Politica globale di sicurezza informatica

ISMS-PLS-A05

Azione	Autore	Funzione	Dati
Preparato	Andrea Ceiner	ISM	16/2/2026
Verificato	Lorenzo Savadori	CIO	16/2/2026
Approvato	Leonardo Romanelli	CEO	18/2/2026

SOMMARIO

1 Contesto 3
2 Introduzione 3
3 Ambito 5
4 Miglioramento continuo 5
5 Struttura 5
6 Rischi 5
7 Politica di Sicurezza Informatica 6
8 Organizzazione della sicurezza informatica 6
9 Sicurezza delle risorse umane 7
10 Gestione degli Asset 7
11 Controllo degli accessi 8
12 Crittografia 8
13 Sicurezza fisica 8
14 Sicurezza operativa 8
15 Sicurezza delle comunicazioni 9
16 Acquisizione, sviluppo e manutenzione del sistema 9
17 Rapporto con il fornitore 9
18 Gestione degli incidenti di sicurezza informatica 10
19 Aspetti della sicurezza delle informazioni della continuità del business 10
20 Conformità 10

1 CONTESTO

In quanto azienda moderna orientata al futuro, Bluegreen riconosce ai livelli alti la necessità di garantire che la propria attività funzioni in modo impeccabile e senza interruzioni, a beneficio dei propri clienti, azionisti e altre parti interessate.

Per garantire un tale livello di funzionamento continuo, Bluegreen ha implementato un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) in linea con lo Standard Internazionale per la Sicurezza dell'Informazione, ISO/IEC 27001:2022. Questo standard definisce i requisiti per un ISMS basandosi sulle migliori pratiche riconosciute a livello internazionale.

Il funzionamento dell'ISMS offre molti vantaggi per l'azienda, tra cui:

- Protezione delle fonti di ricavo e della redditività dell'azienda
- Garantire la fornitura di beni e servizi ai clienti
- Mantenimento e potenziamento del valore per gli azionisti
- Conformità ai requisiti legali e normativi.

Una definizione chiara dei requisiti per la sicurezza delle informazioni all'interno di Bluegreen sarà concordata e mantenuta con i clienti interni del business e dei servizi cloud, in modo che tutta l'attività ISMS sia focalizzata sul rispetto di tali requisiti. Saranno inoltre documentati e contributi al processo di pianificazione i requisiti statutari, normativi e contrattuali. I requisiti specifici riguardanti la sicurezza di sistemi o servizi nuovi o modificati saranno raccolti nella fase di progettazione di ciascun progetto.

È un principio fondamentale del Sistema di Gestione della Sicurezza Informatica Bluegreen che i controlli implementati siano guidati dalle esigenze aziendali e che saranno regolarmente comunicati a tutto il personale attraverso riunioni di team e documenti informativi.

2 INTRODUZIONE

2.1 L'organizzazione è definita da Bluegreen srl.

2.2 L'informazione è un bene che l'organizzazione ha il dovere e la responsabilità di proteggere. La disponibilità di informazioni complete e accurate è essenziale per il funzionamento efficiente dell'organizzazione e per fornire prodotti e servizi ai clienti.

2.3 L'organizzazione è consapevole che la riservatezza, l'integrità e la disponibilità degli asset sono un vero valore per l'azienda. È per questo che l'organizzazione ha sviluppato un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) per proteggere i propri asset.

