

POL Politica di sicurezza delle informazioni

v1 del 12/01/2026

Obiettivi di sicurezza delle informazioni

Cotril S.p.A. persegue i seguenti obiettivi strategici per la sicurezza delle informazioni, coerenti con la propria missione aziendale e con il contesto normativo in cui opera:

- Proteggere la riservatezza, l'integrità e la disponibilità del patrimonio informativo aziendale, a presidio della continuità dei processi di progettazione, produzione e distribuzione.
- Adottare un approccio sistematico alla gestione del rischio di sicurezza informatica, proporzionato alla natura, alla dimensione e alla complessità delle attività e dei servizi svolti.
- Assicurare la piena conformità ai requisiti normativi e regolamentari applicabili, con particolare riguardo a ISO/IEC 27001:2022, alla Direttiva (UE) 2022/2555 e al D.Lgs. 138/2024.
- Mantenere un elenco aggiornato dei sistemi informativi e di rete rilevanti e delle attività e dei servizi categorizzati ai sensi della Determinazione ACN 379907/2025, documentati nel *MOD Censimento risorse, infrastrutture, asset* e nel *MOD Categorizzazione delle attività e dei servizi NIS*.
- Promuovere la consapevolezza e la competenza del personale in materia di sicurezza informatica e di igiene digitale di base.
- Favorire il miglioramento continuo dell'efficacia dei controlli di sicurezza, attraverso la misurazione, il monitoraggio, l'audit interno e il riesame della direzione.
- Garantire la resilienza dei servizi critici e la capacità di risposta tempestiva agli incidenti di sicurezza delle informazioni.

Principi fondamentali di sicurezza delle informazioni

Cotril S.p.A. adotta e documenta politiche di sicurezza informatica per ciascuno degli ambiti previsti dalla Determinazione ACN 379907/2025, in coerenza con i requisiti di ISO/IEC 27001:2022 e del D.Lgs. 138/2024. I principi che seguono esprimono l'orientamento dell'organizzazione per ciascun ambito e trovano attuazione nelle politiche, nelle procedure e nelle istruzioni operative del SGI. Le politiche di sicurezza sono approvate dagli organi di amministrazione e direttivi e rese note alle articolazioni competenti dell'organizzazione, nel rispetto del principio della necessità di conoscere.

L'organizzazione definisce e mantiene una struttura organizzativa dedicata alla sicurezza informatica, i cui ruoli, responsabilità e poteri sono chiaramente assegnati e comunicati. L'elenco del personale con specifici compiti in materia di sicurezza è mantenuto aggiornato e comprende il **Punto di contatto NIS2**, il **Sostituto punto di contatto NIS2** e il **Contatto CSIRT**. Ruoli e responsabilità sono riesaminati con cadenza almeno biennale e aggiornati in caso di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce. L'assegnazione dettagliata dei compiti è formalizzata nella *POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni* e nella *PRO Procedura dei ruoli e responsabilità*.

Cotril S.p.A.

Soggetta a direzione e coordinamento da parte di Artesani S.r.l.

Via Trento, 59 – 20021 Ospiate di Bollate (MI) – Italia – Tel. 02.38.34.32.1 r.a. – Fax 02.38.34.32.31

P. Iva / Codice fiscale / Reg. Imp. Milano 06260170961 – R.E.A. 1880322 / Cap. Soc. € 3.000.000,00 i.v.

www.cotril.it | info@cotril.it

Gestione del rischio

L'organizzazione fonda la protezione del proprio patrimonio informativo su un approccio basato sul rischio, adottando una metodologia strutturata che considera la probabilità di occorrenza e l'impatto potenziale degli eventi avversi. I rischi identificati sono trattati mediante mitigazione, accettazione, trasferimento o eliminazione; l'accettazione del rischio residuo, compresi i relativi piani di trattamento, è riservata al **CEO** per conto degli organi di amministrazione e direttivi. La valutazione del rischio è condotta almeno annualmente e aggiornata a seguito di incidenti significativi, variazioni organizzative o mutamenti del panorama delle minacce. Principi, metodologia e responsabilità operative sono definiti nella *POL Politica di gestione del rischio* e nella *PRO Procedura di gestione dei rischi*.

