BIG SB S.p.A.
ROMA_ RM 00161
Via Arezzo, 1

P. IVA_ 13495321005
REA RM_ 1451778
C. S. € 400.000,00 I. V.

POLITICA
Per la SICUREZZA delle INFORMAZIONI
Standard ISO/IEC 27001

Il presente documento descrive la politica BIG SB S.p.A. (in seguito BIG) in materia di sicurezza delle informazioni, in conformità allo standard internazionale ISO/IEC 27001:2013.

La politica di sicurezza delle informazioni guida l'impegno della direzione di BIG nell'espletamento delle attività perseguendo

- il *miglioramento continuo del Sistema per la Gestione,* appropriato al contesto dell'organizzazione, quale strumento strategico attraverso il quale conseguire gli obiettivi del proprio business;
- un'*adeguata gestione dei rischi e delle opportunità* che possono influenzare la conformità delle attività svolte al fine di soddisfare le esigenze e le aspettative di tutte le parti interne ed esterne interessate e mantenere la loro piena fiducia in BIG, quale partner e fornitore di soluzioni.

Tutti i nostri impegni, attività e soluzioni vengono considerati come un'espressione di Qualità e sono contestualmente volti a proteggere il patrimonio informativo. Le richieste e le aspettative del cliente devono essere soddisfatte dalle nostre attività e dalle nostre soluzioni conformemente a quanto concordato, proteggendo tutte le informazioni in nostro possesso. Tale impegno si realizza sia valorizzando sistemi che offrano protezioni allineate alle risorse ed alle attuali tecnologie secondo le esigenze dettate dalle analisi dei rischi, sia definendo ruoli, responsabilità e procedure.
La Direzione di BIG si impegna a garantire la pianificazione, la realizzazione, il controllo e lo sviluppo del sistema di gestione delle informazioni adeguato, sia nel rispetto degli obblighi di legge e contrattuali che delle scelte aziendali legate alla certificazione del proprio ISMS secondo lo standard internazionale ISO / IEC 27001:2013. Pertanto, il processo di gestione della qualità e della sicurezza delle informazioni in BIG persegue i seguenti principi fondamentali:

- PROFESSIONALITÀ, COMPETENZA E RESPONSABILITA'
- SODDISFAZIONE DEL CLIENTE
- INNOVAZIONE e DIVERSIFICAZIONE DEL SERVIZIO
- SICUREZZA DELLE INFORMAZIONI GESTITE
- MIGLIORAMENTO CONTINUO DEL SERVIZIO
- COINVOLGIMENTO DI TUTTE LE PARTI INTERESSATE
- RISPETTO DEI REQUISITI COGENTI e RICHIESTI DAI CLIENTI

Nel dettaglio, invece, BIG persegue i seguenti obbiettivi puntuali:

- La predisposizione di un'adeguata organizzazione aziendale al fine di soddisfare le richieste e le aspettative del cliente
- L'importanza e attenzione data all'integrità, disponibilità e riservatezza delle informazioni pervenute dai nostri clienti e fornitori
- L'impostazione e l'attuazione di un Sistema Integrato in accordo con le Norme Internazionali, le leggi in termini di sicurezza e il Rispetto delle previste normative cogenti
- La formazione e la motivazione di tutti i collaboratori al miglioramento continuo della qualità del proprio lavoro, con il riesame periodico degli obbiettivi assegnati
- Il riesame periodico della presente politica, appropriata agli scopi della Nostra organizzazione e comunicata a tutte le parti interessate, per verificarne la validità ad intervalli prestabiliti ed ogni qualvolta la Direzione ne identifichi la necessità per garantirne la continua idoneità
- La diffusione della presente politica tramite sua affissione negli spazi comuni dell'azienda ma anche sua messa a diposizione al pubblico (pubblicazione sul sito internet aziendale), garantendo la consultazione alle parti interessate esterne
- Salvaguardare gli interessi della Società, dei propri dipendenti e delle terze parti che operano in BIG SPA nel campo dello scopo definito nel Manuale per la Sicurezza delle informazioni
- Salvaguardare i diritti di proprietà intellettuale così da garantire la conformità ai requisiti legali, normativi e contrattuali che tutelano i diritti di proprietà intellettuale legati alle soluzioni fornite
- Effettuare tutte le azioni che vengono valutate idonee sulla base dell'analisi dei rischi dal punto di vista organizzativo ed economico per evitare gli eventi che possano danneggiare riservatezza, integrità e disponibilità del patrimonio informativo gestito attraverso l'applicazione dei controlli così come indicato nello Statement of Applicabilità dell'ISM dell'azienda

- Pianificare e quantificare gli obbiettivi per le azioni di miglioramento continuo del Sistema di gestione per la sicurezza delle informazioni di BIG.

