POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

PRINCIPI E MOTIVAZIONI

Il Sistema Informativo (inclusivo delle risorse tecnologiche - hardware, software, dati, documenti elettronici, reti telematiche – e delle risorse umane dedicate alla loro amministrazione, gestione e utilizzo) rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi di ErgonGroup, in considerazione della criticità dei processi aziendali che dipendono da esso.

ERGONGROUP ha adottato un Sistema di Gestione per la Sicurezza delle Informazioni, cybersecurity e protezione della privacy conforme alla ISO/IEC 27001:2024 e ISO/IEC 27017:2015.

Il presente documento ha l'obiettivo di definire le politiche sui sistemi informativi e la policy sulla sicurezza informatica ed è approvato dalla Direzione e sarà revisionato periodicamente sia in caso di eventi esogeni, quali ad esempio modifiche della normativa esterna ovvero indicazioni delle Autorità, sia di modifiche organizzative ed operative che abbiano impatto sui Sistemi Informativi e sulla sicurezza informatica. Le revisioni sono approvate dalla Direzione.

NORME E STANDARD DI RIFERIMENTO

Il controllo e lo sviluppo del Sistema di Gestione sulla Sicurezza Informazioni viene sviluppato in conformità alle norme:

- UNI CEI EN ISO/IEC 27001:2024;
- UNI CEI EN ISO/IEC 27002:2023;
- ISO/IEC 27017:2015;
- Regolamento Generale sulla Protezione dei Dati (GDPR) - Regolamento UE 2016/679;
- Cybersecurity Act - Regolamento UE 2019/881;
- Codice in materia di protezione dei dati personali - D.Lgs. 196/2003 (modificato dal D.Lgs. 101/2018)

OBIETTIVI di SICUREZZA DELLE INFORMAZIONI

Le informazioni ed i requisiti di sicurezza delle informazioni continueranno ad essere allineati con gli obiettivi aziendali ed il Sistema di Gestione per la Sicurezza delle Informazioni è destinato a essere un meccanismo di abilitazione della condivisione delle informazioni per l'operatività di ErgonGroup e per ridurre i rischi relativi alle informazioni a livelli accettabili considerando anche gli impatti derivanti dai cambiamenti climatici in atto; la scelta strategica aziendale di orientarsi verso l'utilizzo di cloud provider 'green' è in questa ottica.

La presente politica riguarda la gestione e l'utilizzo del sistema informativo in tutti i suoi aspetti e definisce i seguenti obiettivi:

- Protezione della riservatezza, integrità e disponibilità: Garantire che tutte le informazioni trattate siano protette da accessi non autorizzati, alterazioni non intenzionali e indisponibilità, attraverso misure tecniche e organizzative adeguate.
- Gestione efficace dei rischi: assicurare l'identificazione, la valutazione e il trattamento dei rischi relativi alle attività aziendali, incluse le configurazioni dei servizi Microsoft gestiti per i clienti.

- Sicurezza degli accessi e delle identità: applicare controlli di accesso basati sul principio del minimo privilegio, garantendo gestione strutturata delle identità, uso di autenticazioni robuste e verifiche periodiche dei privilegi amministrativi.
- Configurazioni sicure dei prodotti Microsoft: assicurare che tutte le configurazioni applicate ai tenant dei clienti seguano criteri di sicurezza riconosciuti e best practice Microsoft, inclusi logging, audit, protezioni email, gestione identità e hardening dei servizi.
- Protezione dei dati e delle comunicazioni: garantire che i dati aziendali e dei clienti siano protetti tramite controlli adeguati quali cifratura, protezioni delle comunicazioni, criteri di Data Loss Prevention e strumenti nativi Microsoft.
- Gestione strutturata degli incidenti: mantenere un processo efficace di rilevamento, analisi, gestione e documentazione degli incidenti di sicurezza, con comunicazioni tempestive interne ed esterne quando applicabile.
- Continuità operativa: assicurare che le attività interne e le funzioni di supporto ai clienti possano essere mantenute o ripristinate tempestivamente in caso di interruzioni tramite adeguati piani e test periodici.
- Conformità normativa e contrattuale: garantire il rispetto di normative applicabili, requisiti dei clienti, obblighi contrattuali e requisiti definiti dai vendor (es. Microsoft Partner Program, modelli di responsabilità condivisa).
- Formazione e consapevolezza: assicurare che il personale mantenga un adeguato livello di consapevolezza sui rischi informatici, sulle pratiche di sicurezza e sull'uso sicuro delle piattaforme Microsoft.
- Gestione dei fornitori e della supply chain: valutare e monitorare i fornitori critici, in particolare Microsoft e altri partner tecnologici, verificando adeguatezza delle misure di sicurezza, SLA, requisiti contrattuali e rischi associati.