Affidabilità delle risorse umane

Cotril S.p.A. riconosce che l'affidabilità del personale costituisce un presupposto essenziale per la protezione degli asset informativi. In fase di selezione, l'organizzazione verifica l'identità e le referenze professionali dei candidati; per i ruoli che accedono a sistemi informativi e di rete rilevanti o a informazioni classificate come confidenziali, sono previsti controlli aggiuntivi proporzionati al livello di rischio, nel rispetto della normativa sulla protezione dei dati personali. L'estensione di tali controlli è documentata in coerenza con la Determinazione ACN 379907/2025. Gli amministratori di sistema sono individuati previa valutazione dell'esperienza, delle capacità e dell'affidabilità e sono tenuti a garantire il pieno rispetto della normativa in materia di sicurezza informatica.

Il rapporto di lavoro è formalizzato mediante contratto che include gli obblighi di riservatezza, l'accettazione del *Codice di condotta* e l'impegno al rispetto delle politiche di sicurezza del SGI. Durante l'onboarding, il personale riceve la documentazione sulle regole aziendali, sulla protezione dei dati personali e sulle politiche di sicurezza delle informazioni. Al cambio di ruolo o alla cessazione del rapporto, l'organizzazione attiva la revoca tempestiva degli accessi, la restituzione degli asset e la conferma degli obblighi di riservatezza che permangono dopo la conclusione del rapporto, in coerenza con quanto previsto dal D.Lgs. 138/2024. Le modalità operative sono descritte nella *PRO Procedura di gestione delle risorse umane*.

Gestione degli asset e uso accettabile delle informazioni

L'organizzazione censisce e classifica i propri asset informativi, ne attribuisce la responsabilità e ne governa l'intero ciclo di vita, dalla presa in carico alla dismissione sicura. L'assegnazione degli asset al personale è documentata attraverso il *MOD Modulo di assegnazione dei beni*; alla cessazione del rapporto, la restituzione è formalizzata mediante il *MOD Modulo di restituzione dei beni*.

Cotril S.p.A. esige che tutto il personale utilizzi le informazioni e le risorse associate esclusivamente in modo conforme alla loro classificazione e alle regole stabilite dal SGI. Ciascun membro del personale aderisce a tutte le politiche del sistema di gestione della sicurezza delle informazioni, comprese quelle relative alla gestione delle credenziali, alla classificazione delle informazioni e alla protezione dei dispositivi assegnati. L'uso responsabile delle risorse aziendali è un obbligo contrattuale, e violazioni gravi comportano conseguenze disciplinari proporzionate alla gravità dell'infrazione. I criteri di classificazione, le regole di etichettatura e i requisiti di protezione per

Cotril S.p.A.

Soggetta a direzione e coordinamento da parte di Artesani S.r.l.

Via Trento, 59 – 20021 Ospiate di Bollate (MI) – Italia - Tel. 02.38.34.32.1 r.a. – Fax 02.38.34.32.31

P. Iva / Codice fiscale / Reg. Imp. Milano 06260170961 – R.E.A. 1880322 / Cap. Soc. € 3.000.000,00 i.v.

www.cotril.it | info@cotril.it

COTRIL

ciascun livello sono stabiliti nella *POL Politica di classificazione ed etichettatura delle informazioni*; il ciclo di vita degli asset è disciplinato nella *PRO Procedura di configurazione, gestione e smaltimento degli asset*.

Gestione dell'autenticazione, delle identità digitali e del controllo degli accessi

Cotril S.p.A. adotta il principio del minimo privilegio e il controllo degli accessi basato sui ruoli, affinché ogni utente disponga esclusivamente delle abilitazioni necessarie allo svolgimento delle proprie mansioni. Le credenziali sono strettamente personali e gli account amministrativi sono riconducibili a un singolo individuo. I diritti di accesso sono sottoposti a revisione periodica; la creazione, la modifica e la revoca delle utenze avvengono su richiesta interna formalizzata. Le modalità operative sono disciplinate nella *PRO Procedura di gestione e controllo degli accessi logici*.