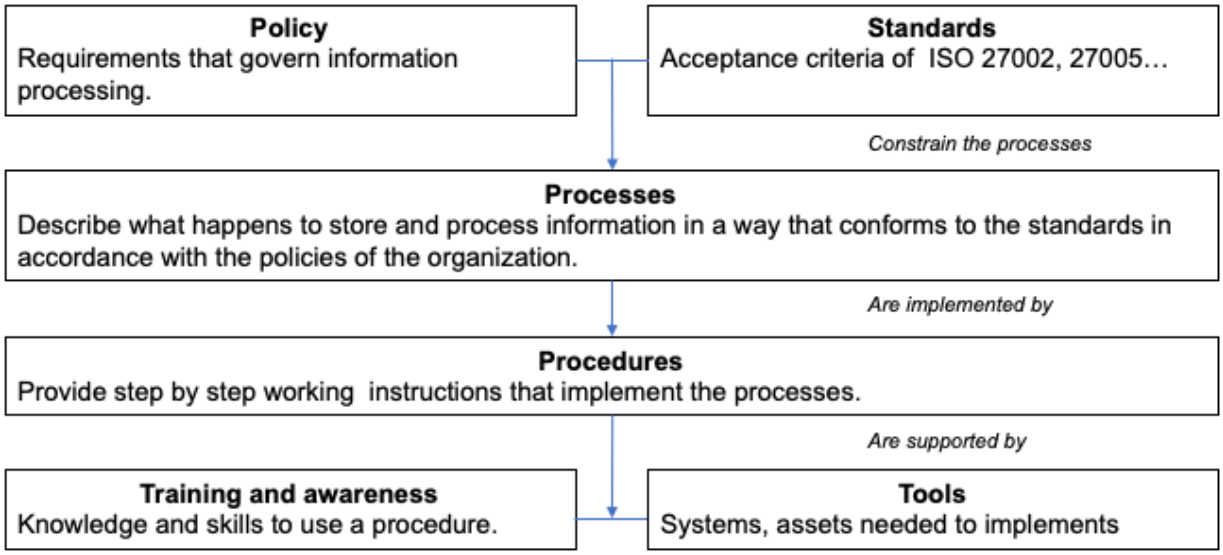
2.4 L'organizzazione detiene e processa informazioni riservate e personali su privati, dipendenti, partner, clienti e fornitori, nonché informazioni relative alle proprie operazioni. Nel trattamento delle informazioni, l'organizzazione ha la responsabilità di proteggerle e prevenirne l'uso improprio.

2.5 Lo scopo e l'obiettivo di questa Politica sulla Sicurezza delle Informazioni è definire un quadro per la protezione degli asset informativi dell'organizzazione:

- proteggere le informazioni dell'organizzazione da tutte le minacce, interne o esterne, deliberate o accidentali,
- per abilitare la condivisione sicura delle informazioni,

- incoraggiare un uso coerente e professionale delle informazioni,
- Per garantire che tutti siano chiari sui propri ruoli nell'uso e nella protezione delle informazioni,
- per garantire la continuità del business e minimizzare i danni aziendali,
- per proteggere l'organizzazione da responsabilità legali e dall'uso inappropriato di
- informazioni.

2.6 La Politica di Sicurezza Informatica è un documento di alto livello e adotta una serie di controlli per proteggere le informazioni. I controlli sono attuati da politiche, standard, processi, procedure, supportati da campagne di sensibilizzazione e formazione, e strumenti.



3 AMBITO

3.1 Questa Politica sulla Sicurezza delle Informazioni delinea il quadro per la gestione della Sicurezza delle Informazioni all'interno dell'organizzazione (vedi 1.1).

3.2 La Politica, gli standard, i processi e le procedure sulla sicurezza informatica si applicano a tutto il personale e ai dipendenti dell'organizzazione, alle terze parti contrattuali e ai loro consulenti che hanno accesso ai sistemi informativi o alle informazioni dell'organizzazione.

3.3 La Politica sulla Sicurezza Informatica si applica a tutte le forme di informazioni, incluse quelle categorie di asset:

- Hardware,
- Software,
- Reti, computer,
- Organizzazione,
- Fisico e locali,
- Dati,
- Diritti degli utenti.

4 MIGLIORAMENTO CONTINUO

4.1 Il miglioramento continuo è un concetto chiave del sistema informativo dell'organizzazione nella misura in cui il sistema informativo evolve e con esso i rischi esogeni ed endogeni ad esso associati.

4.2 Quando possibile, verrà utilizzata la ruota di Deming (PDCA). Così le operazioni saranno pianificate, sviluppate, verificate e adattate.

4.3 Questo miglioramento costante è sostenuto dalla direzione di alto livello e guidato dai vari responsabili di reparto.

4.4 Le varie prerogative in termini di consapevolezza e formazione sono uno strumento essenziale per il miglioramento continuo.

5 STRUTTURA

5.1 Questa politica si basa su ISO 27001(2022) e ISO27002(2022) ed è strutturata per includere i 4 domini e 93 controlli.

5.2 Questa politica è di alto livello integrata da ulteriori politiche di sicurezza che forniscono politiche dettagliate, linee guida e istruzioni di lavoro relative a specifici controlli di sicurezza.

