Brescia
Infrastrutture

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

(Documento approvato dal Consiglio di Amministrazione in data 11/05/2021)

REV.	DATA	REDATTO	AUTORIZZATO	DESCRIZIONE VARIAZIONI APPORTATE
00	11/05/2021	RSGQ	Presidente del CdA	Prima emissione.

Il Sistema di Gestione di Sicurezza delle Informazioni di Brescia Infrastrutture S.r.l.

1. DICHIARAZIONE DI PRINCIPIO

La Politica di Sicurezza delle Informazioni in Brescia Infrastrutture S.r.l. ha l'obiettivo di proteggere le risorse informative da tutte le minacce, siano esse organizzative o tecnologiche, interne o esterne, accidentali o intenzionali.
A tal fine, Brescia Infrastrutture S.r.l. approva il presente documento finalizzato a:

- garantire la riservatezza delle informazioni;
- mantenere l'integrità delle informazioni;
- assicurare la disponibilità dei servizi informatici;
- rispettare i requisiti normativi, legislativi e le regole interne;
- formare il personale alla sicurezza delle informazioni;
- tenere traccia e studiare qualsiasi incidente, reale o presunto, che interessi la sicurezza delle informazioni;
- stabilire regole, elaborare piani e adottare misure per attuare la migliore politica di sicurezza delle informazioni;
- indicare l'Organo Amministrativo quale responsabile della attuazione della Politica di sicurezza delle informazioni;
- stabilire che i Dirigenti ed i Responsabili di Area/U.O. sono responsabili nei rispettivi servizi e funzioni, della applicazione e del rispetto della Politica di sicurezza delle informazioni;
- assegnare ad ogni operatore di Brescia Infrastrutture S.r.l, dipendente e/o collaboratore, la responsabilità per il rispetto della politica di sicurezza delle informazioni.

2. ASPETTI GENERALI

La Politica di sicurezza delle informazioni di Brescia Infrastrutture S.r.l. è attuata per proteggere, per quanto possibile e comunque ad un livello ottimale e ad un costo compatibile con le specificità dell'Azienda, il Sistema di gestione delle informazioni, da eventi intesi come *minacce* o *incidenti*, esterni e/o interni, oggettivi e/o soggettivi, che possono compromettere l'erogazione dei servizi.
Lo scopo di questo documento è indicare le esigenze, gli obiettivi, le finalità, ed i modelli organizzativi della strategia di sicurezza che Brescia Infrastrutture S.r.l. intende perseguire, al fine di orientare lo sviluppo, la gestione, il controllo e la verifica dell'efficacia della sua attuazione.

2.1 Esigenza di una politica della sicurezza delle informazioni

Brescia Infrastrutture S.r.l. è una società di gestione patrimoniale che si occupa di progettazione e realizzazione delle infrastrutture di proprietà della città di Brescia. E' una società a responsabilità limitata con socio unico il Comune di Brescia, che le ha conferito un patrimonio immobiliare e infrastrutturale, fra cui la Metropolitana Leggera Automatica di Brescia ed i Parcheggi in struttura.

Dal momento che le informazioni gestite possono essere soggette ad *intrusioni* risulta necessaria una politica di sicurezza delle informazioni che consenta di proteggerne l'integrità e l'autenticità.

2.2 Scopo

E' obiettivo di assoluta priorità per Brescia Infrastrutture S.r.l. salvaguardare la sicurezza del proprio sistema informativo e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.

In tale contesto, si intende per:

- Riservatezza: la garanzia che una determinata informazione sia preservata da accessi impropri e sia utilizzata esclusivamente dai soggetti autorizzati.
- Integrità: la garanzia che ogni informazione sia realmente quella originariamente inserita nel sistema informatico e sia stata modificata in modo legittimo da soggetti autorizzati.
- Disponibilità: la garanzia di reperibilità dell'informazione in relazione alle esigenze di continuità di erogazione del servizio e di rispetto delle norme che ne impongono la conservazione sicura.
- Autenticità: la garanzia che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che l'ha trasmessa.

Brescia Infrastrutture S.r.l. pone a base della politica di tutela delle informazioni, una idonea Analisi dei Rischi di tutte le risorse (asset) che costituiscono il sistema di gestione delle informazioni, al fine di comprendere le vulnerabilità, di valutare le possibili minacce e di predisporre le necessarie contromisure.

