certificazione delle competenze e trasversalità delle conoscenze;
- Il coinvolgimento e la partecipazione di tutto il personale per la piena condivisione della politica e degli obiettivi aziendali;
- La responsabilizzazione di tutto il personale, al fine di renderlo consapevole dei propri obblighi;

- Che tutto il personale riceva adeguata informazione e formazione sui requisiti del Sistema di Gestione Qualità e ne comprenda le implicazioni per quanto riguarda il proprio ruolo nell'azienda e il proprio comportamento nel lavoro;
- Che i consulenti esterni che collaborano con l'azienda operino nel rispetto dei criteri stabiliti dalla Enigma Defense.

3.2 Obiettivi per la Qualità

Nel quadro dei principi generali enunciati, Enigma Defense si pone gli Obiettivi per la Qualità descritti di seguito al fine di raggiungere un miglioramento delle prestazioni aziendali. Tali obiettivi devono essere misurabili in modo da permettere la verifica del loro raggiungimento in sede di Riesame, e possono essere sintetizzati come segue:

- Per la soddisfazione del cliente:
  - Rispetto dei requisiti specificati e dei programmi (misurato dal numero di Non Conformità riferibili all'esecuzione);
  - Miglioramento dell'indice di soddisfazione degli Utenti e parti interessate (misura soddisfazione).
- Per il rispetto delle norme vigenti:
  - Rispetto della normativa cogente e volontaria applicabile (obiettivo permanente: zero Non Conformità riferibili all'aspetto normativo).
- Per la prevenzione dei problemi ed il miglioramento dei processi:
  - Miglioramento del grado di applicazione e consapevolezza del Sistema di Gestione (applicazione di adeguate azioni correttive/preventive per tutte le Non Conformità riscontrate);
  - Miglioramento continuo del rapporto con il Cliente (Nessun reclamo relativo all'erogazione dei prodotti/servizi);
  - Ottimizzazione degli indici di efficacia dei processi individuati nelle schede di processo (Confronto con gli indici del Riesame precedente).
- Per il corretto funzionamento del Sistema:
  - Ottimizzazione del rapporto costi/benefici relativamente ai servizi/prodotti offerti (verifica del rispetto degli effettivi tempi e costi di fornitura del servizio rispetto a quelli previsti);
  - Rispetto della pianificazione delle Verifiche Ispettive Interne per un costante monitoraggio delle attività.

Tali obiettivi vengono quantificati e formalizzati nel corso del Riesame di Direzione annuale; il grado di conseguimento degli obiettivi è verificato tramite gli indicatori specifici individuati (ove necessario).

La Direzione ha il compito di valutare tutte le misure strategiche per il mantenimento del sistema, l'RSGI, è comunque promotore ed artefice di tali misure nonché garante delle misure organizzative e tecniche e della corretta applicazione del Sistema.

4 Principi e obiettivi per la Sicurezza delle informazioni

Enigma Defense, anche e soprattutto in ragione della missione aziendale, ritiene il SGI un fattore critico e abilitante per la competitività e qualificazione sul mercato, irrinunciabile per la protezione del patrimonio informativo dei propri clienti, ed un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo. In tal senso l'Azienda pone particolare attenzione ai temi riguardanti la sicurezza durante l'erogazione del servizio, che deve essere ritenuto un bene primario dell'azienda e promulga la salvaguardia, a tutti i livelli aziendali, della riservatezza delle informazioni, ottenute o generate durante lo svolgimento delle attività, riguardanti i Clienti e tutte le parti interessate, ai sensi della normativa cogente in tema di sicurezza delle informazioni e dei requisiti dello standard ISO/IEC 27001:2017.

Nel quadro sopra enunciato, Enigma Defense si pone gli obiettivi per la Sicurezza delle informazioni ed i principi di seguito espressi al fine di mantenere e garantire sempre, per sé e per le terze parti coinvolte, un adeguato livello di sicurezza ovvero assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento delle informazioni.

La gestione della Sicurezza delle informazioni costituisce una priorità politica per Enigma Defense e per la sua mission aziendale, che attribuisce importanza strategica al trattamento delle informazioni e concretizza, quali obiettivi generali, la volontà di:

- Assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati - **Riservatezza**;
- Salvaguardare la consistenza dell'informazione da modifiche non autorizzate - **Integrità**;
- Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e ai sistemi afferenti quando ne fanno richiesta - **Disponibilità**;
- Assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati - **Controllo**;
- Garantire una provenienza affidabile dell'informazione – **Autenticità**;
- Garantire la protezione ed il controllo dei dati personali - **Privacy**.

4.1 Principi ed obiettivi di riferimento

L'Organizzazione sposa e si impegna a garantire, per la sicurezza delle informazioni, gli obiettivi e i principi guida di seguito descritti. L'osservanza e l'attuazione di questi principi sono responsabilità di tutto il personale che, a qualsiasi titolo, collabora con Enigma Defense ed è in qualche modo coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del SGI. Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.

4.1.1 Politica della sicurezza

Obiettivo: *Formulare, emettere, diffondere e periodicamente revisionare la Politica e le procedure per la sicurezza delle informazioni a tutela della protezione delle informazioni ottenute/generate durante lo svolgimento delle attività, riguardanti i Clienti e tutte le parti interessate, ai sensi della normativa cogente in tema di sicurezza delle informazioni e dei requisiti dello standard ISO/IEC 27001.*

Enigma Defense ha definito una Politica per la qualità e la sicurezza delle informazioni approvata dalla Direzione e che definisce l'approccio dell'Azienda per la gestione degli obiettivi e dei principi relativi alla sicurezza delle informazioni. Tale politica è sostenuta da: specifiche procedure che declinano i principi e che guidano l'attuazione operativa degli obiettivi per la sicurezza delle informazioni, da moduli che supportano nelle misurazioni, registrazioni e monitoraggi, dai regolamenti aziendali interni che indirizzano il corretto comportamento dei dipendenti/collaboratori.

