POL Politica di sicurezza operativa

Storia della versione

Versione	Data	Autore	Approvato da
1	28/04/2026	Glauco Timoteo	William Palozzo

Indice

Scopo

La presente politica ha lo scopo di garantire il funzionamento corretto, sicuro e resiliente di tutti i sistemi, le reti e le strutture di elaborazione delle informazioni di DG Impianti Industriali S.p.A. Essa definisce i controlli e le disposizioni necessarie per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni durante le operazioni quotidiane, riducendo al minimo i rischi di interruzione del servizio, perdita di dati e incidenti di sicurezza. Questa politica opera in sinergia con le altre politiche e procedure del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e traduce in regole operative gli impegni assunti dal Top Management. Il suo rispetto è condizione imprescindibile per la tutela del patrimonio informativo aziendale e per il mantenimento della fiducia dei clienti e dei partner — sia pubblici che privati — con cui l'organizzazione collabora nei settori energia, oil & gas, petrolchimico e farmaceutico. Le procedure operative per le strutture di elaborazione delle informazioni devono essere documentate e rese disponibili a tutto il personale che ne abbia necessità.

Campo di applicazione

La presente politica si applica a tutti i sistemi informativi di DG Impianti Industriali S.p.A., inclusi server, postazioni di lavoro, dispositivi mobili, reti, applicazioni e servizi cloud utilizzati per le attività aziendali. L'ambito copre entrambe le sedi operative: la sede legale di Via Napo Torriani n. 22 a Milano e l'ufficio operativo di Via Antonio Vivaldi n. 4 a Montesilvano (PE).

Sono destinatari della presente politica tutti i dipendenti, i collaboratori, i consulenti e le terze parti che accedono, anche temporaneamente, alle risorse informatiche e alle informazioni dell'organizzazione. Le regole qui stabilite si applicano indipendentemente dalla modalità di accesso — sia essa in sede, da remoto o tramite dispositivi mobili.

Riferimenti normativi

- **ISO/IEC 27001:2022** — Requisiti per i sistemi di gestione della sicurezza delle informazioni.
- **ISO/IEC 27002:2022** — Linee guida per i controlli di sicurezza delle informazioni.
- **Regolamento (UE) 2016/679 (GDPR)** — Protezione delle persone fisiche con riguardo al trattamento dei dati personali.
- **D.Lgs. 196/2003** — Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. 101/2018.

Termini e definizioni

- **Backup** — Copia dei dati eseguita per finalità di ripristino in caso di perdita o danneggiamento dell'originale.

- **BYOD (Bring Your Own Device)** — Utilizzo di dispositivi personali del dipendente per accedere a risorse aziendali.
- **Log** — Registrazione cronologica degli eventi che si verificano in un sistema informatico.
- **MDM (Mobile Device Management)** — Soluzione software per la gestione centralizzata dei dispositivi mobili.
- **MFA (Multi-Factor Authentication)** — Autenticazione a più fattori che richiede almeno due metodi distinti di verifica dell'identità.
- **PII (Personally Identifiable Information)** — Qualsiasi informazione che possa identificare direttamente o indirettamente una persona fisica.
- **RBAC (Role-Based Access Control)** — Modello di controllo degli accessi basato sui ruoli assegnati agli utenti.
- **RPO (Recovery Point Objective)** — Quantità massima di dati che può essere persa, misurata in tempo, a causa di un incidente.
- **RTO (Recovery Time Objective)** — Tempo massimo accettabile entro cui un sistema deve essere ripristinato dopo un'interruzione per evitare conseguenze inaccettabili.
- **SIEM (Security Information and Event Management)** — Piattaforma che centralizza la raccolta, la correlazione e l'analisi degli eventi di sicurezza provenienti da diverse fonti.
- **Vulnerabilità** — Debolezza di un sistema che può essere sfruttata da una minaccia per causare un danno.

Ruoli e responsabilità

- **ICT-RSGSI** — Supervisiona la conformità complessiva della presente politica e implementa e gestisce i controlli tecnici in essa descritti, quali i sistemi di backup, la protezione antimalware, la configurazione dei log, il monitoraggio delle reti e la gestione delle vulnerabilità; gestisce inoltre le richieste di eccezione e i casi di violazione.
- **Responsabile del sistema di gestione** — Supporta il mantenimento della documentazione relativa alla presente politica, ne verifica la coerenza con il quadro normativo e con le procedure del sistema di gestione e collabora alla pianificazione degli audit interni sulla sicurezza operativa.
- **Dipendenti e Collaboratori** — Ciascun dipendente e collaboratore è tenuto a rispettare le regole di uso accettabile definite dalla presente politica, a proteggere le proprie credenziali di autenticazione e a segnalare immediatamente qualsiasi anomalia o sospetto incidente di sicurezza al ruolo ICT-RSGSI.

