ISO/IEC 27001
Gestione sicura delle informazioni

Salvaguardare il patrimonio dati
Guida al prodotto

bsi.

...making excellence a habit.™

Che cos'è la ISO/IEC 27001?

ISO/IEC 27001 è lo standard internazionale in materia di gestione sicura dei dati e fornisce informazioni dettagliate per l'adozione di un affidabile ISMS (Information Security Management System).

Per approfondire i dettagli e le implicazioni di questa norma, suggeriamo di iscriversi ad uno dei nostri corsi.
bsigroup.it/formazione

Sicurezza dei dati significa salvaguardia della privacy, integrità e disponibilità delle informazioni, che esse siano in forma scritta, verbale o in formato elettronico. Poiché tutte le organizzazioni raccolgono, conservano e gestiscono informazioni di vario tipo, la questione della sicurezza dei dati è di primaria importanza.

ISO/IEC 27001 offre un approccio alla pianificazione e all'implementazione dell'ISMS (Information Security Management System) basato sui rischi, grazie al quale è possibile raggiungere un livello di sicurezza organizzativa adeguata e sostenibile. In tal modo garantisce che vengano selezionati gli individui, i processi, le procedure e le tecnologie giuste affinché ogni azienda possa tutelare il proprio patrimonio dati.

ISO/IEC 27001 è applicabile a organizzazioni di ogni dimensione, qualunque sia il loro settore di attività. La norma è particolarmente utile per le aziende ad elevata regolamentazione, quali banche, agenzie di servizi finanziari, sanitari, del settore pubblico e IT. Essa è inoltre altamente efficace per le organizzazioni che gestiscono informazioni per conto terzi, in quanto rappresenta un mezzo ideale per dimostrare la messa in opera di controlli di sicurezza adeguati e per consentire ai clienti una scelta informata nella gestione della conformità ai requisiti per la protezione dei dati e ad altre norme relative.

Perché adottare la norma ISO/IEC 27001?

ISO/IEC 27001 fornisce un quadro di riferimento che consente di implementare un sistema di gestione in grado di proteggere sia le informazioni che l'azienda, riducendo rischi, contenziosi e periodi di fermo operativo.

In considerazione dell'accresciuta facilità di accesso ai dati aziendali tra le diverse organizzazioni, diventa ancora più cruciale ridurre al minimo la propria vulnerabilità in termini di privacy. Sia che i dati in questione siano informazioni finanziarie, codici software o portafogli clienti/fornitori, e, a prescindere dalle modalità di immagazzinamento prescelte, è necessario che vi siano controlli di sicurezza attendibili.

Una chiara strategia di tutela garantisce alle parti interessate, in particolare ai clienti, che i loro dati sensibili siano al sicuro. Avvalendosi di questo standard internazionale, un'organizzazione dimostra un approccio basato sui rischi nella scelta e nella implementazione di controlli per la sicurezza dei dati.

Inizialmente si può avere la sensazione che l'adozione di un ISMS imponga l'impiego di grandi risorse offrendo tuttavia un ritorno economico di modesta entità. In realtà, si è riscontrato che i costi sono ampiamente compensati dalla prevenzione e riduzione dell'impatto e della frequenza degli incidenti.

A partire dalla riforma della norma BS 7799, il valore della certificazione ISO/IEC 27001 ha subito un rapido incremento in molti settori del mercato globale. Essa è spesso strumento e punto di riferimento in materia di conformità e, sempre più frequentemente, specificamente inclusa fra le clausole contrattuali.

Acquisire la certificazione ISO/IEC 27001 significa consentire alla propria organizzazione un approccio strutturato alla pianificazione, implementazione e gestione di un ISMS atto a ridurre il numero di incidenti e incrementare la fiducia delle parti interessate.

