Via Gramsci 25
27100, Pavia
PI 01606500187
0382/413825
commerciale@bls.it
www.bls.it

Politica per la Sicurezza delle informazioni

Premessa Generale

BLS Consulting S.r.l. (d'ora in avanti BLS) è nata per supportare le aziende e le P.A. nei processi di innovazione e transizione digitale e opera nei seguenti ambiti:

- sicurezza informatica
- progettazione e realizzazione di sistemi informatici, reti locali, metropolitane e geografiche, smartcity
- servizi cloud IaaS e SaaS
- assistenza ai clienti

BLS, accompagna le organizzazioni nell'adozione delle migliori pratiche e dei nuovi modelli organizzativi determinati dalla trasformazione digitale.

BLS eroga i servizi dalla sede operativa situata in Pavia mentre l'infrastruttura tecnologica per l'erogazione dei servizi ai propri clienti in modalità IaaS e SaaS è dislocata in due data center:

- Data4 Milano situato a Cornaredo/MI: uno dei più evoluti e affidabile data center in Italia (99,999% disponibilità dei servizi, nessuna interruzione di servizio nella sua storia, completa assenza di rischi naturali, ambientali, sociali e aerei)

- IT.NET situato a Roma: usato come data center di disaster recovery (99,999% disponibilità dei servizi, completa assenza di rischi naturali, ambientali, sociali e aerei)

I due siti sono collegati con modalità che garantiscono elevati standard di sicurezza (collegamenti in fibra 99,999% garantita, doppio provider, BGP, linea dedicata per il collegamento tra i data center)

Tutti i fornitori sono certificati ISO 9001 e 27001 e i data center sono certificati ANSI TIA 942 TIER IV.

Doc ID: bf7fe20a77e4398953308c3d7e13d8929aaca9bd

Via Gramsci 25
27100, Pavia
PI 01606500187
0382/413825
commerciale@bls.it
www.bls.it

Dichiarazione sulla politica aziendale per la sicurezza delle Informazioni

BLS ritiene che la sicurezza delle informazioni rappresenti un fattore critico sia per quanto riguarda i processi di progettazione e sviluppo di soluzioni tecnologiche che per quanto riguarda l'erogazione dei servizi.

Per BLS la gestione della sicurezza delle informazioni ha come obiettivo primario la protezione dei dati al fine di tutelare il patrimonio rappresentato dalle conoscenze aziendali, quello dei propri clienti e delle persone fisiche di cui si trattano i dati personali.

Per le caratteristiche dei servizi che BLS offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business, la politica della sicurezza delle Informazioni rappresenta un indirizzo strategico fondamentale e prioritario.
La politica della sicurezza delle Informazioni definisce e organizza la riservatezza, l'integrità, la confidenzialità e disponibilità dei dati e dei servizi.

La politica per la sicurezza delle informazioni per BLS è costituita da un insieme di attività che comprendono:
l'identificazione degli asset primari, la gestione dei rischi, dei sistemi e della rete, l'identificazione delle vulnerabilità e degli incidenti, il controllo degli accessi, la gestione della privacy e della compliance, la valutazione dei danni e tutti gli altri aspetti che possono impattare sulla gestione della sicurezza delle informazioni.

Per perseguire questo obiettivo BLS, attraverso un approccio by design, pone grande attenzione alla progettazione, alla gestione e alla manutenzione della propria struttura tecnologica, fisica, logica ed organizzativa.

BLS impegna quindi la propria organizzazione a sviluppare e manutenere un sistema di gestione della sicurezza delle informazioni nell'ambito delle attività svolte e dei servizi erogati al fine di garantire la disponibilità l'integrità e la riservatezza dei dati.

Tutte le persone che lavorano e/o collaborano con BLS sono impegnate a rispettare i seguenti principi:

1. Riservatezza: per assicurare che le informazioni siano accessibili solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;

2. Integrità: per salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;

3. Disponibilità: per assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta e salvaguardia quindi il patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati;

4. Privacy: per garantire la protezione ed il controllo dei dati personali.

Doc ID: bf7fe20a77e4398953308c3d7e13d8929aaca9bd

Via Gramsci 25
27100, Pavia
PI 01606500187
0382/413825
commerciale@bls.it
www.bls.it

La Direzione è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con BLS nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati.
In particolare, questo obiettivo è perseguito attraverso l'impegno a garantire:

- il rispetto delle leggi e normative vigenti;
- l'efficienza operativa e affidabilità dei processi di sviluppo prodotti e servizi correlati;
- le condizioni di salute e sicurezza sui luoghi di lavoro per il personale e per i collaboratori;
- la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o casuali sulla sicurezza dei dati/informazioni gestite;
- la protezione dei mezzi resi disponibili, ed il loro corretto utilizzo;
- la riservatezza, la correttezza e la disponibilità delle informazioni gestite da BLS e la salvaguardia della proprietà intellettuale;
- l'adozione di misure di prevenzione di anomalie di processo/prodotto/servizio.