Backup

DG Impianti Industriali S.p.A. adotta una strategia di backup e ripristino completa per garantire la continuità operativa e la disponibilità dei dati critici. Per ciascun sistema critico devono essere definiti e documentati precisi obiettivi di RTO e RPO, in coerenza con l'analisi d'impatto sulle attività condotta nell'ambito della *PRO Procedura di continuità operativa e di ripristino di emergenza* .

L'organizzazione esegue backup giornalieri automatizzati delle macchine virtuali ospitate nell'infrastruttura Private Cloud mediante tecnologia Veeam Backup and Replication. La politica di retention prevede la conservazione degli ultimi sette giorni di backup, con esecuzione pianificata su base quotidiana. I dati di backup sono conservati presso un data center geograficamente separato dall'ambiente di produzione, su storage SSD protetto da RAID hardware e dotato di meccanismi di immutabilità del dato per la difesa contro attacchi ransomware. È inoltre attiva la replica del repository di backup su un secondo sito, in conformità con il principio 3-2-1: tre copie del dato, su due supporti differenti e una copia off-site.

Tutti i dati di backup, sia in transito che a riposo, devono essere protetti tramite crittografia e l'accesso ai sistemi di backup è strettamente controllato tramite credenziali personali e un modello di autorizzazione basato sul principio del minimo privilegio. Le notifiche automatiche relative all'esito dei processi di backup — successo, avviso ed errore — devono essere inviate al personale ICT-RSGSI per garantire la tempestiva rilevazione di anomalie. L'integrità e l'efficacia dell'intero processo vengono validate tramite test periodici di ripristino, effettuati almeno una volta all'anno o in caso di modifiche significative all'infrastruttura. I risultati di tali test devono essere documentati e conservati come evidenza del SGSI.

Ridondanza delle strutture di elaborazione

L'organizzazione deve pianificare i propri sistemi affinché il livello di disponibilità necessario sia raggiunto in conformità con i requisiti di business. L'infrastruttura cloud è progettata con componenti ridondanti — server con doppia alimentazione, doppio sistema di raffreddamento, RAM ECC e doppio switch di accesso configurato in alta affidabilità. La topologia di rete e le scelte architetturali per la ridondanza devono essere documentate nel *MOD Diagramma di rete* e riesaminate periodicamente in sede di riesame della direzione.

Protezione dei dati personali

L'organizzazione si impegna a proteggere i dati personali (PII) e gli altri dati sensibili attraverso misure tecniche e organizzative adeguate, al fine di garantire la conformità al GDPR e alla normativa nazionale applicabile. Il *MOD Registro dei trattamenti del titolare* costituisce lo strumento primario per documentare le attività di trattamento e i relativi presidi di sicurezza.

Dove necessario e sulla base di una valutazione del rischio, devono essere implementate tecniche quali il mascheramento dei dati, la pseudonimizzazione o l'anonimizzazione per proteggere efficacemente le informazioni personali. Tali metodi sono progettati per interrompere o attenuare il legame tra i dati e gli individui a cui si riferiscono, utilizzando tecniche come la crittografia, l'annullamento di caratteri o la sostituzione di valori con i relativi hash.

La progettazione dei sistemi e delle query di accesso ai dati deve sempre seguire il principio di minimizzazione, esponendo agli utenti soltanto le informazioni strettamente necessarie per lo svolgimento delle proprie funzioni. Le registrazioni aziendali — comprese quelle relative al trattamento dei dati personali — devono essere protette da perdita, distruzione, falsificazione, accesso non autorizzato e diffusione non autorizzata, in

conformità con i criteri di conservazione definiti nel *MOD Conservazione delle informazioni e degli asset* .

