

# Politica per la gestione del rischio di cybersecurity

## 1. Introduzione e Inquadramento Normativo

La sicurezza informatica è una priorità fondamentale per il Gruppo ERCA.

Questa politica stabilisce l'impegno della Direzione ad adottare un "Modello di Cybersecurity", finalizzato a proteggere i sistemi informatici aziendali, nonché le informazioni in essi contenute, da minacce interne ed esterne.

La presente Politica definisce le linee strategiche e operative delle società italiane facenti capo a ERCA Group per garantire un livello elevato di sicurezza delle reti e dei sistemi informativi, in piena conformità al D.Lgs. 4 settembre 2024, n. 138 (denominato Decreto NIS), che recepisce la Direttiva UE 2022/2555.

Lo scopo del presente documento è stabilire i principi per la gestione dei rischi e la resilienza cibernetica, assicurando la continuità operativa e la protezione degli asset digitali.

I principali riferimenti normativi che regolano la conformità del Gruppo sono:

- **D.Lgs. 4 settembre 2024, n. 138:** Quadro normativo primario sulla cybersicurezza nazionale.
- **Determinazione obblighi di base (ACN):** Disciplina le modalità di adempimento agli artt. 23, 24 e 25 del decreto.
- **Allegato 1:** Misure di sicurezza di base per i soggetti importanti.
- **Allegato 3:** Tipologie di incidenti significativi per i soggetti importanti.
- **Determinazione 127434/2026:** Termini perentori per i soggetti inseriti nell'elenco a partire dal 2026.

## 2. Obiettivi

L'adozione di un'efficace "Modello di Cybersecurity" persegue i seguenti obiettivi:

- proteggere le informazioni aziendali da accessi non autorizzati, modifiche, divulgazioni o distruzioni;
- assicurare la continuità operativa, minimizzando i rischi legati alla Cybersecurity;
- conformarsi alle normative e agli standard di sicurezza informatica applicabili;
- contribuire ad incrementare il livello nazionale e comunitario di cybersecurity, a tutela della società e del mercato

## 3. Ambito di applicazione

Le aziende del gruppo si impegnano ad adottare misure tecniche, operative ed organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete, utilizzati nella propria attività o nella fornitura dei propri servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei propri servizi. Le misure adottate sono basate su un approccio multirischio, mirato a proteggere i sistemi IT e comprendono:

- politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
- piani di gestione degli incidenti e condivisione delle informazioni sulle minacce;
- piani di continuità operativa;
- politiche di crittografia per la protezione dei dati critici e sensibili, in transito e a riposo;

- politiche di autenticazione a più fattori per gli accessi critici e procedure di comunicazione sicura in situazioni di emergenza;
- misure di sicurezza nell'acquisizione, nello sviluppo e nella manutenzione dei sistemi informativi, inclusa la gestione delle vulnerabilità;
- criteri di valutazione e gestione del rischio dei fornitori critici.

#### 4. Referente per la Cybersicurezza Nazionale

Ai sensi dell'art. 8 del Decreto NIS, il Gruppo individua al proprio interno un Referente per la Cybersicurezza Nazionale, quale punto di contatto con l'Agenzia per la Cybersicurezza Nazionale (ACN). Il Referente è responsabile della trasmissione delle comunicazioni obbligatorie, del coordinamento delle notifiche di incidente e dell'aggiornamento dei dati anagrafici presso la piattaforma ACN. Il nominativo del Referente è formalizzato in apposito atto della Direzione e comunicato secondo le modalità previste dall'ACN.

#### 5. Responsabilità, formazione, consapevolezza

- Direzione aziendale: esercita il potere decisionale in ambito di Cybersecurity; assegna ruoli e responsabilità; approva le misure di sicurezza; sovrintende alla loro attuazione.
- Personale IT: si occupa dell'implementazione, monitoraggio ed aggiornamento delle misure di sicurezza informatiche.
- Dipendenti: seguono le politiche, le procedure e le regole di sicurezza; partecipano alla formazione sulla sicurezza; segnalano tempestivamente eventuali incidenti.
- Fornitori e terze parti: devono rispettare gli stessi standard di sicurezza applicabili ai dipendenti interni e garantire adeguate misure di protezione.

Le società del gruppo forniranno regolare formazione ed aggiornamenti sulla sicurezza informatica a tutti i dipendenti, per assicurare la consapevolezza e la comprensione delle migliori pratiche di Cybersecurity.

I fornitori verranno selezionati in modo che garantiscano adeguati standard di sicurezza, monitorandone periodicamente il livello di affidabilità. Per i fornitori critici, il Gruppo effettua una valutazione del rischio proporzionata alla criticità del servizio fornito e prevede, nei relativi contratti, requisiti minimi di sicurezza informatica e clausole di verifica.

#### 6. Revisione della politica

L'applicazione della presente politica sarà regolarmente monitorata ed eventualmente integrata, in caso di variazioni significative nelle minacce informatiche o nei requisiti normativi.

La Direzione è pertanto impegnata al miglioramento continuo della propria postura di Cybersecurity, per proteggere le proprie risorse, consolidare la fiducia degli stakeholders e contribuire allo sviluppo, alla sicurezza ed al progresso della società.

La Direzione valuta inoltre con cadenza periodica l'efficacia delle misure di sicurezza adottate, anche mediante attività di verifica e audit interni o esterni, al fine di garantirne l'adeguatezza nel tempo rispetto all'evoluzione delle minacce e dei requisiti normativi.

Grassobbio, 24/09/2026