La Politica viene riesaminata dalla Direzione e dal RSGI almeno una volta l'anno in occasione del Riesame di Direzione, tenendo conto tra l'altro:

- delle modifiche che possono interessare l'azienda e gli obiettivi prefissati, di eventuali modifiche dei riferimenti legislativi e normativi applicabili e delle informazioni di ritorno derivanti dal monitoraggio delle attività eseguite.
- degli eventuali nuovi indirizzi di business e/o evoluzioni organizzative e/o tecnologiche e/o i contenuti normativi a cui la Politica intende essere conforme.
- delle informazioni di ritorno derivanti dal monitoraggio delle attività eseguite al fine di gestire nel tempo l'efficacia dei principi espressi e l'ottimizzazione del rapporto costi/benefici dei controlli implementati.

4.1.2 Organizzazione della sicurezza delle informazioni

Obiettivo: *Definire una struttura organizzativa e conseguenti responsabilità assegnate per intraprendere e controllare l'attuazione e l'esercizio della sicurezza delle informazioni all'interno dell'Azienda. Assicurare la sicurezza per tutte le modalità operative adottate. Garantire la sicurezza nell'uso dei dispositivi portatili utilizzati per svolgere le mansioni lavorative e l'erogazione dei servizi ai Clienti.*

Enigma Defense ritiene che creare un valido ambiente di sicurezza significa operare su più fronti: strutturale ed organizzativo. In tal senso la sicurezza deve essere gestita e controllata mediante una struttura organizzativa interna e conseguenti responsabilità assegnate - in ottemperanza al principio del *need-to-know* e del *need-to-use* - ed inserite nell'organigramma e funzionigramma aziendali; questo a supporto dell'intera Azienda e garantendo un ruolo di guida per tutti gli aspetti relativi alla sicurezza delle informazioni.

A prescindere dal ruolo assunto, tutto il personale in forza alla Enigma Defense è edotto, responsabilizzato e consapevole che, fra le altre, è precisa responsabilità di ognuno svolgere le proprie mansioni con un approccio al miglioramento continuo e alla sicurezza delle informazioni a garanzia di una costante ricerca della qualità e a tutela di tutte le informazioni a vario titolo trattate nei progetti assegnati. Il personale è inoltre edotto e responsabilizzato sull'uso corretto dei dispositivi mobili attraverso la sottoscrizione di puntuali regole di comportamento.

Enigma Defense è in contatto attivo con numerose associazioni e Autorità di settore e segue su differenti canali informativi (mailing list, social, ...) molteplici *security group* per la corretta e continua raccolta di informazioni, alert e warning di sicurezza. È inoltre predisposto un documento in dotazione alla Direzione e alla Segreteria contenente i principali riferimenti delle Autorità da contattare in caso di emergenze/incidenti in merito alla sicurezza delle informazioni ed alla sicurezza fisica e del lavoro.

4.1.3 Sicurezza delle risorse umane

Obiettivo: *Adottare misure idonee a garantire la sicurezza delle risorse umane oltre che la continua informazione e formazione di tutto il personale - dipendenti e collaboratori - tesa alla piena consapevolezza delle problematiche relative alla sicurezza delle informazioni a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.*

Il processo di selezione adottato dalla Enigma Defense prima dell'impiego di un professionista prevede un puntuale controllo delle precedenti esperienze del candidato dal punto di vista relazionale, di affidabilità, dei "soft skill" e delle conoscenze tecniche necessarie e richieste per la posizione di lavoro aperta. Nei colloqui preliminari sono chiariti al candidato alla collaborazione i requisiti di sicurezza richiesti dall'Azienda e formalizzati all'atto della contrattualizzazione con i collaboratori e dipendenti attraverso specifiche clausole circa la riservatezza e sicurezza delle informazioni.

All'inizio della collaborazione i nuovi assunti ricevono formazione sulla sensibilizzazione alla sicurezza delle informazioni prima che venga dato loro accesso a qualunque struttura per la gestione delle informazioni. La Enigma Defense promuove la periodica sensibilizzazione di tutto il personale (dipendenti e collaboratori) circa le responsabilità per la sicurezza delle informazioni che possiede ogni ruolo aziendale, ne consegue che tutto il personale è:

- Edotto in merito ai rischi collegati alla gestione dei dati, alle misure disponibili per prevenire tali rischi, alla disciplina sulla protezione dei dati personali in rapporto alla propria attività lavorativa, nonché ai propri doveri;
- Informato circa le proprie responsabilità in tema di sicurezza;
- Adeguatamente formato e sensibilizzato, secondo appositi piani di formazione sui temi della sicurezza delle informazioni e privacy in funzione dei ruoli e delle responsabilità di sicurezza attribuiti, per il rispetto puntuale dei principi e l'applicazione delle regole adottate;
- Chiamato ad operare secondo norme di comportamento e di uso accettabile dei beni aziendali;
- Chiamato a segnalare anomalie (incidente, data breach o sospetto tale), e ogni comportamento non in linea con quanto definito, nelle norme emanate dall'Azienda;
- Invitato a svolgere le proprie attività sulla base del principio "della necessità del sapere" (*need to know*) e in conformità con le regole relative al grado di riservatezza classificato delle informazioni;
- Consapevole di quali implicazioni disciplinari possono scaturire dalla violazione delle politiche e delle regole - aziendali e non - in merito alla sicurezza delle informazioni.

La consapevolezza dei temi della sicurezza che si auspica per tutti i dipendenti e collaboratori è raggiunta non solo attraverso gli strumenti contrattuali, la formale documentazione aziendale, ma anche dalla continua formazione e sensibilizzazione sul tema.

Tutti i dipendenti sono tenuti a rispettare un accordo di riservatezza nell'ambito dei loro termini e delle loro condizioni di impiego iniziali e sono edotti circa le conseguenze disciplinari che comporta un comportamento scorretto. Sono definiti accordi di riservatezza anche verso le terze parti che, nell'ambito della fornitura dei propri servizi/prodotti, entrino direttamente o indirettamente a contatto con informazioni personali e/o critiche per Enigma Defense.

A conclusione del rapporto lavorativo, il collaboratore in uscita restituisce gli asset utilizzati nel corso della collaborazione con l'azienda ed è reso consapevole di quali responsabilità circa la sicurezza delle informazioni permangano e per quanto tempo dopo la cessazione del rapporto di lavoro e della collaborazione con l'Azienda.