Gestione dei log

Per garantire la tracciabilità delle operazioni e supportare le indagini sugli incidenti, tutti i sistemi di produzione — server, postazioni di lavoro, dispositivi di rete e applicazioni — devono essere configurati per generare registri dettagliati (log). Il Visualizzatore eventi di Windows è attivo su tutti i PC e i server del dominio aziendale e costituisce la fonte primaria per la registrazione degli eventi di sistema. Devono essere registrate almeno le seguenti attività:

- Accessi e disconnessioni degli utenti
- Operazioni di creazione, lettura, aggiornamento e cancellazione su utenti e oggetti di sistema
- Modifiche alle impostazioni di sicurezza
- Accessi ai dati da parte degli amministratori di sistema

Ogni voce di log deve contenere almeno le seguenti informazioni:

Campo	Descrizione
ID utente	Identificativo univoco dell'utente che ha eseguito l'azione
Indirizzo IP	Indirizzo di rete di origine della sessione
Timestamp	Data e ora dell'evento, sincronizzato con fonte oraria approvata
Tipo di azione	Categoria dell'operazione eseguita (accesso, modifica, cancellazione)
Oggetto	Risorsa o entità su cui l'azione è stata compiuta

I log devono essere conservati per un minimo di 180 giorni e protetti da qualsiasi manomissione o accesso non autorizzato, al fine di garantirne l'inalterabilità. L'accesso ai log è riservato al personale ICT-RSGSI e deve essere gestito secondo il principio del minimo privilegio. L'organizzazione utilizza una piattaforma SIEM per centralizzare la raccolta, la correlazione e l'analisi degli eventi di sicurezza provenienti dai server e dai dispositivi di rete aziendali. Il SIEM classifica automaticamente gli alert per livello di gravità e consente funzionalità avanzate di threat hunting, rilevamento malware, valutazione della configurazione, monitoraggio dell'integrità dei file e mappatura MITRE ATT&CK. Devono essere configurati avvisi automatici per eventi critici — quali tentativi multipli di autenticazione falliti, modifiche non autorizzate alle configurazioni o anomalie nel traffico —

che attivino il processo di risposta descritto nella *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Sincronizzazione degli orologi

Tutti gli orologi dei sistemi di elaborazione devono essere sincronizzati con una fonte oraria autorevole e approvata basata sul protocollo NTP. La fonte oraria di riferimento deve essere configurata sui domain controller del dominio Active Directory, i quali propagano la sincronizzazione a tutti i dispositivi membri. La sincronizzazione è indispensabile per garantire la correlazione accurata degli eventi tra i diversi sistemi e per supportare le analisi forensi in caso di incidente.

Il ruolo ICT-RSGSI è responsabile della verifica periodica, con cadenza almeno trimestrale, del corretto funzionamento della sincronizzazione NTP su tutti i dispositivi del dominio, documentandone l'esito. In caso di errore di sincronizzazione, devono essere intraprese azioni correttive immediate — quali la sostituzione della fonte oraria, la riconfigurazione del servizio NTP o l'adozione di una fonte oraria alternativa — e l'anomalia deve essere registrata nel sistema di gestione dei rilievi e tracciata fino alla completa risoluzione.

Monitoraggio di reti, sistemi e applicazioni

Le reti, i sistemi e le applicazioni devono essere monitorati in tempo reale per rilevare comportamenti anomali e valutare potenziali incidenti di sicurezza. L'organizzazione utilizza strumenti dedicati di network monitoring per sorvegliare lo stato di tutti gli host e i servizi critici, con classificazione automatica degli eventi in livelli di gravità. L'adeguatezza dei meccanismi di monitoraggio deve essere riesaminata periodicamente dal ruolo ICT-RSGSI.

Sicurezza e segregazione delle reti

Le reti aziendali devono essere protette, gestite e controllate per salvaguardare le informazioni nei sistemi e nelle applicazioni. I gruppi di servizi informativi, gli utenti e i sistemi devono essere separati logicamente mediante segmentazione della rete, firewall e liste di controllo degli accessi (ACL). L'architettura di rete, inclusi i criteri di segregazione, deve essere documentata nel *MOD Diagramma di rete* e aggiornata in occasione di ogni modifica significativa. I meccanismi di sicurezza, i livelli di servizio e i requisiti dei servizi di rete devono essere identificati, documentati e monitorati, indipendentemente dal fatto che tali servizi siano erogati internamente o da fornitori esterni. Le specifiche tecniche e le regole di configurazione dei dispositivi di rete sono definite nella *PRO Procedura di gestione della sicurezza della rete* .