Doc ID: bf7fe20a77e4398953308c3d7e13d8929aaca9bd

Via Gramsci 25
27100, Pavia
PI 01606500187
0382/413825
commerciale@bls.it
www.bls.it

Il sistema di Gestione della Sicurezza della Informazioni (SGSI)

Per dare attuazione alla propria politica della sicurezza delle informazioni, BLS, ha sviluppato e si impegna a mantenere un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della Norma ISO/IEC 27001 e delle estensioni ISO/IEC 27017 e ISO/IEC 27018 come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

Nell'ambito della gestione dei servizi offerti, BLS, assicura:

- l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione SGSI
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza per la propria infrastruttura tecnologica e organizzativa
- fornisce la garanzia di selezionare partner affidabili dal punto di vista della gestione in sicurezza delle informazioni e della protezione dei dati personali.

La politica per la sicurezza delle informazioni di BLS si applica a tutto il personale interno e quello delle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

La politica della sicurezza di BLS rappresenta in concreto l'impegno dell'organizzazione nei confronti di clienti e delle terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

In sintesi, la politica della sicurezza delle informazioni di BLS garantisce che:

1. l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti di volta in volta la loro criticità, al fine di agevolare l'implementazione di adeguati livelli di protezione;
2. l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
3. l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
4. l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
5. le anomalie e gli incidenti aventi ripercussioni sul sistema informativo, sui servizi e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business;
6. l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
7. la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
8. la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
9. la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite;
10. i trattamenti dei dati personali, sia nei casi in cui BLS operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvenga nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016.

Doc ID: bf7fe20a77e4398953308c3d7e13d8929aaca9bd

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso un riesame annuale, per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso la sua pubblicazione sul sito.

Backup dei dati

BLS effettua i backup dei propri server secondo la più opportuna politica e con le opportune retention, inoltre effettua i backup delle macchine virtuali dei clienti in base ai piani di backup concordati commercialmente.
I backup vengono almeno una volta a settimana effettuati off-site nel data center di disaster recovery o in sede centrale di BLS.
BLS implementa un sistema automatico di monitoraggio dell'esito dei job di backup con apertura automatica dei ticket in caso di problemi e garantisce la presa in carico e possibilmente la risoluzione di eventuali problemi entro il giorno lavorativo successivo.

Disaster recovery

BLS implementa un piano di disaster recovery che permette avviare i servizi propri e dei clienti che hanno sottoscritto il servizio di disaster recovery.
Almeno annualmente vengono:

- valutati i requisiti di business continuity dei servizi e definiti RPO (Recovery Point Objective) e WRT (Work Recovery Time)
- aggiornato il piano di business continuity e disaster recovery
- effettuate delle prove di disaster recovery

Politiche di accesso

BLS garantisce che ogni accesso, di tipo fisico o informatico, sia autorizzato, controllato e monitorato sulla base dei seguenti criteri:

1. l'accesso è autorizzato al personale abilitato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere);
2. l'accesso è autorizzato al personale abilitato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati);
3. l'accesso alla struttura e ai locali è autorizzato al personale abilitato.

L'accesso ai locali di BLS è autorizzato, controllato e monitorato in linea con la politica aziendale.

Responsabilizzazione del personale

BLS si impegna che tutto il personale sia responsabilizzato all'obbligo di:

1. garantire il rispetto delle norme, leggi e regolamenti vigenti, di natura cogente, contrattuale e volontaria rese applicabili negli ambiti del SGSI;
2. proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite da BLS, la proprietà intellettuale e il patrimonio di BLS o da questa affidati a terze parti;
3. aver cura dei beni materiali, i sistemi e le risorse di BLS;
4. salvaguardare e gestire in modo appropriato ogni informazione e dato afferenti le attività di propria competenza;
5. contattare la Direzione, il Responsabile della Sicurezza delle informazioni e/o altre autorità competenti in caso di effettive o sospette violazioni della sicurezza;
6. segnalare qualsiasi necessità di modifiche alle procedure relative alla gestione della sicurezza delle informazioni.