4.1.4 Gestione degli asset

Obiettivo: *Definire un catalogo/inventario costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni corredato con la loro classificazione e con gli aspetti di responsabilità funzionale. Prevenire la divulgazione non autorizzata, la modifica, la rimozione o la distruzione delle informazioni archiviate sui sistemi.*

Enigma Defense censisce e classifica i sistemi e le informazioni oltre che i luoghi ove opera, formalizzandoli in un documento di inventario. Tale documento è periodicamente rivisto, corretto ed integrato. Le informazioni aziendali sono classificate in tre principali categorie - *Public*, *Protected* e *Confidential* - nonché etichettate e trattate, così come i sistemi, in funzione di tale classificazione.

Ogni appartenente all'Azienda è chiamato ad utilizzare i sistemi aziendali per tutte e sole le finalità di adempimento delle mansioni lavorative affidate e consentite e comunque per l'esclusivo perseguimento degli obiettivi aziendali. In tal senso le regole per l'utilizzo corretto degli asset e delle informazioni sono state identificate, documentate e sottoscritte dal personale tutto. Inoltre, ogni dipendente e collaboratore è responsabile dei dati memorizzati sulla propria stazione di lavoro, a prescindere dalla loro classificazione. Il trattamento dei supporti removibili è normato attraverso una specifica procedura e da un regolamento sottoscritto da tutti i dipendenti e collaboratori.

4.1.5 Controllo degli accessi

Obiettivo: *Definire e adottare un processo di identificazione ed autenticazione per limitare l'accesso alle informazioni e ai servizi di elaborazione delle informazioni nel quale le autorizzazioni di accesso siano differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in conformità ai principi del need-*

to-know e need-to-use, e che tali autorizzazioni siano periodicamente sottoposte a revisione. Sensibilizzare e responsabilizzare i dipendenti/collaboratori in merito alla salvaguardia delle loro informazioni di autenticazione.

Enigma Defense ritiene che il controllo degli accessi logici rappresenti uno dei principali strumenti di gestione, controllo e tutela del proprio patrimonio informativo, costituendo infatti l'insieme delle regole che disciplinano le modalità di accesso da parte degli utenti alle informazioni, ed è finalizzato a prevenire l'utilizzo non autorizzato delle stesse. I diritti di accesso sono concessi alla funzione/ruolo ricoperto dalla risorsa in ottemperanza ai principi di *need-to-know* e *need-to-use*, così da permettere solo l'accesso ai dati, applicazioni, sistemi e dispositivi aziendali strettamente necessari al ruolo organizzativo della risorsa. L'architettura della rete interna di Enigma Defense garantisce l'applicazione del principio del *need-to-use* con accessi selettivi per reti (con particolare riferimento alle reti wireless) e servizi.

L'accesso agli asset informativi avviene attraverso l'assegnazione di una o più utenze individuali al personale per lo svolgimento delle proprie mansioni lavorative. I diritti di accesso a reti e sistemi sono concessi in ottemperanza ai principi di *need-to-know* e *need-to-use*. Alla consegna delle credenziali, l'utente viene informato – mediante specifica disposizione aziendale – che l'identificativo e la password sono strettamente personali, e che deve farne uso operando esclusivamente nell'ambito delle autorizzazioni ricevute. In caso di variazione di funzione del dipendente/collaboratore, sono modificati i diritti di accesso conformemente alle necessità legate al nuovo ruolo assunto; tale processo si origina al mutare delle esigenze di accesso ai dati, applicazioni, sistemi e dispositivi aziendali. La creazione di utenze c.d. "generiche", ossia utenze il cui nome utente non sia chiaramente riconducibile alla risorsa, è fortemente scoraggiata. Nel caso di utenze di servizio, le credenziali sono gestite direttamente dagli AdS.

Le credenziali relative a profili amministrativi sono gestite con opportune cautele e la tracciatura degli accessi è adottata secondo quanto richiesto dal provvedimento emesso dal Garante per la Privacy (Provvedimento del Garante del 27 novembre 2008). L'utilizzo di utenze privilegiate è limitato alle reali necessità dell'Azienda e autorizzato dal RSGI. In tal senso l'Amministratore di sistema, unico incaricato alla gestione della sicurezza e della configurazione dei sistemi, possiede le credenziali relative alle utenze Amministrative. Conformemente a quanto richiesto dalla normativa vigente in tema di Amministratori di Sistema, l'assegnazione di una utenza amministrativa è formalizzata mediante apposito documento di nomina e le attività sottoposte al monitoraggio tramite la registrazione dei log di accesso e controlli almeno annuali.

Le password costituiscono il primo livello di protezione per l'accesso a qualunque tipo di risorsa informatica. Per questo motivo e, al fine di ridurre al minimo il rischio di furto o intercettazione, la loro gestione è normata da un processo formale e documentato oltre che da chiare regole di comportamento sottoscritte da tutti i dipendenti/collaboratori. Ove possibile, sono presenti configurazioni applicative tali da forzare l'utente alla scelta di password robuste e al periodico aggiornamento delle stesse.

Periodicamente, e comunque almeno una volta l'anno o in caso di variazioni organizzative, sono rivisti i diritti di accesso degli utenti in modo che siano correttamente applicati i principi di *need-to-know* e *need-to-use*, ovvero che i diritti di accesso attribuiti siano in linea con le mansioni.

Tutto il personale della Enigma Defense è chiamato a seguire le specifiche di sicurezza relative alle password diffuse attraverso il Regolamento Aziendale ed è inoltre responsabilizzato all'osservanza delle procedure e delle misure di sicurezza definite.

L'accesso alle informazioni da parte degli utenti è limitato in ottemperanza al principio di *need-to-know* sia per quanto concerne l'accesso a sistemi/applicazioni che contengano informazioni di proprietà dell'azienda ed in generale le informazioni interne, che per quello a sistemi/applicazioni che consentano il trattamento di dati di terze parti. Ove necessario, per la tutela di informazioni confidenziali sono applicate procedure di log-on sicure, come ad esempio canali SSL con mutua autenticazione o procedure di autenticazione a due fattori se richiesto. La scelta delle credenziali di accesso da parte di tutta la popolazione aziendale di Enigma Defense deve essere conforme alle disposizioni aziendali relative all'utilizzo della strumentazione informatica. Ove

possibile sono implementati meccanismi automatici di controllo della qualità delle credenziali (robustezza, divieto di inserimento di una delle ultime password già utilizzate, autenticazione su canale cifrato). Per l'accesso ai sistemi dei Clienti, gli operatori di Enigma Defense seguono linee guida, procedure e policy dettate dal Cliente, ferme restando le best practice relative alla gestione sicura delle credenziali di autenticazione.