Uso accettabile delle informazioni e degli asset

Le informazioni proprietarie e dei clienti archiviate su qualsiasi dispositivo — sia di proprietà dell'organizzazione che del dipendente o di terzi — rimangono di proprietà esclusiva di DG Impianti Industriali S.p.A. L'assegnazione degli asset aziendali è tracciata attraverso il *MOD Modulo di assegnazione dei beni* e ciascun dipendente è responsabile della custodia e del corretto utilizzo delle risorse affidategli.

Ogni dipendente ha l'obbligo di segnalare tempestivamente il furto, lo smarrimento o la divulgazione non autorizzata di informazioni o apparecchiature aziendali. L'accesso e l'utilizzo delle informazioni sono permessi esclusivamente nella misura in cui siano autorizzati e necessari per adempiere alle proprie mansioni lavorative.

Sono severamente vietate, senza eccezioni, le seguenti attività:

- La violazione dei diritti di proprietà intellettuale, compresa l'installazione o la distribuzione di software privo di regolare licenza
- La copia non autorizzata di materiale protetto da diritto d'autore
- L'introduzione deliberata di programmi dannosi (virus, worm, trojan) nella rete o nei sistemi aziendali
- L'accesso a dati, server o account per scopi diversi dalla conduzione delle attività aziendali, anche qualora si disponga di un accesso autorizzato
- L'elusione dei sistemi di autenticazione o di sicurezza di qualsiasi host, rete o account
- L'esecuzione di scansioni di porte o di sicurezza senza preventiva notifica e autorizzazione scritta del ruolo ICT-RSGSI
- Qualsiasi forma di monitoraggio della rete che intercetti dati non destinati al proprio host, salvo che ciò rientri nelle mansioni lavorative espressamente assegnate

Per motivi di sicurezza, l'organizzazione si riserva il diritto di monitorare apparecchiature, sistemi e traffico di rete in qualsiasi momento per verificare il rispetto della presente politica.

Protezione da malware

L'organizzazione deve implementare e mantenere aggiornata una soluzione antimalware centralizzata su tutti i dispositivi endpoint — postazioni di lavoro, server e dispositivi mobili aziendali. La piattaforma di endpoint protection adottata copre l'intera flotta aziendale ed esegue scansioni in tempo reale con aggiornamento automatico delle firme e dei motori di rilevamento. Il ruolo ICT-RSGSI monitora lo stato di salute e di conformità dei dispositivi attraverso la console di gestione centralizzata, verificando che lo score complessivo di protezione si mantenga entro i livelli target definiti per agent mode, tamper protection, policy compliance e firewall. Ogni dipendente ha il divieto assoluto di disabilitare, aggirare o interferire con il funzionamento del software antimalware installato sui dispositivi aziendali. Qualsiasi evento di rilevamento malware deve essere immediatamente segnalato al ruolo ICT-RSGSI.

Installazione di software

L'installazione di software sui sistemi aziendali è riservata esclusivamente al personale ICT-RSGSI o a soggetti da esso espressamente delegati. Gli utenti standard non dispongono dei privilegi amministrativi necessari per installare, modificare o rimuovere applicazioni sui propri dispositivi; tale restrizione è imposta tramite i criteri di gruppo (Group Policy) del dominio Active Directory. Qualsiasi richiesta di installazione di nuovo software

deve essere sottoposta al ruolo ICT-RSGSI, che ne verifica la compatibilità, la legittimità della licenza e l'assenza di rischi per la sicurezza prima dell'autorizzazione.

Programmi di utilità privilegiati

L'uso di programmi di utilità in grado di ignorare i controlli del sistema operativo o delle applicazioni — quali editor del registro, strumenti di debug e utility di rete avanzate — deve essere limitato ai soli account amministrativi nominali e strettamente controllato. Gli account di Domain Admin del dominio Active Directory sono univocamente riconducibili a singoli operatori autorizzati e il loro utilizzo è registrato nei log di sistema. Le credenziali privilegiate sono gestite tramite un vault centralizzato con accesso ristretto.