La consapevolezza che non è possibile ottenere, in ambito informatico come del resto in natura, una condizione di sicurezza assoluta, comporta che lo scopo della politica di sicurezza delle informazioni è quello di gestire il rischio ad un livello accettabile attraverso la progettazione, l'attuazione ed il mantenimento di un "Sistema di Gestione della Sicurezza delle Informazioni" (SGSI).

2.3 Campo di applicazione e destinatari

La politica di sicurezza delle informazioni è valida per l'intera Azienda.

La politica si applica a tutte le informazioni trattate nell'ambito sopra definito, qualsiasi natura e forma esse abbiano o prendano, e a tutti i sistemi di gestione e supporti di memorizzazione utilizzati per il loro trattamento e conservazione.

I destinatari della politica sono tutti i collaboratori di Brescia Infrastrutture S.r.l. dipendenti o consulenti, a tempo pieno e a tempo determinato. Sono tenuti al rispetto della politica tutti i soggetti che a vario titolo fruiscono dei servizi informativi di Brescia Infrastrutture S.r.l., nonché i visitatori e gli ospiti.

In particolare, sono tenuti al rispetto della politica di sicurezza, i fornitori di servizi informatici (ad esempio Brescia Mobilità S.p.A.) per la loro tipica condizione di operare direttamente sui sistemi di gestione delle informazioni.

2.4 Obiettivi

- Garantire un adeguato livello di consapevolezza del personale e dei collaboratori, attraverso appositi corsi previsti nel "*Piano annuale di*

Formazione", circa la loro responsabilità rispetto alla sicurezza delle informazioni;
- Garantire un adeguato livello di consapevolezza dei fornitori esterni al fine di assicurare il rispetto dei requisiti di sicurezza delle informazioni;
- Mantenere allineato l'SGSI rispetto ai cambiamenti nelle procedure interne;
- Garantire un livello adeguato dei requisiti di riservatezza, integrità e disponibilità nei servizi erogati attraverso specifici applicativi.

2.5 Revisione, controllo e gestione dei cambiamenti

L'Organo Amministrativo è responsabile della revisione periodica della politica affinché sia allineata agli eventuali e significativi cambiamenti intervenuti nell'organizzazione e/o nelle tecnologie utilizzate per la protezione delle informazioni.
La revisione sarà fatta secondo necessità, in occasione di significative modifiche organizzative e/o tecnologiche rilevanti per la gestione delle informazioni.

3. CONTINUITA' OPERATIVA

La responsabilità della "Continuità Operativa" di Brescia Infrastrutture S.r.l. è dell'Amministratore di Sistema Brescia Mobilità S.p.A. che predispone il *"Piano di Continuità di Servizio" (Business Continuity Plan - BCP)*, inteso come indicazione delle attività organizzative e tecnologiche, finalizzate alla continuità dei processi che concorrono alla missione dell'Azienda.

3.1 Obiettivo

L'obiettivo della Gestione della Continuità Operativa è assicurare la continuità dei processi/servizi essenziali di un'organizzazione (processi critici) ad un determinato livello di servizio, nell'eventualità di un evento disastroso.

3.2 Requisiti per l'operatività

Brescia Infrastrutture S.r.l. mediante le precauzioni contenute nel BCP ritiene di poter contenere l'impatto di eventuali avvenimenti disastrosi, nell'ambito dei requisiti di ripristino definiti.
L'Azienda riconosce che i sistemi di elaborazione delle informazioni sono elementi di criticità per la corretta erogazione dei servizi e una loro prolungata indisponibilità risulta essere altamente dannosa per l'operatività dell'Azienda.

3.3 Elementi di pianificazione

Le metodologie che consentono di redigere, realizzare e mantenere un BCP sono diverse e fanno riferimento a standard emanati da importanti istituti internazionali. Gli elementi comuni a tutti gli standard sono:

- identificazione delle strutture di coordinamento della strategia di ripristino; in Brescia Infrastrutture S.r.l. è il Direttore la figura identificata per la gestione dell'evento disastroso, congiuntamente all'Amministratore di Sistema Brescia Mobilità S.p.A.;

- valutazione dei risultati della Analisi dei rischi per l'individuazione dei processi e dei servizi critici e delle priorità di intervento;
- predisposizione delle procedure da effettuare in caso di attuazione del BCP;
- sviluppo, documentazione e verifica del BCP. Brescia Infrastrutture S.r.l. chiederà all'Amministratore di Sistema Brescia Mobilità S.p.A., la verifica del BCP annualmente e comunque a seguito di significativi cambiamenti degli elementi che lo compongono.