L'utilizzo di utility che permettono di aggirare i controlli applicativi e di sistema è proibito, salvo specifica autorizzazione da parte del RSGI per ruolo, esigenze di progetto o necessità puntuali di gestione di problemi o analisi.

4.1.6 Crittografia

Obiettivo: *Assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni.*

Enigma Defense ha analizzato, anche in ragione degli obblighi di conformità rispetto ai temi della Privacy, la necessità di applicare tecniche di crittografia al fine di salvaguardare la riservatezza dei dati aziendali. Il risultato di tale analisi ha portato ad identificare in quali circostanze risulti necessaria l'applicazione di controlli crittografici tesi a salvaguardare la confidenzialità, l'integrità e la disponibilità dei dati, sia in fase di trasporto e condivisione (*in motion*) che in fase di elaborazione e archiviazione (*at rest*).

Relativamente ai dati ***in motion*** è richiesto:

1) l'utilizzo di canali di comunicazione sicuri basati su protocolli crittografici sicuri (es. TLS);
2) L'utilizzo di connessioni di tipo tunneling attraverso VPN per le attività che prevedono l'accesso ai sistemi remoti dei clienti.

Per quanto concerne i dati ***at rest***, le informazioni classificate come *Confidential* sono trattate esclusivamente su sistemi dotati di crittografia a livello di sistema operativo o attraverso l'utilizzo di tool di cifratura.

4.1.7 Sicurezza fisica ed ambientale

Obiettivo: *Garantire un adeguato livello di sicurezza fisica degli ambienti operativi - sedi e singoli locali aziendali - dove risiedono le apparecchiature, gli archivi e sono gestite le informazioni. Prevenire la perdita, il danneggiamento, il furto o la compromissione dei sistemi nonché l'interruzione dei servizi erogati.*

Enigma Defense, recependo la protezione del luogo di lavoro e del lavoratore come obiettivi primari, li riconosce, in ogni caso ed in ogni occasione, come prioritari nell'applicazione della propria strategia di sicurezza fisica. Oltre a tale fondamentale principio, Enigma Defense intende la sicurezza fisica come elemento propedeutico al successo della sicurezza logica, ritenendo infatti che lacune sulla prima, oltre che generare rischi di tipo fisico, possano ridurre sensibilmente l'efficacia delle misure di protezione di tipo logico.

L'azienda identifica nella propria sede operativa estesa e nelle sedi dei propri Clienti, le principali aree fisiche di riferimento per l'operatività e il trattamento delle informazioni.

Per quanto concerne la propria sede operativa, Enigma Defense si avvale di più livelli di sicurezza ovvero di più livelli di accesso con controllo di identità prima di poter accedere all'ufficio vero e proprio e adotta misure di sicurezza fisica tese a garantire, all'interno del perimetro fisico di riferimento per l'Azienda, la sicurezza dei dipendenti e dei visitatori, la prevenzione dal danneggiamento e/o dalla perdita di asset aziendali e delle informazioni in essi contenute.

Per la più corretta gestione del tema della sicurezza sul lavoro, l'Azienda si avvale di un RSPP che ha provveduto alla redazione del DVR come da D.Lgs. 81/2008. Valutando quale obiettivo prioritario quello della tutela della sicurezza e della salute delle persone fisiche sono periodicamente svolte attività di sensibilizzazione e formazione a tutti i dipendenti e collaboratori in conformità ai requisiti del D.Lgs. n. 81/2008.

Presso la sede operativa sono definiti chiaramente i perimetri di sicurezza fisica (in relazione al grado di criticità delle attività che vi si svolgono e del valore degli asset informativi che vi sono conservati) secondo una suddivisione in tre principali aree, per tipologia di accesso: **aree pubbliche**, **aree di carico e/o scarico**, **aree riservate**. Tali aree sono identificate e mantenute adeguatamente separate tra loro; in tal senso le aree riservate sono accessibili solo attraverso percorsi visibili e sempre controllati così come le aree di carico/scarico. L'accesso ai visitatori è controllato e registrato anche in conformità alle misure per il contrasto e il contenimento della diffusione della sindrome da coronavirus COVID-19 negli ambienti di lavoro.

In riferimento alla protezione delle apparecchiature informatiche e dei cablaggi, il loro posizionamento avviene in modo da ridurre al minimo necessario il passaggio, ovvero l'accesso, da parte di visitatori nelle aree di lavoro (aree riservate) e ottimizzare l'attivazione di misure di sicurezza mirate alla protezione dell'effettivo valore delle apparecchiature. Tutti i sistemi sono sottoposti ad interventi di manutenzione, al fine di garantirne l'efficienza nel tempo, svolti conformemente a quanto indicato dal produttore ed effettuati da personale specializzato; nel caso in cui la manutenzione avvenga al di fuori della sede aziendale sono adottate specifiche misure di protezione dei dati presenti sulle apparecchiature.

I sistemi aziendali, con particolare riferimento a quelli di supporto dati (analogici e/o digitali), non sono trasferibili se non previa autorizzazione del RSGI o di un responsabile da esso delegato. Ogni apparecchiatura/sistema che non sia più utilizzato dall'Azienda è sottoposta ad un preliminare controllo dei contenuti e ad una successiva cancellazione dei dati a basso livello attraverso tool dedicato. Per quanto concerne il riutilizzo delle apparecchiature, i sistemi che vengono riutilizzati sono sottoposti a controllo, successiva sovrascrittura (ivi comprese le utenze del precedente assegnatario) e configurazione per il nuovo utilizzo.

L'Azienda ha infine definito e diffuso, attraverso il regolamento aziendale, specifiche direttive di tipo "clear desk" e "clear screen" sottoscritte da tutti i dipendenti e collaboratori.