In conseguenza di quanto sopra la Direzione di BIG supporta lo sviluppo del processo di gestione integrato, basandosi sulle seguenti direttive operative:

- Progettazione, realizzazione e gestione di sistemi di protezione delle informazioni (preventivi e di emergenza) secondo le politiche e le linee guida definite dall'organizzazione
- Pianificazione e attuazione di attività di formazione e sensibilizzazione relativamente agli argomenti inerenti alla qualità e l'ISMS di BIG SPA
- Ottimizzazione dell'efficienza delle misure di sicurezza secondo quanto previsto dai documenti di Risk Management aziendale, sia in ambito qualità sia in ambito sicurezza delle informazioni.

La Politica di sicurezza sintetizza e guida l'impegno di BIG volto a progettare un livello di protezione conforme alle normative vigenti, definendo i necessari strumenti organizzativi (ruoli, responsabilità, procedure) che permettono di disporre di un'elevata garanzia sulla efficacia delle protezioni realizzate e della loro corretta gestione.
Le attività aziendali e commerciali di BIG necessitano quindi di una protezione in grado di fronteggiare eventuali attacchi che potrebbero essere arrecati sia dall'ambiente esterno, sia da azioni intenzionali, o semplicemente dovute ad imperizia o negligenza, del personale interno o esterno. In Azienda il tema della *security* è considerato prioritario e affrontato secondo criteri e regole comuni, al fine di garantire una protezione generalizzata e coerente che tenga conto delle peculiarità legate all'attività svolta da BIG, e per garantire un servizio continuo e affidabile si avvale di personale con esperienza e professionalità specifica e dotazione tecnologica (hardware e software) all'avanguardia.

REQUISITI di SICUREZZA delle INFORMAZIONI

L'informazione costituisce il patrimonio fondamentale su cui si basa il business dell'azienda, in quanto l'organizzazione le attribuisce un valore strategico per il conseguimento della propria missione. L'informazione si esplicita in diverse forme: stampata o scritta su carta, memorizzata elettronicamente, trasmessa tramite posta o strumenti elettronici, mostrata in filmati, oppure espressa in conversazioni. Qualunque sia la forma presa dall'informazione, o il mezzo utilizzato per condividerla o memorizzarla, deve essere sempre adeguatamente protetta. Una corretta gestione della sicurezza deve prevedere la protezione delle informazioni, indipendentemente dal tipo di registrazione e dal trattamento effettuato, da un'ampia gamma di minacce, assicurando la continuità della missione aziendale, minimizzando i danni in caso di incidenti e massimizzando l'efficienza negli interventi di sicurezza. La sicurezza delle informazioni è assicurata dalla salvaguardia dei seguenti requisiti:

- *Riservatezza*, che garantisce che un'informazione sia accessibile solo a chi è autorizzato;
- *Integrità*, che salvaguarda l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione;
- *Disponibilità*, che garantisce, quando richiesto e autorizzato, l'accesso alle informazioni e ai beni associati.

Gli obiettivi fissati sono conseguiti attraverso l'adozione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) aderente allo standard ISO/IEC 27001, che assicura il rispetto di tali requisiti, sulla base di un approccio sistematico, basato sull'analisi e il trattamento dei rischi, stabilisce, realizza, attua, controlla, rivede, riadatta e migliora la sicurezza delle informazioni gestite da BIG.

La politica generale enunciata si riferisce e si applica a tutte le informazioni gestite da BIG, siano esse di origine interna o collegate ai servizi erogati ai clienti.