4. INVENTARIO DELLE RISORSE INFORMATICHE

4.1 Obiettivo

Identificare, classificare e registrare le risorse hardware e software utilizzate da Brescia Infrastrutture S.r.l., al fine di tracciare l'intero "ciclo di vita": acquisizione, assegnazione, aggiornamento, manutenzione, dismissione.
L'inventario delle risorse informatiche è necessario per monitorare l'obsolescenza delle risorse utilizzate, pianificare il loro ammodernamento, rinnovare le licenze e programmare gli investimenti in tecnologie dell'informazione.

4.2 Inventario

Brescia Infrastrutture S.r.l. è dotata di un "Inventario informatizzato delle risorse informatiche" che compongono il sistema di gestione delle informazioni e la gestione è affidata al "Referente della informatizzazione interna e gestione infrastrutture informatiche", mentre la responsabilità è in capo al Direttore.

4.3 Inventario hardware

Le risorse hardware sono classificate e per ciascuna di esse sono definite le caratteristiche tecniche, il fornitore da cui sono state acquisite, l'anno e la modalità di acquisizione, ecc., utili sia per una corretta gestione delle garanzie, sia per una gestione efficace della manutenzione e/o aggiornamento.

4.4 Inventario software

I programmi software sono classificati e per ciascuno di essi viene individuata la tipologia, il produttore, il fornitore, e nel caso di acquisizione con licenza d'uso l'anno di acquisizione utile per il pagamento dei relativi canoni di licenza annuali.

5. SICUREZZA FISICA E AMBIENTALE

Costituisce la forma di tutela che attiene alla protezione dei sistemi di elaborazione delle informazioni e si manifesta con misure fisiche dirette a garantire i servizi di controllo contro accessi non autorizzati ai locali ove sono ubicati i sistemi di gestione dell'informazione, al fine di preservare l'integrità e la disponibilità dei sistemi di elaborazione dell'informazione di Brescia Infrastrutture S.r.l.

5.1 Obiettivo
Minimizzare gli impatti delle minacce ai sistemi di elaborazione delle informazioni dovuti a danni o intrusioni.

5.2 Sicurezza delle aree
Le aree che comprendono i locali ove risiedono i sistemi di gestione dell'informazione dell'Azienda, sono dotate di porte ad accesso controllato.

5.3 Sicurezza dei locali
I locali sono dotati di sistemi, atti a garantire e mantenere la sicurezza e l'integrità delle apparecchiature e degli impianti, al fine di evitare guasti che possono causare interruzione fisica al funzionamento delle attività.

5.4 Controllo accessi ai locali
Tutti i sistemi e apparecchiature di rete sono ubicati in edifici sicuri e con accesso vigilato.

6. CONTROLLO DEGLI ACCESSI LOGICI

6.1 Obiettivo
Impedire accessi non autorizzati e proteggere le informazioni ed i sistemi di elaborazione e di comunicazione con misure tecnologiche ed organizzative atte a garantire il controllo degli accessi, la qualità delle informazioni, nonché la loro riservatezza ed integrità.

6.2 Accesso ai sistemi e alle applicazioni

Regola dell'accesso
I collaboratori interni ed i soggetti esterni (utenti), devono accedere solo ai sistemi a cui sono stati autorizzati. Ogni abuso di accesso a sistemi diversi da quelli autorizzati, è perseguito ai sensi dell'articolo 615-ter del Codice Penale "Accesso abusivo ad un sistema informatico o telematico.

Accesso alle applicazioni (autorizzazioni)
Brescia Infrastrutture S.r.l. abilita i fornitori con i quali è in essere un contratto, ad essere autorizzati, se del caso, ad accedere ad alcune cartelle di Drive oppure all'applicativo Archibus. Il "Referente della informatizzazione interna e gestione infrastrutture informatiche" controlla periodicamente, almeno una volta all'anno, la validità funzionale di tutte le autorizzazioni attive alle cartelle di Drive e del software Archibus. La revoca all'accesso alla cartella di Drive o al software Archibus del fornitore esterno viene attuata qualora decadano le caratteristiche di abilitazione di un utente.

