POLITICA PER LA QUALITÀ E LA SICUREZZA DELLE INFORMAZIONI – BIM ITALIA

UNI EN ISO 9001:2015 – Quality Management System

ISO/IEC 27001:2022 – Information Security Management System

GPI
The Healthcare Partner

bim italia

I NOSTRI PRINCIPI

Il nostro impegno

BEST PRACTICES

Supportare l'adozione e implementare i **principi**, gli **standard tecnologici** e le **best practices internazionali** per garantire la **sicurezza** delle **informazioni**.

SISTEMA DI GESTIONE INTEGRATO

Sviluppare, mantenere e migliorare nel tempo il sistema di gestione integrato per la qualità e la sicurezza delle informazioni al fine di rispondere alle mutevoli esigenze del business e dei processi aziendali.

PROCEDURE

Introdurre e mantenere specifiche **procedure** volte a garantire il **controllo e la qualità** dei servizi forniti, la gestione degli eventi di crisi e l'adozione di misure e controlli di sicurezza delle informazioni.

OBIETTIVI

Stabilire **obiettivi e strategie** per assicurare la sicurezza delle informazioni e la qualità dei servizi offerti, garantendo adeguate risorse (umane, tecnologiche e finanziarie) per il raggiungimento degli obiettivi prefissati.

ANALISI DEI RISCHI

Identificare, valutare e gestire i rischi per la qualità e la sicurezza delle informazioni, allineandoli alle evoluzioni organizzative e tecnologiche dei sistemi e dei servizi

Il nostro impegno

COMPLIANCE

Rispetto dei requisiti normativi e contrattuali previsti per l'erogazione dei servizi o che regolino specifici requisiti di sicurezza delle informazioni finalizzati, ad esempio, alla tutela del dato personale - quali ad esempio il D.Lgs. 196/2003, il Regolamento UE 2016/679, il D.Lgs. 101/2018 e le norme ISO-IEC 270xx

PERSONE

Accurata **selezione e formazione del personale** addetto alla progettazione, sviluppo ed esercizio dei sistemi e dei servizi, garantendone la continuità di servizio e le competenze.

RUOLI E RESPONSABILITA'

Dotarsi di **strutture organizzative** e risorse dedicate a presidio dell'implementazione e della gestione dei processi aziendali e della sicurezza delle informazioni.

FORMAZIONE

Sviluppare **programmi di sensibilizzazione** per fornire un'adeguata formazione sulle modalità di gestione delle situazioni di crisi, creare consapevolezza aziendale e migliorare le competenze necessarie per sviluppare e mantenere il sistema di gestione per la qualità e per la Sicurezza delle informazioni.

STRUMENTI DI SUPPORTO

Progettare, sviluppare e ricercare le **soluzioni tecnologiche** e gli **strumenti utili** e necessari per l'erogazione e la continua evoluzione dei servizi offerti e della sicurezza delle informazioni.

Il nostro impegno

VALORE DELLE RISORSE UMANE

I dipendenti e i collaboratori sono al centro delle politiche di Bim, e ne costituiscono fattore indispensabile di successo e crescita. Il valore di una persona è un valore per l'azienda. L'organizzazione tutela e promuove il valore delle persone allo scopo di migliorare ed accrescere il patrimonio e la competitività delle competenze possedute da ciascun collaboratore. Bim si impegna a fare in modo che l'autorità sia esercitata con equità e correttezza, evitandone ogni abuso. In particolare, viene garantito che l'autorità non si trasformi in esercizio del potere lesivo della dignità del dipendente e del collaboratore.

INTEGRITÀ DELLA PERSONA

BIM garantisce l'integrità fisica e morale dei suoi dipendenti e collaboratori, condizioni di lavoro rispettose della dignità individuale e ambienti di lavoro sicuri e salubri. Perciò non sono tollerate richieste o minacce volte ad indurre le persone ad agire contro la legge e il Codice Etico, o ad adottare comportamenti lesivi delle convinzioni e preferenze morali e personali di ciascuno.

QUALITÀ DEI SERVIZI E DEI PRODOTTI

BIM orienta la propria attività alla soddisfazione ed alla tutela dei propri clienti dando ascolto alle richieste che possono favorire un miglioramento della qualità dei prodotti e dei servizi. Per questo motivo, indirizza le proprie attività di ricerca, sviluppo e commercializzazione ad elevati standard di qualità dei propri servizi e prodotti.