L'85% dei clienti BSI in ambito di sicurezza dei dati ha guadagnato la fiducia dei propri stakeholder adottando un sistema certificato ISO/IEC 27001*

*BSI Excellerator Research

I vantaggi offerti dalla norma ISO/IEC 27001

La certificazione ISO/IEC 27001 offre diversi benefici, se rilasciata da un organismo indipendente quale BSI. Tra questi:

Documentare l'indipendenza e l'obiettività del proprio ISMS e dei relativi controlli di sicurezza, nonché il rispetto dei requisiti aziendali di gestione e di continuità operativa

+

Attestare nella massima autonomia l'esistenza di leggi e regolamenti applicabili e l'attuazione di processi volti a garantire la conformità

+

Distinguersi a livello concorrenziale rispettando le clausole contrattuali e dimostrare ai propri clienti di considerare la sicurezza dei loro dati una priorità assoluta

+

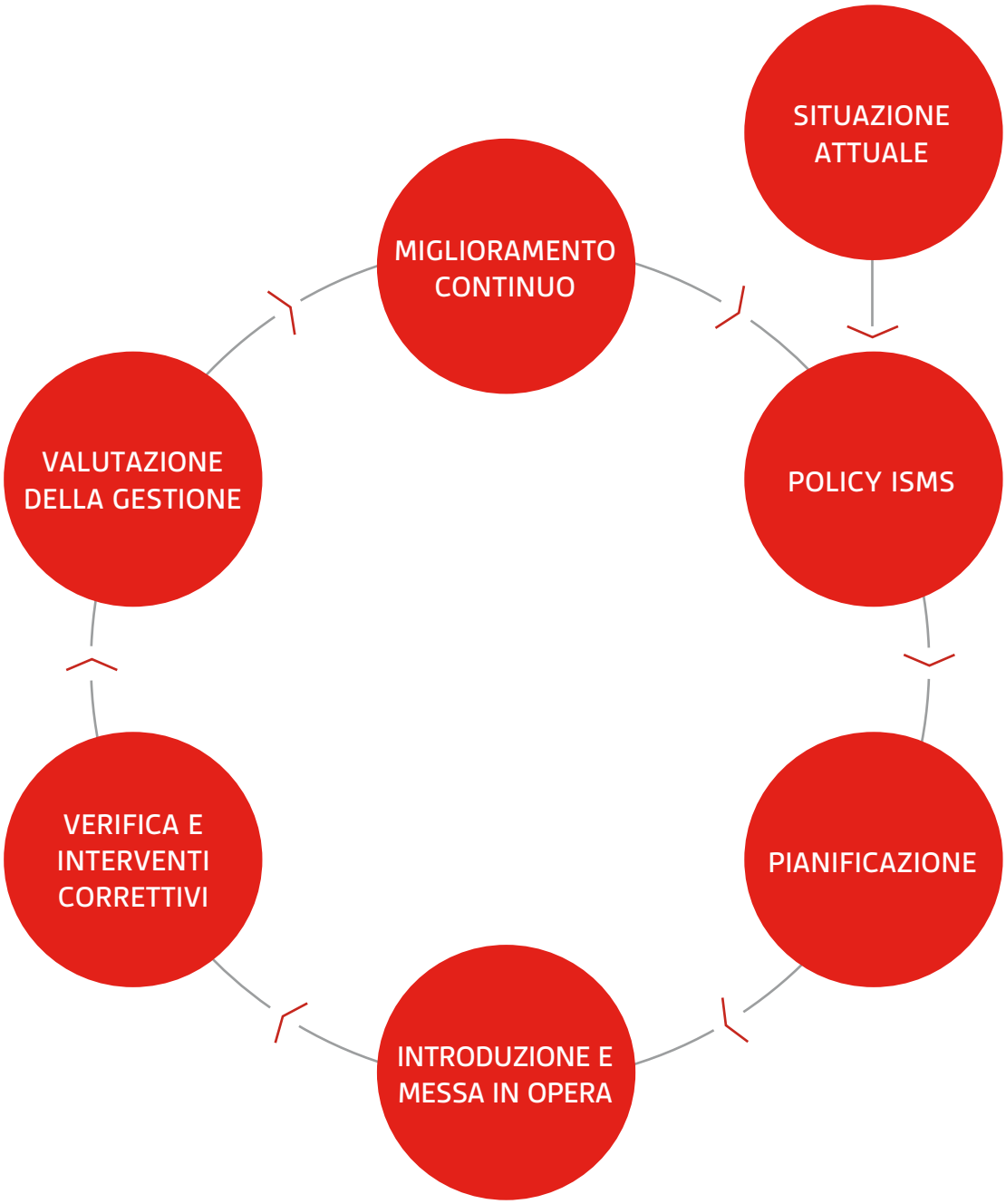
Verificare indipendentemente che l'organizzazione sia in grado di individuare, valutare e gestire correttamente i rischi aziendali, formalizzando al tempo stesso processi, procedure e documentazione relativi alla sicurezza dei dati