Via Gramsci 25
27100, Pavia
PI 01606500187
0382/413825
commerciale@bls.it
www.bls.it

Responsabilizzazione di soggetti terzi

BLS si impegna nei confronti di soggetti terzi a:

1. formalizzare il proprio impegno alla riservatezza e non divulgazione delle informazioni tratte negli ambiti di competenza;
2. proteggere le risorse e le informazioni fisiche e intellettuali a cui possono accedere nella effettuazione delle attività assegnate;
3. garantire la piena osservanza ai requisiti del SGSI nei comportamenti e nell'operatività.

Conservazione

BLS conserva i dati in Italia e solo su propri sistemi, non esporta quindi i dati fuori dal territorio Italiano ne cede a terzi i dati (se non su richiesta esplicita dell'autorità giudiziaria). I dati vengono conservati in locali costantemente monitorati e con accesso limitato mediante badge e con log degli accessi.

Trasferimento

Il trasferimento dei dati tra data center e con le sedi del cliente vengono sempre effettuati in modalità criptata.

Accesso ai portatili di gestione

L'accesso ai portali di gestione è protetto con adeguate misure di sicurezza (password, two factor authentication, indirizzo IP da cui viene effettuato l'accesso), superiori ai requisiti di legge. Vengono conservati i log degli accessi a norma di legge (non modificabilità garantita da timestamp secondo normativa Europea EIDAS). I tentativi di accesso vengono identificati e segnalati immediatamente al cliente via email, gli account soggetti ad attacco vengono anche temporaneamente bloccati.

Data breach

Le eventuali violazioni dei dati personali (data breach) vengono comunicate secondo quanto previsto dalla normativa entro 72 ore al Garante per la protezione dei dati personali ed ai clienti interessati.

Incidenti e non conformità

BLS implementa un sistema di gestione degli incidenti secondo gli standard ISO 27035 e ISO 20000-1 che prevede: segnalazione tempestiva al cliente mediante il più opportuno sistema di comunicazione (SMS o email), evidenziazione di eventuali non conformità collegate agli incidenti, adozione di opportune azioni correttive per evitare il ripetersi degli incidenti, produzione di un report post mortem ed invio al cliente, revisione periodica degli incidenti ad opera del security manager.

Analisi del rischio

Nel portale di gestione è disponibile su richiesta del cliente un evoluto sistema per valutare il livello di sicurezza dei dati e identificare le eventuali componenti di rischio. Il sistema mediante un questionario identifica le minacce alla confidenzialità, integrità e disponibilità dei dati e ne valuta il livello di rischio in base alla tipologia di dati.

Doc ID: bf7fe20a77e4398953308c3d7e13d8929aaca9bd

Via Gramsci 25
27100, Pavia
PI 01606500187
0382/413825
commerciale@bls.it
www.bls.it

Copertura assicurativa

BLS ha attiva una copertura assicurativa su eventuali incidenti che riguardano la protezione dei dati personali.
L'assicurazione comprende la responsabilità civile ai sensi del D. Lgs. n. 196 del 30/6/2003 (Codice in materia di dati personali) per perdite patrimoniali cagionate a terzi, compresi i clienti e/o i dipendenti, in conseguenza dell'errato trattamento (raccolta,registrazione, elaborazione, conservazione, utilizzo, comunicazione e diffusione) dei dati personali di terzi.

In conclusione

BLS si impegna a:

- ☐ adottare un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della Norma ISO/IEC 27001:2013 e delle linee guida ISO 27017 e 27018
- ☐ mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI;
- ☐ garantire mezzi e risorse idonee al suo mantenimento e miglioramento continuo, in particolare per quanto attiene la mitigazione/riduzione dei livelli di rischio sulla sicurezza delle informazioni e l'adozione di misure idonee a prevenire situazioni anomale e di emergenza;
- ☐ rendere consapevoli tutte le persone che dell'organizzazione degli obblighi e delle responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche.

La Direzione

Doc ID: bf7fe20a77e4398953308c3d7e13d8929aaca9bd