POLITICA PER LA CYBERSECURITY

Revisione e data	rev. 0 del 15.01.2026
Classificazione	PUBBLICO

Elenco delle revisioni

Revisione e data	Descrizione	Approvazione
rev. 0 del 15.01.2026	Prima emissione	(il rappr. legale p.t.)

Indice

Ghinzelli S.r.l.
Via I° Maggio, 28 (Zona Industriale Gerbolina) – 46019 Viadana (MN) – Italy
Centralino: 0039 0375 780830 – Fax (Amministrazione) 0039 0375 82471 – Fax (Spedizione) 0039 0375 785907
Codice Fiscale e Partita I.V.A. 03531320368

Premessa

La società Ghinzelli Srl riconosce il ruolo cruciale che le informazioni svolgono nei processi aziendali e la loro importanza per il raggiungimento degli obiettivi di business; oggigiorno e sempre di più si utilizzano sistemi informatici che sono interconnessi tra loro e accedono alla rete Internet, oppure sono accessibili anche da remoto attraverso la rete Internet; sebbene tutto questo rappresenta grandi opportunità, il rischio di attacchi ostili o perdita di dati è una minaccia reale e in costante aumento.

Inoltre, Ghinzelli Srl è tenuta agli adempimenti richiesti dal Decreto Legislativo n. 138 del 4 settembre 2024 ("Decreto NIS") in quanto è riconosciuta "soggetto importante" come individuato nell'ambito di applicazione di cui all'art. 3 comma 1 del Decreto NIS; pertanto, questa politica rappresenta il punto iniziale per l'implementazione del proprio modello organizzativo per la cybersecurity, in conformità ai requisiti del Decreto NIS che viene identificato e recepito quale framework normativo di riferimento.

Per lo scopo di questa politica, il termine cybersecurity utilizzato in questo documento ha il significato equivalente di sicurezza informatica.

1. Riferimenti legislativi e normativi

- DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022*, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.* (di seguito, "direttiva NIS2");
- DECRETO LEGISLATIVO 4 settembre 2024, n. 138 - *Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148* (di seguito "decreto NIS").

1.1. Riferimenti al Framework NIS2

Funzioni interessate	Categorie
GOVERNO - (GV) La strategia di gestione del rischio di cybersecurity dell'organizzazione, i suoi obiettivi e le relative policy sono stabilite, comunicate e monitorate.	**POLITICA (GV.PO):** La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.

Ghinzelli S.r.l.
Via I° Maggio, 28 (Zona Industriale Gerbolina) – 46019 Viadana (MN) – Italy
Centralino: 0039 0375 780830 – Fax (Amministrazione) 0039 0375 82471 – Fax (Spedizione) 0039 0375 785907
Codice Fiscale e Partita I.V.A. 03531320368

2. Scopo ed applicazione

Questa politica stabilisce l'impegno di Ghinzelli Srl verso l'adozione di un modello organizzativo per la cybersecurity, finalizzato a proteggere da minacce interne ed esterne i sistemi informatici e le reti e le informazioni trattate nei processi aziendali, attraverso la definizione di requisiti minimi per la cybersecurity con lo scopo di tutelare e garantire la sicurezza delle informazioni, la proprietà intellettuale ed il vantaggio commerciale, dalle conseguenze derivanti da eventuali incidenti ed altri eventi negativi che possono colpire i sistemi informatici aziendali e le informazioni che vi sono trattate.

L'adozione di un'efficace modello organizzativo di cybersecurity vuole perseguire i seguenti obiettivi:

- proteggere le informazioni aziendali da accessi e modifiche non autorizzati, perdita o distruzione o alterazione, per garantirne i requisiti di integrità, riservatezza e disponibilità;
- assicurare la continuità operativa, minimizzando i rischi legati alla cybersecurity;
- conformarsi alle normative e agli standard di sicurezza applicabili;
- contribuire ad incrementare il livello di sicurezza dell'organizzazione e dei propri sistemi informatici, a tutela di tutte le parti interessate.

Questa politica si applica a tutti i dipendenti, collaboratori, fornitori e terze parti che utilizzano gli strumenti informatici aziendali e accedono ai nostri sistemi informatici ed alle reti aziendali.

3. Principi di cybersecurity

Questa azienda si impegna ad attuare le adeguate misure di sicurezza, tecnologiche ed organizzative, che devono essere proporzionate ai rischi individuati per la sicurezza delle informazioni, dei sistemi informativi e delle reti, allo scopo di prevenire o ridurre al minimo l'impatto degli incidenti e garantire la continuità dei processi aziendali.