+

Dimostrare l'impegno dei quadri dirigenziali ai fini della sicurezza dei dati

+

Un processo regolare di valutazione in grado di sostenere il monitoraggio continuo delle prestazioni e il loro sviluppo



Modello ISO/IEC 27001

Prima di poter adottare un ISMS è necessario capire quali siano le informazioni in possesso dell'azienda e come esse vengano usate ai fini operativi. Attività, prodotti e servizi aziendali hanno tutti un effetto a livello di sicurezza dei dati.

Lo standard ISO/IEC 27001 è utile per acquisire da subito conoscenza e comprensione delle problematiche relative alla protezione delle informazioni e fornisce un chiaro quadro di riferimento per lo sviluppo di un ISMS.

Policy e pianificazione

La norma ISO/IEC 27001 elenca i requisiti in cinque sezioni principali e tratta i diversi controlli di sicurezza, ognuno specifico per argomento e obiettivi, in un'appendice organizzata come segue:

Criteri di sicurezza - Fornire indicazioni amministrative e supportare la tutela delle informazioni conformemente ai requisiti aziendali e nel rispetto di norme e regolamenti relativi.

Organizzazione ai fini della sicurezza dei dati - Gestire le informazioni all'interno dell'azienda e preservare l'integrità

delle strutture per la gestione dei dati eventualmente consultati, elaborati e comunicati a terze parti.
Gestione del patrimonio - Raggiungere e mantenere un adeguato livello di protezione del patrimonio organizzativo.

Sicurezza delle risorse umane - Accertare che impiegati, collaboratori e terze parti comprendano le proprie responsabilità e siano adatti al ruolo per cui vengono presi in considerazione, consci delle minacce alla sicurezza dei dati.

Sicurezza fisica e ambientale - Impedire accessi fisici non autorizzati, danni e interferenze alle sedi aziendali o alle informazioni. Prevenire perdite, danni, furti o compromissione del patrimonio e interruzione delle attività aziendali.

Gestione delle comunicazioni e operazioni - Contribuire a garantire che i dati siano elaborati correttamente, salvati nella massima sicurezza e gestiti in maniera adeguata.

Controllo dell'accesso - Supportare il controllo degli accessi a informazioni, network e applicazioni e prevenire accessi non autorizzati, interferenze, danni e furti.

Acquisto, sviluppo e manutenzione di sistemi informatici - Garantire che la sicurezza sia parte integrante del sistema, supportare la protezione di applicazioni e file e ridurre il livello di vulnerabilità.

Gestione degli incidenti relativi alla sicurezza informatica - Garantire che violazioni e problemi relativi alla sicurezza vengano comunicati con prontezza, così da consentire un intervento tempestivo.

Gestione della continuità operativa - Garantire misure efficaci contro l'interruzione delle attività aziendali e proteggere i processi operativi fondamentali dagli effetti di eventuali anomalie o collassi del sistema informatico.

Conformità - Impedire infrazioni di qualunque obbligo legale, statutario, normativo o contrattuale, nonché di qualunque requisito di sicurezza. Garantire la conformità dei sistemi con le politiche di sicurezza e gli standard aziendali.

Introduzione e messa in opera

Adottare un ISMS è un processo da portare a termine passo dopo passo, in cui ogni intervento si basa su quello precedente e costituisce un insieme logico e coerente. Ed è solo alla fine dell'intero processo che viene effettuata la verifica da parte di BSI.