GOVERNO della SICUREZZA

Il SGSI consente all'azienda di migliorare la capacità e l'affidabilità dei servizi erogati e di ottimizzare gli investimenti in materia di sicurezza, tramite l'attribuzione di ruoli, responsabilità e regole condivise, prevedendo attività di pianificazione, procedure, linee guida, processi e risorse in linea con quanto previsto dal modello indicato dallo standard.
Il SGSI si basa sull'applicazione dei principi del Security Management a cui ricondurre tutte le responsabilità di sicurezza relative alle diverse componenti (organizzativo/procedurale, logiche e fisiche), contraendo il processo decisionale tramite il riporto diretto al vertice aziendale del responsabile della funzione e ottimizzando il rapporto prestazione/investimento nella progettazione e gestione dei sistemi di protezione.
Con il SGSI si vogliono raggiungere i seguenti obiettivi:

- garantire la capacità di gestione della sicurezza, in linea con le aspettative delle parti interessate, con gli obiettivi aziendali e con gli standard internazionali;

- normalizzare i vari approcci, ottimizzando e coordinando le risorse disponibili;
- creare un'organizzazione della sicurezza condivisa, documentata, organica, efficiente e capillare;
- consentire un miglioramento continuo;
- armonizzare le procedure di sicurezza con i processi aziendali del Sistema di Gestione della Qualità (S.G.Q.), al fine di ottimizzare gli impatti sulle attività produttive;
- assicurare che le protezioni previste e attuate siano graduate in funzione della criticità dei beni tutelati, anche per ottimizzare l'aspetto economico.

Il processo di gestione della sicurezza delle informazioni segue la logica del ciclo PDCA (Plan/Pianifica, Do/Realizza, Check/Controlla, Act/Sviluppa) onde permettere, seguendo le fasi indicate nella figura, un miglioramento continuo del SGSI.

Fase 1 - Pianificazione (Plan)

La pianificazione prevede l'approvazione delle politiche, l'assegnazione delle risorse per la sicurezza, la definizione dei criteri per l'accettabilità del rischio. I requisiti di protezione delle informazioni scaturiscono, oltre che da norme e da scelte organizzative, anche dall'attività di analisi e valutazione del rischio e sono tradotti in misure di protezione tramite il processo di trattamento del rischio.

Assessment del rischio

Il processo di Assessment del rischio ha l'obiettivo di valutare le vulnerabilità, le minacce e gli impatti dei potenziali incidenti di sicurezza, relativi alle informazioni (e alle infrastrutture che le trattano) e la loro probabilità di verificarsi. La classificazione delle informazioni compete al Security Manager e consiste nella valutazione dell'impatto derivante dalla perdita di riservatezza, integrità o disponibilità del dato stesso. Il risultato della classificazione concorre alla definizione del livello di protezione ritenuto necessario, in relazione alla criticità del dato. Informazioni con la stessa classe di criticità, a parità di esposizione alle minacce, richiedono protezioni analoghe. È compito del Security Manager fornire gli elementi per effettuare:

- l'analisi delle minacce e delle vulnerabilità;
- la rilevazione dei controlli esistenti.

Il risultato del processo è la valutazione del rischio gravante sui vari beni, rispetto alle singole minacce.

Trattamento del rischio

Sulla base dei risultati dell'Assessment si attiva il processo di trattamento del rischio. Il trattamento del rischio ha l'obiettivo di individuare e valutare i diversi interventi, di selezionare i controlli, di produrre la Dichiarazione di Applicabilità, di ottenere l'approvazione della Direzione aziendale relativamente ai rischi residui, da valutare sulla base dei criteri per l'accettabilità del rischio.

Fase 2 - Azione (DO)

In questa fase è definito il Piano di Trattamento del Rischio e sono attuate le misure di controllo definite. Sono inoltre effettuate le attività di formazione specifica del personale, di gestione dell'operatività del SGSI e la messa a punto di un'efficace gestione degli incidenti.

Fase 3 – Controllo (Check)

Le principali attività in cui si articola la fase di controllo sono le seguenti.

Monitoraggio

Per valutare l'andamento dei processi e individuare opportunità di miglioramento della sicurezza sono utilizzati specifici indicatori.

Verifiche Ispettive Interne

Periodicamente sono programmate ed eseguite verifiche ispettive interne, per valutare:

- l'efficacia del SGSI;
- l'efficacia degli obiettivi di controllo;
- il rispetto dei principi generali di sicurezza.