Caratteristiche e gestione delle password
Brescia Infrastrutture S.r.l. considera la password, conformemente alle norme di sicurezza informatica, come una "informazione confidenziale di

autenticazione composta da una serie di caratteri e/o simboli", utilizzata per l'accesso ai sistemi di elaborazione dell'informazione.
Brescia Infrastrutture S.r.l. assegna password individuali e l'utente è responsabile della sua riservatezza. Le password hanno una durata di 90 giorni.

7. GESTIONE SOFTWARE SU LICENZA

Brescia Infrastrutture S.r.l. acquisisce i software tramite pagamento delle relative licenze ed autorizza i collaboratori, utenti e amministratori, al loro uso.
Nel caso una risorsa necessiti di una installazione di software aggiuntivi, deve esserne fatta specifica richiesta al "Referente della informatizzazione interna e gestione infrastrutture informatiche" che approva il ticket di richiesta oppure la mail.

8. BACK UP DEI DATI ED USO DEI DISPOSITIVI DI MEMORIZZAZIONE

Eventi dannosi dovuti ad errori accidentali possono comportare perdita di dati conservati sul computer con ripercussioni anche gravi sull'attività lavorativa e sull'erogazione dei servizi.
Al fine di evitare il rischio di perdita di dati importanti, i dipendenti sono invitati a salvare periodicamente i dati sul personal computer, nelle cartelle di rete esistenti.

9. SICUREZZA DELLE RETI E DELLE COMUNICAZIONI

Per garantire la sicurezza delle reti e delle comunicazioni occorre prevenire l'accesso alle reti e l'utilizzo illegale di informazioni, da parte di soggetti non autorizzati al fine di preservare la riservatezza dei dati e la disponibilità del servizio.
Il documento *"Obblighi specifici del dipendente in materia di privacy durante l'utilizzo degli strumenti informatici aziendali"* contiene le raccomandazioni sulla sicurezza della rete interna, le regole per la navigazione in Internet e le indicazioni per l'uso appropriato della posta elettronica e la protezione contro il software malevolo.

10. GESTIONE DEGLI INCIDENTI

Un incidente, nell'ambito della sicurezza dell'informazione, è un evento sospetto o una vulnerabilità tale da violare l'integrità, la riservatezza e/o la disponibilità delle applicazioni, dei dati e/o dei sistemi di elaborazione delle informazioni.
Tutti gli utenti devono attenersi alle indicazioni ricevute in materia di sicurezza delle informazioni e contenute nei documenti: "*Obblighi specifici del dipendente in materia di privacy durante l'utilizzo degli strumenti informatici aziendali"* e "*Obblighi specifici del dipendente in materia di privacy durante l'utilizzo degli archivi cartacei aziendali"*.
I dipendenti che individuano o abbiano il sospetto riguardante un incidente al sistema di sicurezza, devono segnalarlo tempestivamente al Data Protection

Officer aziendale, al Direttore e al "Referente della informatizzazione interna e gestione infrastrutture informatiche".

11. UTILIZZO CHIAVETTE USB

Il Direttore incentiva la limitazione dell'utilizzo delle chiavette usb ai dipendenti e ai fornitori per lo scambio di documentazione digitale. Entro il 31.12.2021 si formalizzerà l'eliminazione delle chiavette usb, attraverso appositi eventi formativi, incentivando l'utilizzo della piattaforma Drive e a seguito di suo adeguato potenziamento.

12. FURTO/DIFFUSSIONE DI PATRIMONIO INTELLETTUALE

L'aumento del numero di personale e l'aumento di importanza della Società pongo il tema del furto del patrimonio intellettuale e della sua potenziale diffusione al centro dell'attenzione. Il Risk manager aziendale, il Direttore, i Responsabili di Area/U.O. e l'Organo Amministrativo vigilano sul comportamento del personale dipendente attuando presidi e azioni di miglioramento.

BRESCIA INFRASTRUTTURE S.r.l.

Il Presidente del Consiglio di Amministrazione

f.to Ing. Marcello Peli