Politica per la Sicurezza delle Informazioni

Questo documento stabilisce la Politica per la Sicurezza delle Informazioni, secondo le indicazioni dello standard ISO/IEC 27001, cui la società Base Digitale Platform S.p.A. ha aderito.

Dal momento che il tema della sicurezza delle informazioni ha ormai assunto particolare rilevanza sia a livello nazionale che internazionale, il quadro normativo di riferimento include non solo lo standard ISO di cui sopra, ma anche la legislazione europea, laddove applicabile, in particolare la Direttiva NIS2, ratificata in Italia con il Decreto legislativo 138/2024, che coinvolge BDP in qualità di operatore telefonico e il Regolamento Europeo D.O.R.A. 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario.

Lo scopo della presente politica è di proteggere da tutte le minacce, interne o esterne, intenzionali o accidentali, il patrimonio informativo dell'azienda.

Il presente documento è destinato a tutti i dipendenti e collaboratori dell'azienda.

Esso sarà applicato anche alle parti interessate coinvolte nel trattamento delle informazioni alle quali si richiede di implementare parte delle politiche definite.

Tutti i soggetti destinatari sono responsabili dell'attuazione della presente politica, con il supporto della Direzione Aziendale che ha approvato la politica stessa.

Le informazioni costituiscono beni aziendali che hanno un valore per l'Azienda e devono essere protetti in modo adeguato.

La sicurezza delle informazioni ha il compito di proteggere le informazioni da un ampio numero di minacce in modo da assicurare la continuità del business aziendale, minimizzare i danni e massimizzare il ritorno degli investimenti e delle opportunità commerciali.

La sicurezza delle informazioni, secondo la definizione dello standard ISO 27000, consiste nella salvaguardia della riservatezza, integrità e disponibilità delle informazioni;

Proteggere la sicurezza di un sistema significa:

- ✓ ridurre ad un valore accettabile la probabilità che vengano violati i parametri di sicurezza informatica;
- ✓ individuare tempestivamente quando ed in quale parte del sistema questo accade;
- ✓ limitare i danni e ripristinare i requisiti violati nel minor tempo possibile.

In accordo con le indicazioni dello standard ISO 27001, la protezione viene effettuata attraverso un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), con il quale si intende l'insieme delle misure tecniche ed organizzative volte ad assicurare la protezione della riservatezza, integrità e disponibilità delle informazioni.

I principi che l'azienda sceglie di seguire ed applicare nel perseguire la sicurezza delle informazioni sono:

a) gestione dei rischi ICT secondo framework robusti che ne garantiscano governance e controllo;
b) gestione degli incidenti di ogni genere e in particolare degli incidenti ICT, con processi strutturati e noti e con reportistica il più possibile standardizzata, in modo da velocizzare i tempi di risposta;
c) la sicurezza deve essere continuamente tenuta sotto controllo, gli incidenti devono essere rilevati e gestiti
d) business continuity management e pianificazione di test di resilienza operativa adeguati alla realtà aziendale, periodici e supportati da piani di test di diverso livello di complessità correlati alle valutazioni formalizzate nella BIA e supportati di procedure di recovery;
e) le misure di sicurezza devono essere allineate ai requisiti di business aziendali, conformi alle normative vigenti e agli obblighi contrattuali;
f) gestione del rischio dei fornitori di servizi ICT e dei collaboratori esterni, in modo da stabilire solide relazioni contrattuali di impegno e responsabilità con le terze parti che operano nella filiera di fornitura del servizio ICT erogato;
g) le misure di sicurezza (controlli) da applicare sono identificati a seguito di un processo di valutazione del rischio, con criteri condivisi di accettazione del rischio, in modo da mantenere bilanciato il rapporto tra i costi dei controlli ed il costo del relativo rischio;
h) la sicurezza è un processo per il quale tutto il personale aziendale deve essere formato al fine di accrescere la consapevolezza individuale, che unita ad un utilizzo responsabile delle risorse, svolge un ruolo fondamentale nel conseguimento degli obiettivi prefissati;
i) le misure di sicurezza devono essere semplici da comprendere, al fine di favorirne l'applicazione;
j) nell'ambito dei servizi erogati la sicurezza deve essere pianificata ed integrata in tutte le fasi, a partire da quelle iniziali di progettazione e sviluppo;
k) le autorizzazioni all'accesso alle informazioni devono essere basate sul principio del "need-to-know" correlato al business aziendale
l) la condivisione delle informazioni e dell'analisi delle minacce informatiche tra aziende coinvolte nello stesso perimetro, secondo indicazioni provenienti dalle autorità di competenza, vale come punto di forza finalizzato a migliorare la capacità collettiva di risposta a tali minacce

La Sicurezza delle Informazioni, intesa come protezione delle caratteristiche di Riservatezza, Integrità e Disponibilità (Continuità del Servizio) è considerato un fattore critico di successo su cui l'azienda pone la massima attenzione, sia per le caratteristiche stesse dei servizi che per il posizionamento nel mercato.

A tal fine l'azienda si è dotata di un sistema di gestione della sicurezza delle informazioni (SGSI) che in accordo con i principi sopraelencati e con lo scopo di contenere tali rischi a livelli accettabili e di risultare competitivi nei costi prevede il raggiungimento dei seguenti obiettivi:

a) essere conformi alle normative di legge (a titolo esemplificativo e non esaustivo, al D.Lgs. 196/03, al Regolamento UE 2016/679, al D.Lgs. 231/01 e ss.mm.ii., al Decreto NIS2 e al Regolamento UE DORA), agli standard e regolamenti di settore e ai requisiti contrattuali dei clienti;
b) mantenere un sistema di sicurezza aziendale allineato a buone pratiche e standard internazionali, dandone evidenza alle parti interessate;
c) verificare, mediante un processo di valutazione e gestione del rischio, il continuo allineamento strategico degli obiettivi di sicurezza con il business aziendale;
d) diffondere in azienda una cultura della sicurezza delle informazioni;
e) considerare il miglioramento continuo quale pratica per il mantenimento di un adeguato livello di sicurezza.

La Direzione dell'azienda condivide i Principi e gli Obiettivi per la Sicurezza delle Informazioni sopra descritti e supporta pienamente un programma per la loro attuazione e mantenimento.

La Direzione dell'azienda approva ed emette il presente documento di Politica, quale documento programmatico per la Sicurezza delle Informazioni. L'attuazione di tale Politica sarà facilitata attraverso norme e procedure appropriate.

Saranno perseguite nelle opportune sedi le azioni che, disattendendo le indicazioni della presente Politica in modo intenzionale o riconducibile a negligenza, provocheranno un danno all'azienda.

La presente politica viene riesaminata regolarmente per garantirne l'idoneità rispetto alle finalità dell'azienda ed alle aspettative delle parti interessate.

Versione	Data	Redazione	Verifica	Approvazione	TLP
3	11/11/2024	Compliance	CISO	AD	**VERDE**