Le modalità di verifica ispettiva interna sono descritte nel paragrafo 0.

Gestione degli incidenti di sicurezza

La gestione degli incidenti di sicurezza si propone di:

- contribuire al miglioramento/adeguamento delle protezioni, valutandone e misurandone l'efficacia (proazione);
- minimizzare gli inconvenienti e i danni connessi agli incidenti di sicurezza informatica (reazione);
- migliorare il SGSI sulla base della conoscenza maturata nella gestione degli incidenti (azione di supporto).

Tutto il personale e i collaboratori di BIG sono tenuti a segnalare prontamente incidenti di sicurezza o situazioni anomale che rivelino una potenziale compromissione dei livelli di sicurezza dell'intero sistema.

Fase 4 – Miglioramento (Act)

Le principali attività in cui si articola la fase di miglioramento sono le seguenti.

Sviluppo e miglioramento del SGSI

Le informazioni di ingresso all'attività di sviluppo e miglioramento sono:

- le risultanze del monitoraggio;
- le "non conformità" scaturite da verifiche ispettive;
- le registrazioni degli incidenti di sicurezza;
- le proposte di modifica.

Tali informazioni sono analizzate per valutare l'efficacia del SGSI e attivare piani di miglioramento. Le azioni intraprese per eliminare le possibili cause di "non conformità" devono essere commisurate ai rischi relativi che possono scaturire dalla loro mancata rimozione.

Riesame della Direzione

Il Riesame del SGSI è effettuato, annualmente o in base alle necessità. L'obiettivo del Riesame è quello di:

- assicurare l'adeguatezza e l'efficacia nel tempo del SGSI, in termini di processi, organizzazione e risorse;
- verificare il livello di sicurezza raggiunto;
- rivedere le politiche di sicurezza.

L'attività è svolta tenendo conto dei seguenti fattori:

- efficacia delle azioni preventive e correttive adottate;
- nuove categorie di minacce e vulnerabilità, non presenti nelle precedenti valutazioni;
- indicazioni dei precedenti Riesami.

L'esito del Riesame è documentato in un verbale di riunione, ed è conservato dal Security Manager.

OBIETTIVI

Gli obiettivi che BIG si prefigge di raggiungere tramite l'attuazione e l'osservanza della politica di sicurezza, sono che:

- le informazioni raccolte, trattate, elaborate, conservate a qualsiasi titolo siano protette da accessi non autorizzati;
- si tuteli la riservatezza delle informazioni sia sul versante esterno che interno;
- si protegga l'integrità delle informazioni salvaguardandole da modifiche non autorizzate;
- le informazioni siano sempre disponibili a livello logico e fisico per gli utenti autorizzati;
- si ottemperi ai requisiti legali, regolamentari, contrattuali e normativi in generale (c.d. cogente);
- si prevedano opportune modalità per assicurare il salvataggio dei dati e la continuità del business aziendale, nonché i piani di reazione agli incidenti di sicurezza;
- il personale sia adeguatamente formato sulla sicurezza;

COMMITMENT DIREZIONALE

Si elencano di seguito gli ambiti di sicurezza dei quali sono indispensabili progettazione ed attuazione ai fini dell'ottenimento della certificazione:

1. assegnazione di ruoli e responsabilità in tema di sicurezza;
2. definizione di politiche di dettaglio riguardanti:
    a. aspetti legati alla sicurezza fisica;
    b. controllo accesso a sistemi e dati;
    c. codice di condotta del personale;

d. prevenzione ed individuazione virus;
e. back up e salvataggio dei dati;
f. risposta agli incidenti;
g. conservazione delle registrazioni dell'organizzazione;
h. Business Continuity;
i. formazione e training del personale;

3. definizione di criteri e metodi per l'analisi dei rischi;
4. adeguamento alle correnti norme contrattuali, legislative e regolamentari (con particolare riguardo alla tutela della privacy);
5. definizione di appropriate modalità e criteri di auditing dell'infrastruttura di governo della sicurezza.

RUOLI E RESPONSABILITÀ

In ottemperanza alla categoria di controllo dello standard di riferimento ISO/IEC 27001 Organizational of Information Security è stata effettuata, a livello di Perimetro di certificazione, una suddivisione dei ruoli e delle responsabilità.