4.1.8 Sicurezza delle attività operative

Obiettivo: *Assicurare la sicurezza dei sistemi e delle attività che sottendono al trattamento delle informazioni. Gestire e monitorare efficacemente ed efficientemente il sistema informativo al fine di garantirne la sicurezza e la corretta operatività, il rispetto dei livelli di servizio, preservando la riservatezza e la criticità delle informazioni.*

Enigma Defense ritiene che il proprio Sistema Informativo debba essere gestito in modo efficace ed efficiente nel tempo al fine di garantirne la sicurezza e la corretta operatività e preservare la riservatezza e la criticità delle informazioni; da questo derivano molteplici principi da adottare nelle attività aziendali che si declinano in idonee procedure operative.

Enigma Defense ha definito, documentato e diffuso le procedure operative necessarie alla corretta gestione delle informazioni da parte di tutto il personale interno oltre che di documenti indicanti le misure di sicurezza la cui applicazione è richiesta alle terze parti che a vario titolo concorrono al trattamento delle informazioni di cui Enigma Defense è proprietaria, responsabile o Titolare.

La Direzione di Enigma Defense svolge un controllo continuo e periodico sui cambiamenti interni ed esterni all'azienda che possano direttamente e/o indirettamente influenzare i processi di business, con particolare attenzione ai sistemi che sottendono alla sicurezza delle informazioni. I cambiamenti e le azioni da porre in essere sono discussi almeno annualmente in occasione del Riesame della Direzione e nell'ambito delle riunioni di CDA. Sempre nell'ambito dell'annuale Riesame, la Direzione effettua la valutazione dei fabbisogni di risorse (personale, tecnologia, formazione) necessarie al mantenimento dell'adeguato livello di qualità e sicurezza delle informazioni dei servizi erogati con particolare attenzione alla sicurezza delle informazioni trattate.

Gli ambienti di test e produzione, intesi nell'accezione idonea al contesto in cui Enigma Defense opera, sono sempre mantenuti separati intendendo in tal senso distinti anche i dati utilizzati per le fasi di test e sviluppo

di una soluzione da quelli invece di produzione. I dati di test sono fittizi e in nessun caso vengono utilizzati dati reali di clienti, dipendenti o fornitori di Enigma Defense.

Ogni apparecchiatura/sistema della Enigma Defense è protetta da un software antivirus/DLP teso ad individuare malware, virus ed in generale codice maligno che possa mettere a rischio la sicurezza delle informazioni trattate. La protezione da virus e codice malevolo è attuata anche attraverso la continua sensibilizzazione verso dipendenti/collaboratori che, a prescindere dalla presenza del software antivirus, devono sempre tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software potenzialmente pericoloso.

Enigma Defense individua e pone in essere tutte le tecniche per salvaguardare la disponibilità dei dati confidenziali che tratta a vario titolo. Sono compresi i dati aziendali relativi a risorse umane, contabilità, amministrazione, nonché dati di clienti e configurazioni di sicurezza. Tutti i backup sono eseguiti con cadenza regolare e custoditi in ambienti separati, protetti da sistemi di controllo degli accessi fisici.

Enigma Defense adotta tecnologie per la raccolta dei log di sicurezza generati da sistemi e device di rete a supporto di tutte le attività di analisi nell'ambito della gestione di situazioni di criticità. I log sono consultabili dal solo profilo amministrativo. Conformemente anche a quanto indicato dalla direttiva del Garante Privacy in tema di Amministratori di Sistema, Enigma Defense prevede la raccolta e la storicizzazione degli eventi relativi alle utenze privilegiate con *retention* non inferiore ai sei mesi. I log sono opportunamente protetti e periodicamente riesaminati.

Tutti i sistemi aziendali utilizzati per l'erogazione dei servizi sono consegnati al dipendente con una configurazione protetta (*baseline* di sicurezza) che prevede il sistema operativo e software preinstallati aggiornati alla data di consegna. Non è permesso installare pacchetti applicativi aggiuntivi se non autorizzati direttamente dal RSGI. La baseline di sicurezza è periodicamente rivista dal RSGI per verificare che sia sempre adeguata in termini di sicurezza e soddisfacimento delle esigenze di business. Tutta la popolazione aziendale è tenuta al rispetto delle leggi in materia di tutela dei diritti d'autore sul software e non può installare, duplicare o utilizzare i software al di fuori di quanto consentito dagli accordi di licenza.

Enigma Defense svolge regolari attività di verifica delle vulnerabilità tecniche alle quali possono essere soggetti i propri sistemi. Tale analisi può prevedere sia una attività di monitoraggio delle vulnerabilità note attraverso fonti accreditate e riconosciute a livello internazionale che analisi strumentali sulla rete interna e dalla rete esterna. Ove questo non pregiudichi la funzionalità, tutti i sistemi sono regolarmente aggiornati con patch di sicurezza pubblicate sui canali ufficiali dei vendor.

Gli audit interni dei sistemi informativi sono condotti secondo il calendario e le modalità definite dalla Direzione in fase di Riesame, con cadenza almeno annuale. Le attività di audit sono pianificate e organizzate in modo da minimizzare l'impatto sulle attività operative.

4.1.9 Sicurezza delle comunicazioni

Obiettivo: *Assicurare la protezione delle informazioni sulle reti e nei sistemi utilizzati per l'erogazione dei servizi e il trattamento delle informazioni. Garantire tale protezione delle informazioni in transito sia all'interno che con le entità esterne.*

Enigma Defense implementa tutti i controlli necessari a garantire la sicurezza delle comunicazioni attraverso la propria rete aziendale. Tutti le attività che prevedono la connessione verso i sistemi dei clienti sono veicolate tramite collegamenti VPN Site-to-site. La sicurezza del perimetro della rete è garantita da un cluster firewall gestito da un Amministratore di sistema di Enigma Defense certificato dal produttore. I sistemi sia client che server sono dotati di meccanismi di autenticazione tramite username e password. L'amministratore è in grado, tramite opportuno tool di monitoraggio e analisi del traffico di rete, di monitorare il traffico di rete e individuare eventuali attività anomale. Tutti gli utenti sono edotti sulle regole comportamentali relative all'utilizzo dei servizi di rete.

Enigma Defense applica le best practice relative alla segregazione della propria rete interna, la quale è suddivisa in aree con diversi livelli di accesso garantiti da liste di controllo.