Studio per la delimitazione del campo d'indagine

Il primo passo è definire gli scopi del progetto. Essi dovrebbero riflettere in modo chiaro gli obiettivi aziendali e impostare sedi e dipartimenti di pertinenza, compresi eventuali requisiti specifici. La determinazione di scopo servirà da guida per affrontare i passi successivi.

Valutazione dei rischi

L'analisi dei rischi serve per determinare il patrimonio dati nel suo complesso e valutare pericoli e punti deboli ad esso associati. Ciò consente di stilare un elenco delle possibili minacce che possono essere ordinate secondo il livello di rischio.

Gap analysis

La gap analysis consiste in una valutazione dei progressi compiuti in termini di effettiva applicazione dei requisiti ISO/IEC 27001 e dei relativi controlli di sicurezza. Laddove non siano previste determinate attività, quali, ad esempio, lo svolgimento di transazioni online, i relativi controlli possono essere formalmente esclusi. Una gap analysis, eseguita internamente o avvalendosi dell'assistenza di esperti BSI, fornisce indicazioni utili relative ai requisiti necessari affinché l'ISMS sia conforme alle disposizioni ISO/IEC 27001.

Dichiarazione di applicabilità

La dichiarazione di applicabilità dovrebbe elencare tutti i controlli, specificando le modalità e le ragioni della loro attuazione.

Programma per il miglioramento della sicurezza

A questo punto, la situazione relativa alla sicurezza dei dati dovrebbe essere piuttosto chiara. Occorre quindi procedere allo sviluppo di politiche e procedure mirate, atte a tutelare il patrimonio dati dai rischi identificati, in termini di risorse umane, strumentazione e migliorie tecniche. Per alcuni punti potrebbe essere necessario un intervento immediato, per altri invece solo un aggiornamento di regole o linee guida (eventualmente anche gesti semplici come chiudere a chiave l'archivio dopo averlo consultato).

Prove, controlli e verifiche interne

Man mano che si attuano interventi per una maggiore sicurezza delle informazioni, ogni misura o modifica del processo deve essere testata per verificare che produca i miglioramenti desiderati. A tal fine è possibile richiedere una valutazione esterna da parte di BSI. Va, inoltre, effettuata una verifica interna dell'ISMS.

Implementazione

Una volta elaborati politiche, procedure e controlli, questi devono essere resi operativi. Ogni organizzazione è diversa e diverse sono quindi le procedure. L'adozione di nuove politiche aziendali può essere facilitata da corsi di formazione, discussioni e promozioni. Per introdurre tali cambiamenti è inoltre necessario il coinvolgimento attivo della direzione.

Completamento del documento

La dichiarazione di applicabilità deve essere chiara, concisa e di facile comprensione. Poiché la norma ISO/IEC 27001 richiede uno sviluppo continuo, il documento redatto dovrebbe essere periodicamente verificato e aggiornato per riflettere i cambiamenti in termini di prassi e processi aziendali, come anche i risultati ottenuti dal programma per il miglioramento continuo della sicurezza.

Valutazione della gestione

L'ISMS deve essere sottoposto con regolarità a revisione da parte della direzione aziendale, al fine di garantirne in maniera continuativa idoneità, adeguatezza ed efficacia.
Ciascuna attività svolta quotidianamente a livello aziendale deve essere tesa alla tutela delle informazioni e introdurre le necessarie modifiche in quanto mezzo più idoneo a migliorare il funzionamento dell'intero sistema.

Miglioramento continuo e interventi correttivi

Come avviene per tutti gli standard di gestione, è necessario voltarsi indietro a guardare i progressi compiuti. Verifiche interne e valutazioni della gestione si confermano strumenti fondamentali sia per determinare l'efficacia di un ISMS che per continuare a migliorarlo.
Qualunque non conformità dell'ISMS deve dare luogo a contromisure atte a garantire che questa non si verifichi nuovamente. Come per ogni standard relativo ai sistemi di gestione, anche in questo caso il miglioramento continuo è considerato un requisito fondamentale.