Le misure di sicurezza adottate, basate su un approccio multirischio, sono mirate a proteggere i sistemi informatici e comprendono:

- politiche e procedure per la valutazione ed il trattamento dei rischi alla sicurezza delle informazioni;
- istruzioni e procedure per la gestione degli accessi ai sistemi informatici ed alla reti;
- istruzioni e procedure per l'uso accettabile degli strumenti informatici;
- politiche e procedure per la corretta gestione delle informazioni secondo classificazione e valore;
- procedure di gestione degli incidenti e condivisione delle informazioni sulle minacce e vulnerabilità;
- piani per la continuità operativa;
- misure di sicurezza tecnologiche applicate a strumenti e sistemi informatici ed alla reti.

Ghinzelli S.r.l.
Via I° Maggio, 28 (Zona Industriale Gerbolina) – 46019 Viadana (MN) – Italy
Centralino: 0039 0375 780830 – Fax (Amministrazione) 0039 0375 82471 – Fax (Spedizione) 0039 0375 785907
Codice Fiscale e Partita I.V.A. 03531320368

4. Responsabilità

L'amministratore unico di Ghinzelli Srl, che rappresenta gli organi di amministrazione e direttivi ovvero la direzione aziendale, esercita il potere decisionale per adempiere ai requisiti del decreto NIS, assegna ruoli e responsabilità, accetta i rischi e approva i piani per il loro trattamento e le misure di sicurezza, fornisce le risorse necessarie per la loro implementazione e sovraintende alla loro attuazione.

La direzione aziendale è responsabile per fornire al personale interessato la formazione adeguata e regolarmente aggiornata in merito alla sicurezza informatica, al fine di assicurare la necessaria consapevolezza e la comprensione delle migliori pratiche di cybersecurity.

Il personale incaricato della gestione degli strumenti informatici, avvalendosi del supporto dei fornitori selezionati e specificamente designati, è responsabile dell'implementazione, aggiornamento e monitoraggio delle misure di sicurezza tecnologiche per la sicurezza informatica.

I dipendenti e collaboratori che usano i sistemi informatici e le reti sono responsabili dell'osservanza e dell'applicazione di questa politica, delle procedure e delle regole di sicurezza che vengono loro comunicate; sono informati ed istruiti sui rischi e sulle minacce informatiche che possono affrontare e su come reagire quando si imbattono in attività sospette; sono tenuti alla segnalazione di anomalie, incidenti o disservizi inerenti alla sicurezza delle informazioni di cui dovessero venire a conoscenza.

Il personale esterno, i fornitori e le terze parti che hanno relazioni con i nostri sistemi informatici, ovvero che accedono alle nostre reti, devono rispettare gli stessi standard di sicurezza dei nostri dipendenti e collaboratori e devono garantire le necessarie misure di sicurezza e protezione; Ghinzelli Srl si impegna alla selezione di fornitori che garantiscono gli adeguati standard di sicurezza, monitorandone il livello di affidabilità.

Ogni persona che sarà responsabile di qualsiasi atto deliberato per mettere a rischio la sicurezza delle informazioni gestite con i sistemi informatici e le reti di Ghinzelli Srl, sarà soggetta alle opportune azioni disciplinari e/o legali secondo la gravità del caso.

5. Revisione della politica di cybersecurity

Ghinzelli Srl si impegna al miglioramento continuo del proprio modello organizzativo di cybersecurity, allo scopo di garantire la protezione delle proprie risorse e delle informazioni, per consolidare la fiducia delle parti interessate e contribuire allo sviluppo, alla sicurezza ed al progresso della propria organizzazione.

L'applicazione di questa politica verrà regolarmente monitorata e sarà eventualmente aggiornata o integrata, in caso di variazioni significative delle minacce informatiche, modifiche ai sistemi informatici aziendali, cambiamenti dei requisiti normativi.

6. Comunicazione della politica di cybersecurity

La direzione aziendale stabilisce che questa politica sia divulgata alle parti interessate con le modalità più opportune e sia resa pubblicamente disponibile attraverso il sito web aziendale.

Ghinzelli S.r.l.
Via I° Maggio, 28 (Zona Industriale Gerbolina) – 46019 Viadana (MN) – Italy
Centralino: 0039 0375 780830 – Fax (Amministrazione) 0039 0375 82471 – Fax (Spedizione) 0039 0375 785907
Codice Fiscale e Partita I.V.A. 03531320368