Enigma Defense norma il trasferimento delle informazioni attraverso regole e procedure diffuse all'interno della propria organizzazione. Per quanto concerne gli accordi relativi al trasferimento di informazioni con i propri clienti, fornitori e partner, Enigma Defense predispone accordi di non divulgazione nel quale sono definite, tra le altre, le regole relative allo scambio di informazioni tra le parti. Tale documento è propedeutico alla sottoscrizione di qualsiasi contratto che, a vario titolo, preveda l'accesso a informazioni di Enigma Defense e/o della controparte. Analogamente Enigma Defense prevede la sottoscrizione di un accordo di riservatezza con i propri dipendenti, presentato in fase di assunzione. Gli accordi di riservatezza sono periodicamente rivisti dalla Direzione e, se necessario, aggiornati e fatti sottoscrivere nuovamente.

La gestione della comunicazione delle informazioni attraverso i possibili canali di messaggistica elettronica (*email*, *instant messaging*, *social network*, …) è definita e documentata attraverso regole interne diffuse ai dipendenti/collaboratori, clausole contrattuali e NDA verso le terze parti. Enigma Defense definisce una classificazione delle informazioni a vario titolo trattate nel corso dell'esecuzione di un contratto, e redige appropriati accordi di riservatezza e non divulgazione con le terze parti che a vario titolo trattano le informazioni classificate.

4.1.10 Acquisizione, sviluppo e manutenzione dei sistemi

Obiettivo: *Applicare i principi di security by design e security by default per i quali la sicurezza deve essere elemento costitutivo ed imprescindibile nella fase di progettazione, sviluppo, test, esercizio, manutenzione, assistenza e dismissione dei servizi erogati.*

Enigma Defense intende assicurare che la sicurezza delle informazioni sia parte integrante di tutto il ciclo di vita dei sistemi informativi, inclusa la definizione dei requisiti specifici per i sistemi informativi che forniscono servizi. L'introduzione di un nuovo componente del sistema informativo (derivante da una necessità interna o esterna) prevede un'analisi che valuti con priorità i requisiti di sicurezza delle informazioni, quali la salvaguardia della confidenzialità, integrità e disponibilità dei dati, nonché i principi di continuità operativa e i requisiti normativi, con particolare con riferimento al trattamento dei dati personali. Altri parametri considerati sono: il mercato, la rispondenza tra le caratteristiche servizio con i requisiti funzionali inizialmente indicati, eventuali report di incidenti, il *sentiment* generale verso la soluzione, il fattore costi/benefici, la scalabilità della soluzione. I requisiti relativi alla sicurezza delle informazioni fanno inoltre parte dei requisiti contrattuali richiesti ai fornitori a vario titolo interessati per l'introduzione del nuovo componente.

Enigma Defense non espone alcun servizio su rete pubblica dalla propria rete aziendale. Per quanto riguarda i servizi di cui Enigma Defense usufruisce, tutte le comunicazioni avvengono su canale sicuro cifrato. Con le terze parti coinvolte sono stipulati contratti commerciali che prevedono clausole di riservatezza e garanzia relativamente ai controlli tecnologici, come ad esempio sistemi di autenticazione sicuri e garanzia dei livelli di servizio.

Enigma Defense è consapevole dell'importanza dell'adozione di strumenti e metodologie tese a considerare e implementare opportune attività di sicurezza nel corso di tutte le sue fasi del ciclo di vita del software, sia per rispondere in modo efficace alle problematiche di sicurezza che per ridurre i costi che comportano trascurarla.

La sicurezza del processo di sviluppo del software delle terze parti è regolamentata dagli accordi contrattuali e dai termini di utilizzo dei software commerciali. Enigma Defense richiede ai fornitori la garanzia di pieno supporto agli aggiornamenti di sicurezza e la compatibilità con i sistemi operativi più comuni.

Nel caso in cui si reputi necessario l'aggiornamento dei sistemi operativi utilizzati da consulenti e tecnici, Enigma Defense predispone un piano di aggiornamento che prevede una analisi di compatibilità dei software utilizzati per l'erogazione dei servizi unita ad una valutazione di sicurezza effettuata dal RSGI. Come da Regolamento interno distribuito e sottoscritto da parte di tutti i dipendenti e collaboratori, è fatto

espressamente divieto di modificare in alcun modo i pacchetti software utilizzati per l'installazione o aggiornamento di applicativi utilizzati sui PC aziendali. In particolare, è espressamente vietata l'installazione di software che non sia stato precedentemente approvato dal RSGI. Nei rari casi in cui si renda necessaria la modifica di un pacchetto applicativo, tale modifica deve essere preventivamente approvata dal responsabile del processo aziendale coinvolto e dal RSGI per valutare gli impatti sulla sicurezza delle informazioni che tale modifica potenzialmente può portare.

Enigma Defense applica i principi di ingegnerizzazione sicura ai sistemi aziendali attraverso la definizione delle baseline atte a garantire la configurazione sicura dei sistemi e sviluppate avvalendosi dei requisiti /controlli definiti dalle *best practice* di settore e delle linee guida fornite dal vendor / produttore. La revisione e il monitoraggio delle baseline è effettuata annualmente dal RSGI. Qualora, a valle dell'attività di monitoraggio emergano delle non-conformità nella configurazione dei sistemi, queste sono gestite secondo la procedura di gestione non conformità adottata dall'Azienda. Le eccezioni, intese come accettazione delle non-conformità individuate, devono essere approvate e documentate.

Enigma Defense predispone un ambiente sicuro all'interno della propria rete aziendale dedicato allo sviluppo di soluzioni. Nell'ambito dell'erogazione dei propri servizi, Enigma Defense effettua tuttavia attività di test principalmente sui sistemi/ambienti dei propri clienti, seguendo e applicando i criteri forniti da quest'ultimi e/o il proprio modello di test e collaudo, e, ovviamente le best practice di sicurezza. In ambiente di test, Enigma Defense utilizza (e suggerisce di utilizzare) sempre dati fittizi; in particolare quanto si renda necessario utilizzare dati personali si avvale di dati manipolati (con varie tecniche di manipolazione) non riconducibili a persona fisica. Nel caso in cui, nell'ambito dell'erogazione dei propri servizi, si renda necessario effettuare attività di test su sistemi/applicativi di un cliente, Enigma Defense applica criteri e indicazioni relativamente alla sicurezza dei dati di test fornite da quest'ultimo.