Per informazioni sui nostri corsi di formazione: bsigroup.it/formazione
Per l'acquisto della norma ISO/IEC 27001: shop.bsigroup.com

L'impegno di BSI non termina con un certificato

BSI rilascia, in qualità di terza parte indipendente, la certificazione ISO/IEC 27001. Con BSI il processo di certificazione è semplice: alla ricezione della richiesta, assegniamo ad un responsabile clienti il compito di guidare l'azienda lungo il processo di certificazione. Tuttavia, il nostro supporto non si esaurisce con il rilascio del certificato; continuiamo ad occuparci dell' organizzazione per tre anni, avvalendoci della nostra esperienza per garantire che la conformità sia mantenuta nel tempo. In questo modo non solo si potrà dimostrare alle parti interessate e ai clienti il massimo rispetto delle migliori pratiche in materia di sicurezza delle informazioni, ma anche trarre beneficio dalle verifiche regolari cogliendo le opportunità di miglioramento.

Per ricevere una prima valutazione sulla ISO/IEC 27001

+39 02 6679091
marketing.italy@bsigroup.com

Percorso di certificazione

1. Acquisto dello standard sul sito shop.bsigroup.com
2. Contatto con BSI:
   + 39 02 6679091
   marketing.italy@bsigroup.com
3. Compilazione del modulo di richiesta
4. Pianificazione della formazione con BSI
5. Gap analysis - verifica preliminare alla certificazione (opzionale)
6. Costituzione di un team BSI dedicato
7. Valutazione formale di BSI – stage 1
8. Valutazione formale di BSI – stage 2
9. Rilascio del certificato da parte di BSI
10. Follow up BSI

Le serve aiuto per l'implementazione del suo sistema?

Ci impegniamo per assistervi passo dopo passo.
Abbiamo creato il programma Consulenti Associati (ACP, Associate Consultant Programme) per permettervi, attraverso un servizio imparziale, di accedere alla consulenza che necessitate.
Il nostro obiettivo è rendere il processo di certificazione quanto più semplice possibile. In quanto organismo di certificazione indipendente, non offriamo o raccomandiamo servizi di consulenza specialistica. Per tale ragione abbiamo creato l'ACP, al quale partecipano oltre 100 membri che vantano una consolidata esperienza nel campo dei sistemi di gestione certificati.

Soluzioni BSI per la sicurezza dei dati

Che si desideri adottare la norma ISO/IEC 27001 per proteggere il patrimonio dati e sviluppare delle buone prassi o si richieda la piena certificazione per soddisfare requisiti contrattuali e rassicurare i clienti, BSI può fornire assistenza lungo l'intero percorso. La nostra offerta di prodotti per la sicurezza dei dati comprende:

- Elaborazione di standard e pubblicazioni
- Assistenza e consigli in materia di gestione delle informazioni
- Formazione: corsi in house e public
- Gap analysis
- Certificazione del sistema di gestione
- Entropy SoftwareTM – programma di gestione progettato per migliorare i controlli di sicurezza

Perché BSI?

BSI è riconosciuta quale organismo normativo nazionale del Regno Unito. Sviluppiamo, pubblichiamo e commercializziamo standard e prodotti correlati. La nostra azienda consente alle organizzazioni di ottenere risultati migliori, facendo dell'eccellenza un'abitudine. Per oltre un secolo i nostri esperti hanno combattuto mediocrità e noncuranza per fare dell'eccellenza il terreno su cui possano crescere persone e prodotti per ottenere risultati migliori, ridurre i rischi e svilupparsi in maniera sostenibile. I nostri clienti comprendono marchi riconosciuti a livello mondiale, così come piccole aziende locali, operanti in oltre 150 Paesi.

La nostra azienda è titolare di una concessione reale per lo sviluppo e la fornitura di prodotti e servizi davvero completi.
Il nostro impegno è volto al miglioramento continuo e operiamo nel massimo rispetto dei principi d'integrità.

Per ulteriori informazioni su servizi e prodotti BSI: **bsigroup.it**

BSI Group Italia
Via Fara, 35
20124 Milano

+39 02 6679091
marketing.italy@bsigroup.com
bsigroup.it

The trademarks in this material (for example the BSI logo or the word "KITEMARK") are registered and unregistered trademarks owned by The British Standards Institution in UK and certain other countries throughout the world.