Il ruolo ICT-RSGSI deve applicare le seguenti misure obbligatorie per l'hardening degli account privilegiati nell'ambiente Active Directory:

- Revisione almeno semestrale della composizione del gruppo Domain Admin, con rimozione immediata degli account non più necessari
- Utilizzo di account amministrativi separati e dedicati, distinti dagli account utente ordinari, per tutte le operazioni privilegiate
- Gestione delle password degli account privilegiati tramite il vault centralizzato, con rotazione periodica o compensata dal controllo crittografico del vault stesso
- Inserimento degli account amministrativi nel gruppo Protected Users ove compatibile con i servizi in uso, al fine di mitigare il rischio di furto di credenziali
- Applicazione di criteri di gruppo (GPO) specifici per l'hardening delle sessioni amministrative e la limitazione della delega delle credenziali

Filtraggio web

L'accesso a siti web esterni deve essere gestito per ridurre l'esposizione a contenuti dannosi e a risorse che possono distribuire malware. L'organizzazione implementa un sistema di filtraggio DNS a livello infrastrutturale, configurato sui domain controller aziendali, che instradata tutte le query DNS attraverso resolver dedicati alla protezione e blocca automaticamente l'accesso a categorie di siti ritenuti pericolosi o inappropriati. Il ruolo ICT-RSGSI gestisce le politiche di filtraggio, ne verifica l'efficacia e valuta eventuali richieste motivate di deroga.

Bring Your Own Device (BYOD)

L'uso di dispositivi personali (Bring Your Own Device - BYOD) per accedere alle risorse aziendali è consentito a condizione che vengano rispettati specifici requisiti di sicurezza per proteggere le informazioni dell'organizzazione.

Requisiti di Sicurezza per i Dispositivi Personali

- Autorizzazione: L'utilizzo di un dispositivo personale per accedere a dati e sistemi aziendali deve essere preventivamente autorizzato dal Responsabile ITC.

- Controlli Minimi: Il Responsabile ITC deve definire e comunicare i requisiti minimi di sicurezza che i dispositivi personali devono soddisfare. Questi includono:
  - L'installazione di un software antimalware approvato.
  - L'attivazione della crittografia del disco.
  - L'impostazione di un meccanismo di blocco dello schermo con password o biometria.
- Separazione dei Dati: Laddove tecnicamente possibile, i dati aziendali devono essere mantenuti in un contenitore separato e crittografato sul dispositivo personale per evitare commistioni con i dati personali.
- Software Autorizzato: Sui dispositivi personali utilizzati per lavoro è consentita solo l'installazione di applicazioni approvate dal Responsabile ITC per l'accesso alle risorse aziendali.

Responsabilità dell'Utente

- Manutenzione: L'utente è responsabile di mantenere il proprio dispositivo aggiornato e conforme ai requisiti di sicurezza definiti.
- Segnalazione Incidenti: In caso di smarrimento, furto o compromissione del dispositivo, l'utente deve informare immediatamente l'ICT-RSGSI e il Responsabile ITC per consentire la revoca degli accessi e la cancellazione remota dei dati aziendali, se possibile.

Utilizzo dei servizi cloud

L'acquisizione, l'uso e la gestione dei servizi cloud devono essere conformi ai requisiti di sicurezza delle informazioni di DG Impianti Industriali S.p.A.

Acquisizione e Gestione

- Valutazione della Sicurezza: Prima di acquisire un nuovo servizio cloud, l'ICT-RSGSI deve condurre una valutazione dei rischi per assicurarsi che il fornitore del servizio soddisfi i requisiti di sicurezza dell'organizzazione, inclusi quelli relativi alla protezione dei dati e alla continuità operativa.
- Accordi Contrattuali: Il Responsabile ITC, in collaborazione con l'Ufficio Legale, deve garantire che i contratti con i fornitori di servizi cloud definiscano chiaramente le responsabilità in materia di sicurezza, i livelli di servizio (SLA) e le clausole per la protezione dei dati.
- Configurazione Sicura: Il Responsabile ITC è responsabile di configurare i servizi cloud in modo sicuro, applicando i principi del minimo privilegio per la gestione degli accessi e attivando le funzionalità di sicurezza disponibili (es. MFA, logging, crittografia).