Sicurezza dei dati

L'organizzazione tutela i propri dati lungo l'intero ciclo di vita, dalla creazione alla cancellazione sicura, adottando misure di protezione proporzionate al livello di classificazione attribuito. Le informazioni sono classificate ed etichettate secondo un sistema a tre livelli di riservatezza; per ciascun livello sono definiti requisiti specifici per il trattamento, la trasmissione e la conservazione. L'impiego della crittografia è regolato da criteri che indirizzano la selezione di algoritmi robusti e la gestione dell'intero ciclo di vita delle chiavi crittografiche. Principi e modalità operative sono contenuti nella *POL Politica di classificazione ed etichettatura delle informazioni*, nella *POL Politica di conservazione e cancellazione delle informazioni* e nella *PRO Procedura di crittografia e gestione delle chiavi crittografiche*.

Sicurezza operativa e gestione delle vulnerabilità

Cotril S.p.A. è impegnata a garantire il funzionamento sicuro e resiliente dei propri sistemi e delle proprie infrastrutture informatiche. L'organizzazione definisce controlli per la gestione dei backup, la registrazione e il monitoraggio degli eventi di sicurezza, la gestione delle vulnerabilità tecniche e il governo dei cambiamenti. Promuove regole di scrivania e schermo puliti per prevenire l'esposizione non autorizzata di informazioni su scrivanie e monitor non presidiati. Il personale è tenuto ad assicurare che le comunicazioni riguardanti informazioni aziendali classificate avvengano esclusivamente attraverso i canali autorizzati dall'organizzazione, e a garantire il blocco dello schermo ogni volta che la postazione di lavoro resta incustodita. Il lavoro da remoto è consentito nel rispetto di specifiche misure di protezione, tra cui l'utilizzo obbligatorio della VPN aziendale, l'autenticazione a più fattori e l'adozione di accorgimenti per impedire la visione dello schermo da parte di persone non autorizzate. Principi e controlli operativi sono dettagliati nella *POL Politica di sicurezza operativa*.

Sicurezza fisica e ambientale

L'organizzazione protegge le aree fisiche in cui sono trattate le informazioni aziendali e in cui sono ospitate le apparecchiature di elaborazione, presso la sede di Via Trento n. 59, Bollate (MI). Perimetri di sicurezza e aree ad accesso controllato sono presidiati mediante un sistema di badge

Cotril S.p.A.

Soggetta a direzione e coordinamento da parte di Artesani S.r.l.

Via Trento, 59 – 20021 Ospiate di Bollate (MI) – Italia – Tel. 02.38.34.32.1 r.a. – Fax 02.38.34.32.31

P. Iva / Codice fiscale / Reg. Imp. Milano 06260170961 – R.E.A. 1880322 / Cap. Soc. € 3.000.000,00 i.v.

www.cotril.it | info@cotril.it



COTRIL

con codice univoco assegnato a ciascun dipendente; la sede è dotata di impianto di allarme e telecamere perimetrali. Le apparecchiature critiche sono collocate in ambienti protetti da rischi ambientali e da accessi non autorizzati, e sono soggette a manutenzione periodica. I visitatori sono identificati e la loro presenza è tracciata mediante un registro all'ingresso della sede. Le procedure operative sono definite nella *PRO Procedura di sicurezza fisica e ambientale*.

Protezione delle reti e delle comunicazioni

Cotril S.p.A. adotta misure di protezione della propria rete aziendale fondate su principi di segmentazione, hardening dei dispositivi e controllo dei flussi di traffico. La documentazione della topologia di rete è mantenuta aggiornata e i cambiamenti alle configurazioni dei dispositivi di rete sono gestiti in modo controllato e autorizzato. Le modalità operative sono descritte nella *PRO Procedura di gestione della sicurezza della rete*.

Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete

L'organizzazione gestisce la configurazione, la manutenzione e la dismissione sicura dei propri sistemi informativi e di rete secondo criteri che tutelano la sicurezza in ogni fase del ciclo di vita. I cambiamenti ai sistemi e alle infrastrutture sono valutati sotto il profilo dell'impatto sulla sicurezza, formalmente autorizzati e monitorati nel tempo. Le modalità operative sono disciplinate nella *PRO Procedura di configurazione, gestione e smaltimento degli asset* e nella *PRO Procedura di gestione del cambiamento*.

Formazione e consapevolezza in sicurezza delle informazioni

L'organizzazione promuove una cultura della sicurezza delle informazioni attraverso attività strutturate di formazione e sensibilizzazione, rivolte a tutto il personale e ai collaboratori esterni con accesso a informazioni aziendali. In fase di onboarding, ciascun nuovo membro del personale riceve la documentazione relativa alla normativa interna, alla protezione dei dati personali e alle regole aziendali, accompagnata da una presentazione dei requisiti di sicurezza. Il piano formativo è definito annualmente in funzione dei ruoli, dei rischi identificati e dell'evoluzione delle minacce; prevede sessioni di aggiornamento periodico, formazione specifica per i ruoli critici e iniziative di sensibilizzazione ricorrenti. La partecipazione è tracciata e l'efficacia della formazione viene verificata.

