Organizzazione responsabile (Dir. Technology)
ID OneTrust 732

POLICY IN TEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

VERSIONE 1.0

APPROVATO DAL
COMITATO ESECUTIVO
IN DATA 29 OTTOBRE 2024

Università Bocconi
MILANO

Principi Guida sulla Gestione della Sicurezza delle Informazioni

L'Università Bocconi si impegna a stabilire, attuare, mantenere e migliorare continuamente un Sistema di Gestione della Sicurezza delle Informazioni coerente con le finalità strategiche e i processi dell'Università. Tale sistema viene sviluppato in linea con lo Standard Internazionale ISO/IEC 27001, e le normative vigenti GDPR e D.lgs. 231/2001.

Il presente documento descrive gli obiettivi perseguiti, le modalità con cui è sviluppato il sistema, i principi di riferimento e le regole di base per il controllo e la gestione della sicurezza delle informazioni. Inoltre, rappresenta l'impegno dell'Università nel proteggere le informazioni con responsabilità e misure di sicurezza chiaramente identificate e definite.

Tale impegno contribuisce a rafforzare e mantenere la credibilità e la reputazione dell'Università nei confronti dei suoi studenti, degli alumni, di dipendenti, dei sostenitori, e degli altri partner commerciali e stakeholder, ivi inclusa la Pubblica Amministrazione con cui interagisce in continui scambi di dati e informazioni.

I principi che l'Università Bocconi si prefigge di rispettare attraverso il Sistema di Gestione della Sicurezza delle Informazioni sono:

- Garantire la riservatezza dei dati in modo tale che essi siano disponibili soltanto ai processi e/o alle risorse legittimate al loro utilizzo;
- Garantire l'integrità delle informazioni, delle applicazioni, dei sistemi e delle reti impedendo modifiche non autorizzate o accidentali;
- Garantire la disponibilità delle informazioni in funzione delle specifiche esigenze, consentendo la continuità dei processi.

Tali principi sono declinati in obiettivi, dettagliati in appositi documenti, che devono essere monitorati e misurati per garantire l'efficacia del Sistema di Gestione.

Il Sistema di Gestione rispetta i requisiti ISO27001 ed è strutturato attraverso:

- Identificazione dei ruoli e delle responsabilità coinvolti nelle attività di protezione del patrimonio informativo;
- Adozione di un processo teso a identificare, valutare e monitorare periodicamente i rischi di sicurezza delle informazioni in funzione di cambiamenti avvenuti nel contesto tecnico-organizzativo interno ed esterno, anche al fine di ripercorrere nel tempo le motivazioni delle scelte effettuate;
- Definizione dei protocolli di sicurezza per la gestione degli asset e delle configurazioni, al fine di garantire l'accesso ai dati secondo il principio di minimo privilegio;
- Definizione di linee guida per la protezione degli accessi fisici alle sedi universitarie e in particolare alle aree in cui sono custoditi server e infrastrutture tecnico-informatiche;
- Definizione dei presidi di sicurezza logica attraverso un processo di *Security by Design* nell'ambito dello svolgimento delle diverse iniziative progettuali;
- Definizione delle modalità di rilevazione e gestione dei possibili incidenti sulla sicurezza del patrimonio informativo;
- Definizione dei presidi utili a garantire la continuità dei servizi tecnologici erogati in ambito IT;

- Definizione delle istruzioni finalizzate a gestire la sicurezza delle informazioni in conformità alle esigenze operative, alle procedure aziendali e alle normative esterne di riferimento tra cui, a titolo esemplificativo, il GDPR, il D.lgs. 231/2001, etc.;
- Definizione di un processo teso valutare l'adeguatezza delle terze parti e delle istruzioni e clausole da inserire negli accordi con esse;
- Categorizzazione e classificazione delle informazioni al fine di una efficiente pianificazione degli sforzi e degli investimenti secondo un ordine di priorità oggettivo e condiviso;
- Definizione delle modalità di sensibilizzazione sugli atteggiamenti che incidono sulla sicurezza delle informazioni, a livello di vertici d'Ateneo, soggetti apicali e dei loro collaboratori.

Le presenti disposizioni sono punto di riferimento di altri documenti normativi di livello inferiore che in maniera particolareggiata, nell'osservanza dei principi sopra esposti, descrivono gli obiettivi di sicurezza puntuali, il contesto organizzativo di riferimento, i presidi di controllo previsti dallo Standard ISO/IEC 27001 applicabili all'Università e il Manuale del Sistema di Gestione della Sicurezza delle Informazioni suggerito dalle *best practice* di riferimento alla normativa stessa. Inoltre, il Sistema di Gestione della Sicurezza delle Informazioni si compone di ulteriori documenti operativi di dettaglio.

Ambito di applicazione

L'ambito di applicazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) comprende i processi e le attività gestite dalle Direzioni Staff dell'università a riporto del Consigliere Delegato. Questi processi ed attività comprendono la gestione delle infrastrutture tecnico-applicative, il governo dei processi e delle risorse impiegate nelle attività amministrative, così come la conduzione dei processi a supporto della docenza, della didattica, della ricerca e della terza missione.