Per perseguire gli obiettivi aziendali, le informazioni devono soddisfare determinati requisiti:

- riservatezza: le informazioni devono essere conosciute solo da coloro che ne hanno il relativo diritto, rispettando il principio del minimo privilegio ("necessità di sapere") in base alle mansioni ricoperte ("necessità di operare");
- integrità: le informazioni devono essere precise e complete, devono rispettare i valori e le aspettative aziendali, e devono essere protette da modifiche e cancellazioni non autorizzate. Per soddisfare tale requisito le informazioni devono essere esatte, aggiornate e leggibili;
- disponibilità: le informazioni devono essere disponibili quando richiesto dai processi aziendali e dai clienti, in maniera efficiente ed efficace;
- efficacia: le informazioni devono essere rilevanti e pertinenti al processo aziendale e, allo stesso tempo, devono essere disponibili tempestivamente, senza errori e fornite in modo da poter essere utilizzate dall'utente;
- efficienza: le informazioni devono essere fornite attraverso l'uso ottimale delle risorse sia dal punto di vista della produttività che della economicità;
- affidabilità: le informazioni devono essere appropriate, in modo da permettere ai vertici aziendali di gestire l'azienda e garantire la corretta assunzione delle decisioni; allo stesso modo le informazioni fornite ai responsabili delle varie funzioni devono permettere loro di espletare le loro funzioni, gli obblighi di produzione del bilancio e tutti i report e relazioni previste dalla normativa interna ed esterna.

La gestione del Sistema Informativo aziendale è svolta da personale qualificato che per esperienza, capacità e affidabilità fornisce garanzia del pieno rispetto delle disposizioni interne e delle normative esterne in materia.

I dati personali devono essere trattati:

- in osservanza dei criteri di riservatezza;
- in modo lecito e secondo correttezza;
- per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e successivamente trattati;
- nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

IMPEGNI

ErgonGroup srl si impegna a preservare la riservatezza, l'integrità e la disponibilità di tutte le informazioni (in formato elettronico e non) in tutta l'organizzazione al fine di mantenere il proprio vantaggio competitivo, solidità economica, redditività, conformità ai requisiti applicabili (legali, contrattuali ed altri) ed immagine commerciale.

MIGLIORAMENTO CONTINUO

ErgonGroup si impegna nel miglioramento continuo del proprio sistema di gestione della Sicurezza delle Informazioni. Per poter gestire in modo adeguato il Sistema Informativo è essenziale un efficace processo di monitoraggio che faciliti la pronta individuazione e correzione di eventuali carenze relative a politiche, processi e procedure. Ciò può ridurre considerevolmente la frequenza e/o gravità degli eventi dannosi.

ErgonGroup si avvale del servizio cloud fornito da Microsoft tramite la piattaforma Azure.

ErgonGroup attiva unità organizzative interne che assicurano l'esecuzione di processi atti a:

- diffondere il contenuto dei servizi, conoscere i punti di forza e di eventuale debolezza;
- assicurare agli utenti formazione e accesso alle funzioni secondo criteri di sicurezza aderenti a principi di sana e prudente gestione o comunque alle politiche di gestione del rischio informatico;
- attivare processi volti alla valorizzazione delle risorse informatiche, intese come leva per il raggiungimento degli obiettivi di ErgonGroup;
- realizzare un sistema di comunicazione dei fabbisogni o delle criticità del Sistema Informativo con l'obiettivo di attivare un processo di miglioramento continuo;
- attuare controlli finalizzati a valutare la capacità dell'azienda di attenersi alle politiche interne;
- individuare tempestivamente deviazioni (anomalie, malfunzionamenti, differenze rispetto a quanto conosciuto/approvato/autorizzato);
- favorire azioni correttive.

ErgonGroup predispone ed implementa il proprio Piano di Continuità Operativa ed il Piano di Disaster Recovery in modo tale da assicurare la protezione dei dati e dei sistemi contro le possibili conseguenze dell'attività di software dannoso (c.d. Malware).

Inoltre, ErgonGroup, tenuto conto della particolare criticità dei ruoli connessi alla gestione del Sistema Informativo, in particolare del ruolo di "Amministratore di Sistema", adotta delle cautele volte a prevenire e ad accertare eventuali utilizzi non in linea con gli obiettivi aziendali del Sistema Informativo, inefficienze dello

stesso, accessi non consentiti ai dati, in specie quelli realizzati con abuso della qualità di Amministratore di Sistema.

ErgonGroup valuta con particolare cura l'attribuzione di funzioni tecniche inerenti la gestione del Sistema Informativo, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile, che possono derivare in caso di incauta o inidonea designazione.

L'attribuzione delle funzioni relative alla gestione del Sistema Informativo o alla gestione delle sue componenti si svolge previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni interne ed esterne anche quelle in materia di trattamento dei dati ivi compreso il profilo relativo alla sicurezza.

Nel ricorso ai servizi dei fornitori esterni, ErgonGroup utilizza analoghi criteri di valutazione di esperienza, capacità ed affidabilità del fornitore nello svolgimento dell'incarico affidato e della garanzia fornita del pieno rispetto delle vigenti disposizioni di legge, anche quelle in materia di trattamento dei dati ivi compreso il profilo relativo alla sicurezza.

GESTIONE POLITICA

La presente Policy di Sicurezza Informatica viene pubblicata sulla intranet aziendale per assicurarne la conoscenza da parte di tutto il personale e viene resa disponibile a tutte le terze parti coinvolte nella gestione di informazioni e componenti del Sistema Informativo.

Nell'eventualità di violazione della presente policy e delle norme attuative, saranno applicate -secondo il caso - le sanzioni previste dal Contratto Collettivo Nazionale applicabile.

La politica sarà riesaminata ogni qualvolta sarà necessario e comunque almeno una volta all'anno.

APPELLO AI LAVORATORI

Tutti i dipendenti dell'organizzazione sono tenuti a rispettare le presenti politiche e l'intero Sistema di Gestione per la Sicurezza delle Informazioni.

Data 18/11/25

Il Presidente del CDA

Daniele Della Bianca