4.1.11 Relazioni con le terze parti

Obiettivo: *Assicurare la protezione dei sistemi e delle informazioni dell'Azienda nei rapporti con le terze parti, a livello contrattuale, organizzativo e tecnico. Verificare periodicamente il livello concordato per la sicurezza delle informazioni e gli accordi contrattuali con i fornitori.*

Enigma Defense può ricorrere nell'ambito della propria attività a terze parti (o fornitori esterni) per la fornitura di prodotti/servizi. L'azienda ricorre unicamente a fornitori/consulenti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, nominando questi ultimi, ove previsto, responsabili del trattamento dei dati personali, come prescritto dall'art. 28 del Regolamento (UE) 2016/679.

I rapporti con i Fornitori si svolgono unicamente attraverso accordi o contratti formali che includono adeguati requisiti relativi alla sicurezza delle informazioni; i requisiti sono stabiliti, concordati e contrattualizzati con ciascun fornitore che possa avere accesso, elaborare, archiviare, trasmettere o fornire informazioni. Nello specifico Enigma Defense:

- effettua una mappatura delle tipologie di Fornitori di cui si avvale con le informazioni che per mandato ricevuto essi devono trattare;
- identifica le misure di sicurezza ed i controlli necessari alla protezione e tutela delle informazioni aziendali da concordare con i Fornitori;
- definisce contratti /accordi da far sottoscrivere ai propri fornitori per assicurare che gli opportuni requisiti di sicurezza siano formalmente presenti nelle relazioni esterne.

Enigma Defense, ove il rapporto di fornitura (ad esempio in occasione di gare di appalto) contempli la possibilità di avvalersi di sub-fornitori, subordina il subappalto alle misure di sicurezza e confidenzialità idonee a tutelare i propri prodotti/servizi ovvero le informazioni trattate, attraverso avvalimento, dal Fornitore. In caso di nomina del Fornitore a Responsabile del Trattamento è richiesta da parte dell'Azienda prova formale dell'applicazione delle misure di sicurezza a tutta la filiera oltre che riservarsi la possibilità di compiere su questa attività di audit e verifiche strumentali di sicurezza.

Enigma Defense svolge sui propri Fornitori attività di monitoraggio – ove necessario anche di tipo strumentale - tese a verificare la qualità dei servizi svolti nonché la correttezza e sicurezza di trattamento delle informazioni secondo quanto inizialmente convenuto e sottoscritto. E' inoltre formalmente richiesto ai Fornitori mettere a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di sicurezza cui sono de iure o de facto sottoposti e consentire nonché contribuire alle attività di revisione, comprese le ispezioni - tecniche, organizzative, amministrative - realizzate da Enigma Defense, nonché collaborare attivamente in caso di incidenti di sicurezza per i necessari adempimenti verso le Autorità e le eventuali notifiche ad altre parti interessate.

A fronte di cambiamenti nel contesto di riferimento entro cui si svolge il rapporto di fornitura e comunque almeno una volta l'anno, Enigma Defense rivede (e ove necessario riformula) i contratti di fornitura, in relazione alle eventuali mutate esigenze di sicurezza dell'Azienda, dell'evoluzione degli scenari di rischio e degli incidenti di sicurezza occorsi.

4.1.12 Gestione degli incidenti

Obiettivo: *Adottare un processo di gestione tempestiva degli incidenti e dei data breach efficace, coerente con il contesto in cui l'azienda opera, conforme a quanto richiesto da normative de iure o de facto in tema di sicurezza delle informazioni.*

Enigma Defense è consapevole dell'importanza dell'esistenza di un processo dedicato alla Gestione degli Incidenti, per tempestivamente trattare e, ove possibile prevenire, eventuali incidenti di sicurezza e *data breach*. In tal senso l'Azienda si avvale di un processo (e della relativa procedura) per la gestione degli incidenti di sicurezza e dei *data breach* - conforme a quanto richiesto dalla vigente normativa in tema di tutela e protezione delle informazioni personali - assegnando le opportune responsabilità e compiti.

L'Azienda individua le principali fonti - personale interno, fornitori, clienti - attraverso le quali ricevere segnalazione di situazioni/eventi relativi alla gestione della sicurezza delle informazioni che possano dare indicazione di un potenziale incidente di sicurezza. Per ognuna di queste fonti sono individuati canali e modalità di comunicazione, questo anche a garanzia degli aspetti di celerità e continuità fondamentali nella gestione di un incidente di sicurezza oltre che requisiti cogenti in caso di *data breach* che coinvolga informazioni personali. Dipendenti e collaboratori di Enigma Defense sono tenuti a segnalare con la massima tempestività al proprio responsabile o al RSGI qualunque tipo di vulnerabilità ai sistemi o servizi aziendali che possa potenzialmente portare ad una violazione della sicurezza delle informazioni. La segnalazione - inviata tramite il mezzo che preveda la massima celerità nel comunicare la problematica - deve essere, ove possibile, corredata di un breve resoconto scritto via e-mail al responsabile che descriva le modalità di identificazione della vulnerabilità (es. anomalia operativa, notizie pubbliche, …).

Enigma Defense individua e documenta i criteri per la classificazione degli eventi relativi alla sicurezza delle informazioni. In funzione di tali criteri, il CSIRT dell'azienda effettua una valutazione e definisce se l'evento segnalato debba essere classificato o meno come incidente di sicurezza. In funzione della classificazione individuata è possibile mettere in campo azioni e ruoli adeguati, differenziati e proporzionati a seconda della gravità e dell'impatto dell'evento/incidente. Tutte le azioni in risposta ad un incidente di sicurezza sono opportunamente tracciate in un registro degli incidenti.

Enigma Defense analizza con cadenza regolare gli incidenti di maggiore criticità, al fine di migliorare la procedura e la preparazione alla risposta agli incidenti stessi, e ridurre la probabilità di un loro nuovo accadimento. Le evidenze relative agli incidenti di sicurezza sono raccolte e, se necessario, trasferite in conformità con quanto richiesto dalle procedure di analisi forense riconosciute dagli operatori del settore, oltre che dalle autorità competenti.