6 RISCHI

6.1 Le informazioni raccolte, analizzate, conservate, comunicate e riportate possono essere soggette a furto, uso improprio, perdita e corruzione.

6.2 Informazioni e risorse possono essere messe a rischio da scarsa istruzione e formazione, uso improprio e violazione dei controlli di sicurezza.

6.3 L'organizzazione effettuerà valutazioni dei rischi per identificare, quantificare e dare priorità ai rischi. I controlli saranno selezionati e implementati per mitigare i rischi identificati.

6.4 Le valutazioni del rischio saranno effettuate utilizzando un approccio sistematico per identificare e stimare l'entità dei rischi.

7 Politica di Sicurezza Informatica

7.1 Il documento della Politica sulla Sicurezza delle Informazioni delinea l'approccio dell'organizzazione alla gestione della sicurezza delle informazioni.

7.2 La Politica sulla Sicurezza Informatica è approvata dalla direzione ed è comunicata a tutto il personale e i dipendenti dell'organizzazione, ai terzi contrattuali e agli agenti dell'organizzazione.

7.3 I requisiti di sicurezza per l'organizzazione saranno rivisti almeno una volta all'anno dal Responsabile della Sicurezza delle Informazioni e approvati dal Consiglio. Verranno presentate richieste formali di modifiche per l'incorporazione nella Politica, nei processi e nelle procedure di Sicurezza Informatica.

8 Organizzazione della sicurezza informatica

8.1 È politica dell'organizzazione garantire che le informazioni siano protette dalla perdita di:

- Riservatezza: affinché le informazioni siano accessibili solo a individui autorizzati.
- Integrità: salvaguardare l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione.
- Disponibilità: che gli utenti autorizzati abbiano accesso alle informazioni rilevanti quando necessario.

8.2 Il Responsabile della Sicurezza delle Informazioni esamina e formula raccomandazioni sulla politica di sicurezza, gli standard politici, le direttive, le procedure, la gestione degli incidenti e l'educazione alla consapevolezza della sicurezza.

8.3 I requisiti normativi, legislativi e contrattuali saranno incorporati nella Politica, nei processi e nelle procedure di sicurezza informatica.

8.4 I requisiti della Politica, dei processi e delle procedure di Sicurezza Informatica saranno incorporati nelle procedure operative e negli accordi contrattuali dell'organizzazione.

8.5 L'organizzazione lavorerà per implementare gli standard ISO27000, gli Standard Internazionali per la Sicurezza delle Informazioni.

8.6 Saranno fornite indicazioni su cosa costituisca un Incidente di Sicurezza Informatica.

8.7 Tutte le violazioni della sicurezza informatica, reali o sospette, devono essere segnalate e saranno indagate.

8.8 I piani di continuità operativa saranno prodotti, mantenuti e testati.

8.9 L'educazione e la formazione sulla sicurezza informatica saranno disponibili a tutto il personale e i dipendenti.

8.10 Le informazioni conservate dall'organizzazione saranno appropriate ai requisiti aziendali e normativi, come quelli relativi alla privacy dei dati.

8.11 La sicurezza delle informazioni sarà gestita all'interno di un quadro approvato attraverso l'assegnazione dei ruoli e il coordinamento dell'implementazione di questa politica di sicurezza in tutta l'organizzazione e nei rapporti con terze parti.

8.12 Vi saranno utilizzati consigli esterni specialistici, dove necessario, per mantenere la Politica, i processi e le procedure di Sicurezza Informatica per affrontare minacce e standard nuovi ed emergenti.

8.13 Il Responsabile della Sicurezza Informatica è il proprietario designato della Politica sulla Sicurezza Informatica ed è responsabile della manutenzione e della revisione della Politica, dei processi e delle procedure sulla Sicurezza Informatica.

8.14 I capi dipartimento sono responsabili di garantire che tutto il personale e i dipendenti, le terze parti contrattuali e gli agenti dell'organizzazione siano informati e rispettino la Politica, i processi e le procedure di Sicurezza Informatica.

8.15 I revisori dell'organizzazione esamineranno l'adeguatezza dei controlli implementati per proteggere le informazioni dell'organizzazione e raccomanderanno miglioramenti dove emergano carenze.