Security Manager

Il Security Manager, nella persona del Responsabile SGQ, ha le seguenti responsabilità:

- attuare il sistema di tutela del patrimonio dei beni materiali e delle informazioni aziendali all'interno del Perimetro;
- pianificare le attività di audit e trasmettere i risultati;
- coordinare le attività di tutti i responsabili delle direzioni/reparti organizzativi coinvolti nel Perimetro.

INFORMAZIONE/FORMAZIONE

In ossequio alle linee guida ISO/IEC 27001 Information Security Awareness, Education and Training si stabilisce che la concreta attuazione di un Sistema di gestione dell'informazione si consegua anche grazie alla promozione di una relativa cultura aziendale, realizzata mediante un'attività di informazione e l'attuazione di specifici piani di formazione.

Attività di Informazione

L'attività di informazione riguarda, con opportuna graduazione dei contenuti e adeguata scelta dei canali di comunicazione, tutto il personale a qualunque titolo impiegato all'interno del Perimetro prescelto. Tale attività ha lo scopo di sensibilizzare il personale sugli aspetti normativi, metodologici e comportamentali da osservare per una corretta e completa attuazione di un Sistema di tutela dei beni aziendali.

Contenuti del Programma di Formazione

L'attività di formazione è rivolta al personale dipendente ed ha come scopo quello di approfondirne ed aggiornarne il know how. I programmi di formazione si articolano in due livelli:

- un primo livello, più generale, volto alla formazione dei ruoli definiti all'interno del Perimetro per la tutela dei beni aziendali;
- un secondo livello, più dettagliato, volto alla formazione degli specialisti chiamati concretamente all'attuazione del Sistema di tutela dei beni aziendali.

Il programma di formazione, accanto a modalità di erogazione di tipo tradizionale, potrà essere completato da iniziative e interventi complementari, quali articoli su riviste di settore, la previsione di una specifica area dedicata, nell'ambito del sistema intranet aziendale, alla formazione, cd rom multimediali. In attuazione di quanto previsto nelle linee guida ISO/IEC 27001 è previsto, per il Perimetro di certificazione un sistema di auditing basato su tre livelli:

- verifiche interne;
- audit esterni.

Verifiche interne

Le verifiche interne basate sull'analisi del rischio sono effettuate dal Security Manager di BIG, tenendo conto delle risultanze delle verifiche di autocontrollo ed in conformità alla metodologia prevista dagli standard internazionali.

Audit esterni

Gli audit esterni ovvero la verifica svolta sul sistema di gestione della sicurezza del Perimetro, da parte di personale esterno e appositamente certificato, sono utilizzati nel caso in cui si voglia ottenere una certificazione di Sicurezza. Per le verifiche di terza parte, sono previste le seguenti evenienze:

- può essere incaricato un team di audit appartenente ad un Ente certificatore accreditato;
- può essere incaricata una società di consulenza esterna in possesso dei necessari e di comprovati requisiti di esperienza nel campo della sicurezza.

In funzione delle normative e degli standard di sicurezza vigenti è consigliabile una cadenza almeno annuale delle verifiche di terza parte, salvo situazioni e/o evenienze interne al Perimetro che suggeriscano una frequenza maggiore oppure audit mirati.

Appendice A - Bibliografia

Documenti e Standard di riferimento

[a] ISO/IEC 27002 – Information technology - Security techniques – Code of practice for information security management

[b] ISO/IEC 27001 - Information technology - Security techniques – Information security management systems – Requirements

[c] Panorama Giuridico-Amministrativo

[1] Legge n° 547, 23.12.1993 - "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

[2] D.Lgs. n° 196 del 30/6/2003 (Testo Unico sulla Privacy)

[3] D.Lgs. n° 518, 29.12.1992 - "Attuazione della Direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore".

[4] Direttiva 2002/58/CE del 12 luglio 2002 "Relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche"

[5] D.Lgs. 231/01 “Disciplina della responsabilità amministrativa delle persone giurdiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell’art. 11 della Legge 29/09/00 n. 300” (Corporate Governance).

INDICE DEGLI ARGOMENTI