Uscita dai Servizi Cloud

- Strategia di Uscita: Per ogni servizio cloud critico, l'ICT-RSGSI deve definire una strategia di uscita che garantisca la migrazione sicura dei dati verso un altro servizio o il loro ripristino on-premise, assicurando la continuità operativa.
- Cancellazione dei Dati: Al termine del contratto, il Responsabile ITC deve assicurarsi che tutti i dati aziendali siano stati cancellati in modo sicuro dai sistemi del fornitore, ottenendo una certificazione di avvenuta cancellazione ove possibile.Utilizzo dei supporti di memorizzazione rimovibili

Per ridurre al minimo il rischio di perdita di dati e di introduzione di software dannoso, è severamente vietato archiviare informazioni riservate dell'organizzazione su supporti di memorizzazione rimovibili personali o non approvati, quali chiavette USB, dischi esterni o schede di memoria. L'uso di tali dispositivi per scopi lavorativi è consentito esclusivamente se il supporto è fornito e gestito dall'organizzazione oppure se è stato esplicitamente autorizzato dal ruolo ICT-RSGSI. Qualsiasi supporto rimovibile approvato deve soddisfare i seguenti requisiti:

- Essere protetto da crittografia per tutelare i dati in esso contenuti
- Essere sottoposto a scansione antimalware prima di ogni utilizzo su sistemi aziendali
- Essere etichettato in conformità con la *POL Politica di classificazione ed etichettatura delle informazioni*

La dismissione dei supporti rimovibili deve seguire procedure di cancellazione sicura conformi alle prassi di settore, in modo da rendere i dati irrecuperabili anche con strumenti di analisi forense. Le modalità di smaltimento sicuro degli asset informatici sono disciplinate dalla *PRO Procedura di configurazione, gestione e smaltimento degli asset* .

Scrivania e schermo puliti

Tutti i dipendenti sono tenuti a rispettare le regole di scrivania e schermo puliti per ridurre il rischio di accessi non autorizzati, perdita o danneggiamento delle informazioni durante e al di fuori del normale orario di lavoro. I materiali informativi riservati — documenti stampati, supporti rimovibili, appunti contenenti dati sensibili — non devono mai essere lasciati incustoditi sulle scrivanie o negli spazi di lavoro comuni. Al termine della giornata lavorativa o in caso di assenza prolungata, tali materiali devono essere riposti in cassetti o armadi chiusi a chiave. Tutti i dispositivi, quali laptop e PC, devono essere configurati con uno screen saver protetto da password o da controllo biometrico equivalente, che si attivi automaticamente dopo cinque minuti di inattività. Tale configurazione è imposta centralmente tramite il criterio di gruppo "DG_Lock Screen ON" del dominio Active Directory. È obbligatorio bloccare manualmente lo schermo del proprio dispositivo ogni volta che ci si allontana dalla postazione, anche per brevi periodi.

Gestione delle capacità

L'organizzazione monitora e regola costantemente l'utilizzo delle risorse di elaborazione, archiviazione e di rete per garantire che la disponibilità e le prestazioni dei sistemi soddisfino i requisiti aziendali. Il ruolo ICT-RSGSI definisce soglie di capacità per le risorse chiave — potenza di calcolo, spazio di archiviazione, larghezza di banda e licenze software — e implementa meccanismi di allerta al raggiungimento di valori soglia predefiniti.

La pianificazione della capacità non riguarda solo l'hardware, ma include anche una valutazione periodica delle competenze, della disponibilità e del carico delle risorse umane ICT, considerata parte integrante del processo annuale di valutazione dei rischi. In caso di necessità, è consentito scalare le risorse per aumentare la capacità di elaborazione o archiviazione nell'ambiente cloud al di fuori del processo standard di gestione delle modifiche, a condizione che tali operazioni non introducano modifiche all'architettura del sistema; in caso contrario, devono seguire il processo formale descritto nella *PRO Procedura di gestione del cambiamento* .

Gestione delle vulnerabilità

L'organizzazione adotta un approccio proattivo alla gestione delle vulnerabilità tecniche. Le informazioni sulle nuove vulnerabilità devono essere ottenute tempestivamente tramite diverse fonti, tra cui scansioni automatizzate, test di penetrazione, avvisi dei fornitori e bollettini di sicurezza delle principali organizzazioni di settore. Il modulo di vulnerability detection integrato nella piattaforma SIEM consente di identificare in modo continuativo le applicazioni vulnerabili presenti nell'ambiente aziendale. Devono essere eseguite scansioni di vulnerabilità sui sistemi esposti pubblicamente e sull'infrastruttura interna, nonché test di penetrazione almeno una volta all'anno o a seguito di modifiche significative all'architettura dei sistemi. I risultati devono essere documentati e sottoposti a valutazione da parte del ruolo ICT-RSGSI.