8.16 Tutto il personale e i dipendenti dell'organizzazione, le terze parti contrattuali e gli agenti dell'organizzazione che accedono alle informazioni dell'organizzazione sono tenuti ad aderire alla Politica, ai processi e alle procedure di Sicurezza Informatica.

8.17 Il mancato rispetto della Politica, dei processi e delle procedure sulla sicurezza delle informazioni comporterà azioni disciplinari o correttive.

9 SICUREZZA DELLE RISORSE UMANE

9.1 Le politiche di sicurezza dell'organizzazione saranno comunicate a tutti i dipendenti, ai collaboratori e a terzi per garantire che comprendano le proprie responsabilità.

9.2 Le responsabilità di sicurezza saranno incluse nelle descrizioni del lavoro e nei termini e condizioni di lavoro.

9.3 Verranno effettuati controlli di verifica su tutti i nuovi dipendenti, collaboratori e terze parti.

10 GESTIONE DEGLI ASSET

10.1 Le risorse dell'organizzazione saranno adeguatamente identificate e inventariate.

10.2 I beni dell'organizzazione saranno adeguatamente protetti in base ai risultati delle valutazioni del rischio.

10.3 Tutti i beni (dati, informazioni, software, apparecchiature informatiche e di comunicazione, servizi e persone) saranno contabilizzati e avranno un proprietario.

10.4 I proprietari saranno identificati per tutti gli asset e saranno responsabili della manutenzione e protezione dei loro beni rispetto e del rispetto della metodologia di gestione del rischio.

10.5 Le informazioni saranno classificate in base ai requisiti di criticità e sensibilità.

10.6 Ogni informazione sarà etichettata utilizzando lo schema di classificazione dell'organizzazione.

11 CONTROLLO DEGLI ACCESSI

11.1 L'accesso a tutte le informazioni sarà controllato e in base alla Politica di Classificazione.

11.2 La gestione degli accessi si baserà sul principio del bisogno di conoscere.

11.3 L'accesso alle informazioni e ai sistemi informativi sarà guidato dalle esigenze aziendali. L'accesso sarà concesso, o saranno stipulati accordi per dipendenti, partner e fornitori in base al loro ruolo, solo a un livello che consenta loro di svolgere i loro compiti.

11.4 Sarà implementata una procedura formale di registrazione e disregistrazione di utenti/account per l'accesso a tutti i sistemi e servizi informativi.

11.5 Gli account privilegiati saranno utilizzati solo per gli scopi che richiedono il loro utilizzo.

12 CRITTOGRAFIA

12.1 Ovunque possibile, l'uso della crittografia è la regola di base.

12.2 Verrà impostata una procedura di gestione delle chiavi basata su un ciclo di vita e i requisiti di archiviazione.

13 SICUREZZA FISICA

13.1 Le strutture critiche o sensibili per l'elaborazione delle informazioni saranno ospitate e conservate in aree sicure.

13.2 Le aree sicure saranno protette da perimetri di sicurezza definiti con barriere di sicurezza e controlli d'ingresso appropriati.

13.3 Le informazioni critiche e sensibili saranno protette fisicamente da accessi non autorizzati, danni e interferenze.

14 SICUREZZA OPERATIVA

14.1 Le procedure operative saranno trasmesse a tutti i dipendenti coinvolti in questioni di sicurezza dirette o indirette.

14.2 La gestione del cambiamento eseguirà vincoli di sicurezza come la valutazione del rischio, la valutazione degli effetti collaterali sulla sicurezza e sarà controllata dal Responsabile della Sicurezza Informatica.

14.3 Sarà presa in considerazione la gestione delle capacità e le risorse saranno monitorate.

14.4 Gli ambienti saranno separati in termini di sviluppo, accettazione e produzione.

14.5 Rilevare malware e software dannosi sarà un miglioramento continuo durante le operazioni.

14.6 Strumenti per la prevenzione di malware e software dannosi saranno installati in ogni nood strategico.

14.7 L'organizzazione garantisce che un piano di riserva sia in atto.

14.8 La gestione della registrazione degli eventi sarà stabilita con un piano speciale per gli utenti o account con ampi diritti.