Il piano copre in modo esplicito i temi previsti dalla Determinazione ACN 379907/2025, con particolare riferimento alla gestione degli incidenti, agli obblighi di notifica e ai comportamenti di igiene informatica di base. Le modalità operative sono descritte nella *PRO Procedura di gestione delle risorse umane*.

Sicurezza della catena di approvvigionamento ICT

Cotril S.p.A. governa il rischio di sicurezza informatica derivante dai propri fornitori e dalle terze parti che accedono a sistemi, dati o servizi rilevanti. L'organizzazione mantiene un inventario dei fornitori con relativa classificazione di criticità, determinata in base al servizio erogato, al livello di accesso ai

Cotril S.p.A.

Soggetta a direzione e coordinamento da parte di Artesani S.r.l.

Via Trento, 59 – 20021 Ospiate di Bollate (MI) – Italia - Tel. 02.38.34.32.1 r.a. – Fax 02.38.34.32.31

P. Iva / Codice fiscale / Reg. Imp. Milano 06260170961 – R.E.A. 1880322 / Cap. Soc. € 3.000.000,00 i.v.

www.cotril.it | info@cotril.it



COTRIL

sistemi e ai dati trattati. Per i fornitori qualificati come critici o con livello di rischio medio-alto, sono definiti requisiti minimi di sicurezza, formalizzati attraverso clausole contrattuali specifiche che comprendono misure tecniche e organizzative, obblighi di notifica di incidenti e vulnerabilità, diritti di audit e condizioni di uscita.

La qualifica e il monitoraggio dei fornitori sono ripetuti periodicamente e in occasione di eventi rilevanti, quali incidenti, cambi di ambito o variazioni nella catena dei sub-fornitori. I fornitori rilevanti ai fini NIS sono identificati e sottoposti alla valutazione prevista dalla Determinazione ACN 379907/2025 in materia di gestione del rischio della catena di approvvigionamento. Le modalità operative sono definite nella *PRO Procedura di gestione degli acquisti e delle terze parti*.

Continuità operativa, ripristino in caso di disastro e gestione delle crisi

L'organizzazione è impegnata a garantire la resilienza dei propri servizi critici e la capacità di ripristino rapido a seguito di eventi avversi che possano compromettere la disponibilità dei sistemi informativi e di rete. Cotril S.p.A. identifica le funzioni essenziali, stabilisce gli obiettivi di ripristino e mantiene piani di continuità operativa e di ripristino di emergenza sottoposti a test periodici. I principi e gli impegni strategici sono espressi nella *POL Politica di continuità operativa*; le modalità operative sono disciplinate nella *PRO Procedura di continuità operativa e di ripristino di emergenza*.

Monitoraggio degli eventi di sicurezza

Cotril S.p.A. adotta strumenti e processi per la rilevazione e l'analisi degli eventi di sicurezza generati dai propri sistemi informativi e di rete. I log di sicurezza sono raccolti, protetti e conservati in modo da consentire la ricostruzione di attività anomale e l'indagine su potenziali incidenti. Principi e controlli per il monitoraggio sono definiti nella *POL Politica di sicurezza operativa*.

Segnalazione degli eventi e risposta agli incidenti

L'organizzazione mette a disposizione del personale canali dedicati per la segnalazione tempestiva di eventi di sicurezza delle informazioni osservati o sospetti. Ogni membro del personale comunica senza ritardo qualsiasi anomalia, tentativo di accesso non autorizzato o comportamento sospetto attraverso i canali stabiliti. Gli incidenti sono classificati per gravità e gestiti attraverso un ciclo strutturato di contenimento, eradicazione, ripristino e analisi post-incidente.

In caso di incidenti significativi ai sensi della Direttiva (UE) 2022/2555, il **Contatto CSIRT** effettua le notifiche al CSIRT Italia nei tempi previsti dalla normativa; per le violazioni che coinvolgono dati personali, l'organizzazione ottempera agli obblighi di comunicazione previsti dal Reg. (UE) 2016/679. Le modalità operative sono definite nella *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni*.