Ogni vulnerabilità identificata viene valutata dal ruolo ICT-RSGSI, che ne determina il livello di gravità in base al contesto aziendale. Le tempistiche massime per la risoluzione sono le seguenti:

Livello di gravità	Tempistica di risoluzione
Critico	Entro 7 giorni solari
Alto	Entro 30 giorni solari
Medio	Entro 60 giorni solari
Basso	Entro 90 giorni solari

Qualsiasi eccezione a queste tempistiche deve essere documentata, approvata dal ruolo ICT-RSGSI e registrata come rischio accettato nel registro dei rischi. Oltre alle vulnerabilità applicative, il processo di gestione deve includere i rilievi infrastrutturali emersi dai test di penetrazione e dalle scansioni di configurazione. In particolare, il ruolo ICT-RSGSI deve assicurare la tempestiva risoluzione delle debolezze protocollari e di hardening, tra cui a titolo esemplificativo:

- Disabilitazione di protocolli obsoleti o insicuri (quali SMBv1 e versioni TLS anteriori alla 1.2) su tutti gli host
- Abilitazione della firma obbligatoria sulle comunicazioni SMB (SMB signing) e del LDAP signing e channel binding sui domain controller

- Rimozione degli accessi anonimi ai servizi di rete (FTP anonymous, null session)
- Utilizzo esclusivo di certificati digitali rilasciati da autorità di certificazione riconosciute e affidabili

I risultati dei test di penetrazione e le relative azioni di remediation devono essere tracciati fino alla chiusura di ciascun rilievo e riesaminati nell'ambito del riesame della direzione. Per i rilievi ancora aperti, il ruolo ICT-RSGSI deve definire un piano di remediation con scadenze coerenti con le tempistiche di risoluzione previste dalla presente politica, sottoponendolo alla *PRO Procedura di gestione dei rilievi ed eventi* per il monitoraggio fino alla completa chiusura.

Gestione della configurazione

Le configurazioni di hardware, software, servizi e reti — comprese le configurazioni di sicurezza — devono essere stabilite, documentate, implementate e periodicamente riesaminate. Il ruolo ICT-RSGSI mantiene una baseline di configurazione sicura (hardening) per ciascuna tipologia di sistema e dispositivo, applicata attraverso i criteri di gruppo del dominio Active Directory e verificata tramite il modulo di configuration assessment della piattaforma SIEM. Qualsiasi modifica alle configurazioni di sicurezza deve essere soggetta al processo formale di gestione del cambiamento e tracciata tramite il *MOD Gestione del cambiamento* .

Gestione del cambiamento

Tutte le modifiche alle strutture di elaborazione delle informazioni e ai sistemi informativi devono essere soggette a un processo formale di gestione del cambiamento, come definito nella *PRO Procedura di gestione del cambiamento* . Prima dell'implementazione, ogni modifica deve essere valutata sotto il profilo dell'impatto sulla sicurezza, testata ove possibile, approvata formalmente e documentata. Il processo mira a prevenire l'introduzione di vulnerabilità o l'interruzione dei servizi a causa di modifiche non controllate.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGSI di DG Impianti Industriali S.p.A. e deve essere riesaminata con cadenza almeno annuale, o a seguito di cambiamenti significativi nell'organizzazione, nella tecnologia o nel contesto delle minacce, sotto la supervisione del ruolo ICT-RSGSI. Le versioni aggiornate devono essere approvate dalla direzione, comunicate a tutto il personale interessato e alle parti interessate pertinenti, e rese disponibili nel sistema di gestione documentale aziendale. Le versioni superate devono essere archiviate conformemente a quanto previsto dalla *PRO Procedura di gestione delle informazioni documentate* .

Documenti di riferimento

- *POL Politica di classificazione ed etichettatura delle informazioni*

- *PRO Procedura di gestione del cambiamento*
- *PRO Procedura di gestione degli acquisti e delle terze parti*
- *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni*
- *PRO Procedura di continuità operativa e di ripristino di emergenza*
- *PRO Procedura di gestione della sicurezza della rete*
- *PRO Procedura di configurazione, gestione e smaltimento degli asset*
- *PRO Procedura di gestione delle informazioni documentate*
- MOD Registro dei trattamenti del titolare
- MOD Conservazione delle informazioni e degli asset
- MOD Gestione del cambiamento
- MOD Modulo di assegnazione dei beni
- MOD Diagramma di rete