Dichiarazione e Responsabilità

Dichiarazione e Responsabilità

INFORMAZIONI COME RISORSA AZIENDALE

BIM considera le informazioni come una risorsa aziendale che deve essere **PROTETTA** in quanto costituisce parte essenziale per lo svolgimento dell'attività aziendale. Data la tipologia di attività svolta e la natura dei dati trattati (dati comuni, sensibili, sanitari e giudiziari), ritiene di importanza fondamentale la tutela dei dati personali. Tutti i dati e le relative elaborazioni per la gestione delle attività devono essere protetti per garantire che giungano **INTEGRI** a chi deve utilizzarli, che **SIANO SEMPRE DISPONIBILI** e che **NON SIANO DIVULGATI** a soggetti non autorizzati.

BIM ha impostato un sistema efficiente di sicurezza delle informazioni, atto a ridurre i rischi e le probabilità che si verifichino danni alle informazioni o interruzioni alle attività. Questo permette all'azienda di assicurare la continuità e la qualità delle proprie attività, minimizzare i rischi, garantire il ritorno degli investimenti, le opportunità di business, il rispetto delle leggi e la redditività.

Attraverso la valutazione dei rischi, BIM si propone di rispondere ad ogni minaccia al proprio patrimonio informativo e allo svolgimento dei propri servizi IT con misure di sicurezza più adeguate, stanziando per queste un budget adeguato.

La sicurezza delle informazioni, la tutela dei dati personali e la qualità dei servizi costituiscono un processo sia tecnologico che organizzativo; di conseguenza BIM ha predisposto una serie di procedure operative standard unitamente ad attività formativa rivolta al proprio personale addetto. Le politiche di sicurezza, le procedure operative e la valutazione dei rischi sono riviste periodicamente, al fine di recepire nuovi indirizzi di business, evoluzioni tecnologiche e normative pertinenti.

A garanzia delle proprie attività BIM ha implementato il:

SISTEMA DI GESTIONE PER LA QUALITÀ , in conformità alla Norma UNI EN ISO 9001:2015

SISTEMA DI GESTIONE DI SICUREZZA DELLE INFORMAZIONI, in conformità alla Norma UNI CEI EN ISO/IEC 27001:2017, e alle linee guida ISO/IEC 27017 e ISO/IEC 27018

Incident Management

Incidenti di Sicurezza e di Business Continuity

EVENTO E INCIDENTE DI SICUREZZA DELLE INFORMAZIONI

Un evento relativo alla sicurezza delle informazioni è un evento che indica una possibile violazione della sicurezza delle informazioni o fallimento dei controlli.

Un incidente relativo alla sicurezza delle informazioni è l'insieme di uno o più eventi di sicurezza delle informazioni correlati e identificati che possono danneggiare i sistemi di informazione e/o le risorse di dati o comprometterne le funzionalità. In generale sono eventi di sicurezza delle informazioni che hanno impatti più o meno gravi per il business aziendale.

INCIDENTI DI BUSINESS CONTINUITY

Un incidente di Business Continuity è un evento che può condurre a un'interruzione, a una perdita, a un'emergenza o a una crisi.

Per interruzione si intende un evento, atteso o inatteso, che causa una deviazione negativa, non pianificata dell'erogazione prevista dei prodotti e servizi secondo gli obiettivi di un'organizzazione.

BIM CONSIDERA GLI INCIDENTI DI SICUREZZA E DI BUSINESS CONTINUITY UN IMPORTANTE RISCHIO PER IL PROPRIO BUSINESS E PERTANTO HA

- adottato processo per l'identificazione delle potenziali minacce per l'azienda e degli impatti che tali minacce potrebbero causare alla sicurezza delle informazioni e ai servizi erogati, definendo un sistema in grado di migliorare la resilienza, la capacità di ripristino e di reazione a fronte di una crisi.
- implementato un piano di gestione degli incidenti e le procedure per affrontare le necessarie indagini di follow-up;
- individuato la struttura organizzativa per la gestione degli eventi e degli incidenti, definendo i componenti, le competenze, le modalità operative del Incident Response Team (IRT) e il processo di comunicazione verso gli stakeholder.

Il fine ultimo è quello di evitare, per quanto possibile, l'accadimento di incidenti e, nel caso questi accadessero, di essere in grado di gestirli e di individuare le azioni necessarie per ridurre il rischio del ri-verificarsi dell'incidente.