Conformità e audit di sicurezza

L'organizzazione mantiene un registro aggiornato dei requisiti normativi, contrattuali e regolamentari applicabili in materia di sicurezza delle informazioni, documentato nel *MOD Elenco norme*, e ne verifica periodicamente l'osservanza. Audit interni sono pianificati e condotti con cadenza almeno

Cotril S.p.A.

Soggetta a direzione e coordinamento da parte di Artesani S.r.l.

Via Trento, 59 – 20021 Ospiate di Bollate (MI) – Italia - Tel. 02.38.34.32.1 r.a. – Fax 02.38.34.32.31

P. Iva / Codice fiscale / Reg. Imp. Milano 06260170961 – R.E.A. 1880322 / Cap. Soc. € 3.000.000,00 i.v.

www.cotril.it | info@cotril.it



COTRIL

annuale per accertare l'efficacia dei controlli implementati, l'aderenza alle politiche e alle procedure e la conformità complessiva del SGI. Gli esiti degli audit, comprese le non conformità rilevate e le azioni correttive adottate, sono documentati nel *MOD Rapporto di audit* e sottoposti al riesame della direzione.

Cotril S.p.A. definisce e attua un piano di adeguamento, approvato dagli organi di amministrazione e direttivi, che identifica gli interventi necessari ad assicurare la piena attuazione delle politiche di sicurezza. Parallelamente, mantiene un piano per la valutazione dell'efficacia delle misure di gestione del rischio, comprensivo dei metodi di valutazione impiegati. Gli esiti di entrambi i piani sono comunicati periodicamente agli organi di amministrazione e direttivi mediante apposite relazioni. L'organizzazione coopera con le autorità competenti nei casi previsti dalla normativa, in conformità alla Determinazione ACN 379907/2025.

Protezione degli asset fuori sede

Cotril S.p.A. riconosce la necessità di proteggere gli asset informativi anche quando sono utilizzati al di fuori della propria sede. Sono considerati asset fuori sede, a titolo esemplificativo, notebook e dispositivi mobili in uso durante lo smart working o in trasferta, supporti fisici consegnati a consulenti o fornitori e documenti cartacei trasportati per esigenze operative.

L'organizzazione si impegna a garantire che tali asset siano custoditi con la medesima attenzione riservata a quelli presenti in sede, e promuove i seguenti principi:

- **Custodia:** gli asset non sono lasciati incustoditi in auto, mezzi pubblici o aree comuni di hotel e coworking. In trasferta, il personale assegnatario li custodisce nella cassaforte della struttura ospitante o in altro luogo chiuso a chiave.
- **Trasporto:** l'asset è trasportato in custodia personale. Per consegne a consulenti, fornitori o sedi distaccate l'organizzazione prevede il ricorso a un corriere tracciato.
- **Segnalazione di smarrimento, furto o danneggiamento:** il personale notifica immediatamente al **Responsabile del Sistema di Gestione**, e in ogni caso entro 24 ore dall'accadimento, qualunque smarrimento, furto o danneggiamento di asset aziendali fuori sede. La segnalazione attiva le procedure di blocco remoto del dispositivo, revoca degli accessi e modifica delle credenziali; l'evento è registrato come incidente di sicurezza delle informazioni.
- **Restituzione:** al termine della trasferta, del progetto o del rapporto di lavoro, l'asset è restituito all'organizzazione e la restituzione è formalizzata mediante il *MOD Modulo di restituzione dei beni*.

Il personale che opera da remoto è tenuto a rispettare le misure di protezione delle postazioni remote stabilite nella *POL Politica di sicurezza operativa*, compreso l'uso della VPN aziendale e l'obbligo di non lasciare i dispositivi incustoditi in luoghi pubblici o veicoli.

Cotril S.p.A.

Soggetta a direzione e coordinamento da parte di Artesani S.r.l.

Via Trento, 59 – 20021 Ospiate di Bollate (MI) – Italia - Tel. 02.38.34.32.1 r.a. – Fax 02.38.34.32.31

P. Iva / Codice fiscale / Reg. Imp. Milano 06260170961 – R.E.A. 1880322 / Cap. Soc. € 3.000.000,00 i.v.

www.cotril.it | info@cotril.it