Nel caso specifico di una violazione relativa a dati personali (Data Breach) di cui Enigma Defense sia Titolare o Responsabile del trattamento, si applica quanto previsto dalla normativa vigente in materia di gestione e trattamento dei dati personali - Regolamento (UE) 2016/679.

4.1.13 Continuità per la sicurezza delle informazioni

Obiettivo: *Predisporre un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.*

Enigma Defense ha identificato e documentato i requisiti di continuità rispetto alla sicurezza delle informazioni trattate e delle infrastrutture attraverso le quali tali informazioni sono veicolate. Nella definizione dei requisiti si tiene conto, oltre che dei principi relativi alla gestione della sicurezza delle informazioni e della continuità operativa, degli aspetti sanitari e delle conseguenti restrizioni, ivi compresa la possibilità di non poter accedere alla sede operativa.

L'azienda ha definito un piano di continuità operativa che sintetizza come i requisiti di continuità individuati siano soddisfatti e le azioni da intraprendere in scenari di malfunzionamento e/o crisi siano definite. Parte integrante di tale piano è un processo di esternalizzazione di servizi chiave che contribuisce anche ad elevare il livello di continuità della sicurezza delle informazioni avvalendosi di Fornitori accreditati che garantiscono, con infrastrutture strutturate, la continuità dei servizi, la ridondanza dei relativi sistemi fisici oltre che la tutela delle informazioni trattate.

Con riferimento all'emergenza sanitaria da COVID-19, in ottica di attuazione della continuità operativa Enigma Defense ha attivato per tutte le risorse aziendali contratti di *smart working* garantendo la sicurezza delle informazioni trattate dai dipendenti, con particolare riguardo alla continuità operativa verso i Clienti che richiedono una interazione giornaliera. In tal senso, tutte le risorse che operano su tali clienti sono dotate di dispositivi che garantiscono il supporto ai clienti anche da remoto, ove previsto anche tramite collegamento sicuro in VPN.

Le periodiche attività di audit interno prevedono specifiche verifiche e valutazioni sull'efficacia dei meccanismi di continuità posti in essere. Eventuali non conformità devono essere portate all'attenzione della Direzione per un riesame ed eventuali azioni di rientro.

Enigma Defense garantisce la disponibilità delle apparecchiature/sistemi interni identificati come rilevanti ai fini del trattamento e la gestione delle informazioni, nonché per l'erogazione dei servizi, sia attraverso una ridondanza fisica dei sistemi e acquisto di parti di ricambio, sia attuando, ove possibile, un approccio operativo di tipo *thin client*.

4.1.14 Conformità

Obiettivo: *Assicurare la conformità con i requisiti cogenti e con i principi legati alla sicurezza delle informazioni ovvero garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.*

Enigma Defense ha definito, documentato e mantiene aggiornati tutti i requisiti cogenti e contrattuali pertinenti alle proprie attività, oltre all'approccio per soddisfarli. Oltre ai requisiti stabiliti dai contratti stipulati con i Clienti per l'erogazione dei servizi, Enigma Defense individua (ed opera in conformità con) le seguenti quali normative di riferimento:

- Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali
- D. Lgs. n. 101/2018 e successivi aggiornamenti vigenti in materia di Data Protection
- D. Lgs. 81/2008 e successivi aggiornamenti vigenti in materia di salute e sicurezza nei luoghi di lavoro
- Disposizioni emanate dalla Presidenza del Consiglio dei ministri, dal Ministero della Salute e dall'Istituto Superiore della Sanità per la regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus SARS-CoV-2 e della relativa malattia infettiva respiratoria COVID-19 negli ambienti di lavoro.

Sono considerati inoltre normativa volontaria di riferimento gli standard:

- UNI EN ISO 9001:2015
- ISO/IEC 27001:2017 e ISO/IEC 27002:2017

I requisiti derivanti dalla legislazione applicabile e dai requisiti contrattuali sono mantenuti costantemente aggiornati per riflettere i nuovi impegni assunti verso terze parti e i nuovi obblighi a cui l'Azienda è soggetta. Tale operazione è eseguita sistematicamente al completamento della negoziazione di ogni contratto o all'uscita di ogni norma oppure attraverso aggiornamenti effettuati con una frequenza almeno annuale volta a verificare la presenza di nuovi elementi da prendere in considerazione.

Enigma Defense acquista o acquisisce prodotti o licenze solo da rivenditori/distributori autorizzati il cui legame con il detentore dei diritti di proprietà intellettuale può essere chiaramente tracciato. La registrazione dell'avvenuto acquisto o acquisizione è conservata almeno per tutto il tempo in cui il software viene utilizzato in modo da dimostrare il corretto comportamento dell'Azienda.

Come asset che possono contenere dati critici, i moduli e le registrazioni considerate più sensibili, sono censite e classificate confidenziali e ad esse sono applicate misure di sicurezza proporzionali alla classificazione ovvero al grado di criticità delle informazioni contenute. In funzione delle esigenze dell'Azienda e nel pieno rispetto dei limiti previsti dalla normativa (prima fra tutte quella relativa al trattamento dei dati personali) è stata definita una retention per ogni tipologia di documento.

Enigma Defense applica i controlli crittografici in conformità con la legislazione e i regolamenti emanati dall'Italia e dal UE.

Al fine di avere un valido riscontro sull'andamento della gestione della sicurezza delle informazioni, Enigma Defense pianifica almeno annualmente attività di audit interno tese a valutare l'idoneità dell'approccio alla sicurezza delle informazioni, l'adeguatezza dei processi e delle modalità operative, oltre che aspetti più tecnologici. Ove durante l'audit si riscontrino degli elementi di non conformità, tali elementi sono sottoposti ad analisi al fine di comprenderne a fondo le cause e di intraprendere azioni per il loro superamento puntuale ma anche sistematico. Nell'ambito delle periodiche attività di verifiche interne o nel caso di esigenze puntuali o evidenze derivanti dal monitoraggio dei sistemi e degli eventi, sono svolte analisi strumentali tese a identificare e correggere eventuali vulnerabilità tecniche e di architettura dell'infrastruttura di sicurezza.

Tutto il personale di Enigma Defense e le terze parti che con essa si relazionano operano per assicurare la privacy e la protezione dei dati personali, come richiesto dalla legislazione e dai regolamenti pertinenti o applicabili.