14.9 Verranno implementate soluzioni di monitoraggio in base alla criticità degli eventi.

14.10 L'organizzazione presta particolare attenzione alla sincronizzazione degli orologi e stabilirà controlli in tal senso.

14.11 Per prevenire lo sfruttamento delle vulnerabilità tecniche, le organizzazioni elaboreranno un piano per raccogliere, valutare e testare le vulnerabilità tecniche.

14.12 Verranno effettuati audit regolari per valutare i rischi e ridurre la superficie di attacco.

15 SICUREZZA DELLE COMUNICAZIONI

15.1 L'organizzazione gestirà in modo sicuro i propri impianti di elaborazione delle informazioni.

15.2 Saranno stabilite responsabilità e procedure per la gestione, l'operatività e la sicurezza e disponibilità continua di tutte le strutture di elaborazione dati e informazioni.

15.3 Verranno introdotte procedure operative appropriate.

15.4 La segregazione dei doveri sarà implementata, dove opportuno, per ridurre il rischio di uso negligente o deliberato del sistema

15.5 Il trasferimento delle informazioni si baserà su una Politica di Classificazione che determinerà come le informazioni dovranno essere trasferite sia internamente che esternamente.

16 ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEL SISTEMA

16.1 I requisiti di sicurezza delle informazioni saranno definiti durante lo sviluppo dei requisiti aziendali per nuovi sistemi informativi o modifiche ai sistemi informativi esistenti.

16.2 I controlli per mitigare eventuali rischi identificati saranno implementati dove appropriato.

16.3 I requisiti di sicurezza delle informazioni saranno considerati in ogni sviluppo. Tali requisiti saranno basati su un rapporto di valutazione del rischio.

16.4 Dovrà essere seguito un ciclo di sviluppo in base ai rischi contenuti dal progetto. Questo ciclo di vita includerà documentazione registrata.

16.5 Tutte le fasi del ciclo di sviluppo saranno monitorate e supervisionate.

17 RAPPORTO CON IL FORNITORE

17.1 Così come i fornitori possono essere un vettore principale di rischio, l'organizzazione può anche essere una fonte di rischio per i suoi partner; Pertanto, tutto sarà fatto per prevenire la diffusione delle minacce.

17.2 Canali di comunicazione appositamente istituiti per la sicurezza dovranno essere messi in atto e imposti a partner e fornitori.

17.3 Qualsiasi cambiamento che possa avere un impatto sul livello di sicurezza dell'organizzazione deve essere segnalato all'organizzazione.

17.4 L'organizzazione garantirà che siano in vigore accordi di audit con i fornitori.

18 GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

18.1 Gli incidenti di sicurezza informatica e le vulnerabilità associate ai sistemi informativi saranno comunicati in modo tempestivo. Verranno adottate le azioni correttive appropriate.

18.2 Saranno implementate segnalazioni formali degli incidenti e escalation.

18.3 Tutti i dipendenti, i collaboratori e gli utenti terzi saranno informati sulle procedure per segnalare i diversi tipi di incidenti di sicurezza o vulnerabilità che potrebbero influire sulla sicurezza degli asset dell'organizzazione.

18.4 Gli incidenti e le vulnerabilità sulla sicurezza delle informazioni saranno segnalati il più rapidamente possibile al desk ICT Service.

19 ASPETTI DELLA SICUREZZA DELLE INFORMAZIONI DELLA CONTINUITÀ DEL BUSINESS

19.1 L'organizzazione metterà in atto accordi per proteggere i processi aziendali critici dagli effetti di grandi guasti dei sistemi informativi o disastri e per garantirne la ripresa tempestiva.

19.2 Verrà implementato un processo di gestione della continuità operativa per minimizzare l'impatto sull'organizzazione e recuperare dalla perdita di risorse informative. I processi aziendali critici saranno identificati.

19.3 Verrà effettuata un'analisi dell'impatto aziendale sulle conseguenze di disastri, fallimenti di sicurezza, perdita di servizio e mancanza di disponibilità.

20 CONFORMITÀ

20.1 L'organizzazione rispetterà qualsiasi obbligo legale, statutario, normativo o contrattuale che riguardi i suoi sistemi informativi.

20.2 La progettazione, il funzionamento, l'uso e la gestione dei sistemi informativi saranno conformi a tutti i requisiti di sicurezza statutari, normativi e contrattuali.

FINE.