La presente disposizione riguarda tutto il personale staff ed i collaboratori e fornitori coinvolti nelle attività specificate. Questo documento è diffuso a livello interno all'università e messo a disposizione delle parti interessate tramite i canali di comunicazione interna ed esterna dell'istituzione. Inoltre, il documento è soggetto a revisioni periodiche per assicurare che rimanga sempre adeguato, appropriato ed efficace rispetto alle esigenze dell'università e agli sviluppi del contesto esterno.

Con riferimento alle attività connesse alla produzione accademica, queste sono deliberate sotto la piena autonomia e autoregolamentazione della docenza che opera al di fuori del perimetro di competenza del Consigliere Delegato. In questo contesto, il Sistema di Gestione della Sicurezza delle Informazioni si configura per la docenza come un insieme di linee guida che, benché debbano essere rispettate, non possono costituire, nel rispetto delle libertà accademiche garantite ai docenti, oggetto di controllo diretto da parte di Direzioni amministrative sottoposte al Consigliere Delegato.

Leadership del Sistema di Gestione della Sicurezza delle Informazioni

Il Sistema di Gestione della Sicurezza delle Informazioni dell'università è strutturato attorno a due ambiti di azione principali:

- **Sicurezza delle Infrastrutture Tecnico-Applicative**. Questo ambito si focalizza sulla protezione delle infrastrutture IT, inclusi asset critici come server, reti e dispositivi quali laptop e smartphone istituzionali. Le misure di sicurezza applicate comprendono ad esempio gli standard di definizione e cambio password, le politiche di autenticazione avanzate (es. multi fattore), la gestione della sicurezza delle reti e delle comunicazioni, la configurazione del firewall, lo sviluppo sicuro di sistemi informativi, il controllo degli accessi nei sistemi informativi.
- **Governo della Sicurezza**. Questa area stabilisce i ruoli e le responsabilità del personale nell'utilizzo sicuro degli applicativi e degli asset istituzionali, definendo norme comportamentali e controlli organizzativi e di processo operati dalle Direzioni Staff universitarie. Ad esempio, la verifica delle competenze IT in fase di assunzione, il divieto di condivisione delle credenziali, l'obbligo di accesso ai dati e alle funzionalità solo per necessità lavorative, il divieto di utilizzare soluzioni di memorizzazione non autorizzate, il divieto di installare applicazioni non preventivamente autorizzate dall'Università, l'obbligo di adottare misure crittografiche nella gestione di dati sensibili.

La responsabilità di promuovere e sviluppare il Sistema di Gestione, perseguendo le azioni descritte, è del Consigliere Delegato, che ha inoltre la responsabilità di sviluppare la cultura della sicurezza nelle Direzioni che gli sono sottoposte. Tale responsabilità si estende a tutte le attività amministrative dell'università come specificato nell'Ambito di Applicazione.

Il Consigliere Delegato si avvale delle Direzioni che gli sono sottoposte per attuare gli ambiti di azione, attribuendo specifiche responsabilità per area di competenza, in particolare alla Direzione Technology a cui spetta l'esecuzione di ogni adempimento di carattere tecnologico. In tale contesto il Consigliere Delegato nomina un Responsabile del Sistema di Gestione della Sicurezza delle Informazioni che fungerà da punto di riferimento per la Direzione Technology e le altre Direzioni impattate, garantendo lo sviluppo, il monitoraggio e l'aggiornamento efficace del sistema.

L'università si impegna a promuovere il miglioramento continuo del SGSI, attraverso la regolare revisione e aggiornamento del sistema, delle politiche e delle procedure di valutazione del rischio, in risposta a eventuali cambiamenti significativi o all'emergere di nuove esigenze di sicurezza, garantendo così l'adeguatezza e l'efficacia del sistema nel tempo.

E' responsabilità di tutto il personale staff ed i collaboratori e fornitori coinvolti nelle attività specificate di agire nel rispetto dei requisiti di sicurezza espressi nel Sistema di Gestione della Sicurezza.

Informativa agli Organi di Governance d'Ateneo

Il Consiglio di Amministrazione, l'Organismo di Vigilanza e il Collegio dei Revisori vengono periodicamente informati sull'andamento delle attività, sulla valutazione dei rischi e sull'implementazione dei presidi posti in essere per la loro mitigazione.

Il Consiglio di Amministrazione viene puntualmente informato in caso di particolari criticità che mettono a rischio la sicurezza delle informazioni, la continuità operativa o la mancata compliance alle normative di riferimento, tra cui il mantenimento della certificazione ISO 27001.

L'Organismo di Vigilanza, in particolare, viene informato in caso di criticità relative al rischio di reati informatici previsti dall'D.lgs. 231/2001 per elusione o mancata applicazione dei presidi definiti dal Sistema di Gestione della Sicurezza delle Informazioni.