PH Facility S.r.l. riconosce la sicurezza delle informazioni, la sicurezza informatica e la resilienza operativa come requisiti essenziali per la continuità dei servizi, la tutela dei clienti e degli stakeholder, la conformità normativa e il conseguimento degli obiettivi aziendali

SCOPO E RIFERIMENTI

La Direzione adotta, diffonde e mantiene la presente Politica per garantire un livello di sicurezza adeguato ai rischi relativi alle informazioni e ai sistemi informativi e di rete utilizzati nelle attività aziendali e nella fornitura dei servizi. La politica integra il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e stabilisce gli impegni minimi in materia di governo, gestione del rischio, prevenzione, rilevamento, risposta, ripristino e miglioramento continuo.

La politica è definita tenendo conto, nelle versioni pro tempore vigenti, dei seguenti riferimenti:

- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio (Direttiva NIS2);
- decreto legislativo 4 settembre 2024, n. 138 (decreto NIS), in particolare gli articoli 7, 23, 24, 25, 26, 30 e 31;
- determinazioni, specifiche di base, linee guida e indicazioni dell'Agenzia per la cybersicurezza nazionale (ACN), inclusa la Determinazione ACN n. 379907/2025 e successive modifiche o integrazioni;
- norme ISO/IEC 27001:2022 e ISO/IEC 27002:2022;
- ulteriori disposizioni legali, regolamentari, contrattuali e di settore applicabili, incluse quelle in materia di protezione dei dati personali, segreto, proprietà intellettuale e continuità dei servizi.

CAMPO DI APPLICAZIONE E APPLICABILITÀ NIS

La presente politica si applica a tutte le articolazioni, sedi, processi, attività e servizi di PH Facility S.r.l., nonché a tutto il personale, agli amministratori, ai collaboratori, ai consulenti e ai soggetti terzi che accedono o gestiscono informazioni, sistemi o servizi per conto dell'organizzazione.

Il campo di applicazione comprende le informazioni in qualsiasi forma e supporto e tutti i sistemi informativi e di rete rilevanti, inclusi dispositivi, reti, applicazioni, servizi cloud, strumenti mobili, infrastrutture fisiche, sistemi OT/IoT, di telecontrollo o automazione, ove presenti, e le relative dipendenze interne ed esterne.

La Direzione assicura che sia verificata e documentata almeno annualmente l'applicabilità del decreto NIS, la classificazione dell'organizzazione come soggetto essenziale o importante, i settori e sottosettori pertinenti e le attività e i servizi NIS. Qualora l'organizzazione sia inserita nell'elenco nazionale NIS, gli obblighi e le specifiche ACN applicabili sono attuati nei termini comunicati dall'Autorità e registrati nel calendario di conformità.

PRINCIPI E OBIETTIVI DI SICUREZZAI

PH Facility S.r.l. adotta i seguenti principi:

- **Confidenzialità**: le informazioni sono accessibili esclusivamente a soggetti autorizzati e per finalità legittime;
- **Integrità e autenticità:** informazioni, dati, configurazioni e processi sono protetti da alterazioni non autorizzate e la loro origine è verificabile;
- **Disponibilità e resilienza:** servizi, informazioni e risorse sono disponibili quando richiesto e possono essere ripristinati entro tempi coerenti con la criticità;
- **Approccio multirischio:** i rischi informatici, fisici, organizzativi, umani e della catena di approvvigionamento sono valutati in modo integrato;
- **Proporzionalità e stato dell'arte:** le misure sono adeguate al rischio, alla dimensione, alla criticità dei servizi, alla probabilità e gravità degli incidenti, tenendo conto delle conoscenze aggiornate e dei costi di attuazione;
- **Sicurezza by design e by default:** la sicurezza è integrata nella progettazione, acquisizione, sviluppo, modifica, esercizio e dismissione di sistemi e servizi;
- **Minimo privilegio e separazione dei compiti:** gli accessi sono limitati alle necessità operative e le funzioni incompatibili sono separate;
- **Responsabilizzazione e tracciabilità:** decisioni, controlli, eccezioni, incidenti e attività rilevanti sono documentati con evidenze verificabili;

- **Miglioramento continuo:** carenze e non conformità sono corrette senza indebito ritardo e le misure sono riesaminate in base a risultati, cambiamenti e lezioni apprese.

GOVERNANCE, RUOLI E RESPONSABILITÀ

ORGANI DI AMMINISTRAZIONE E DIREZIONE

Gli organi di amministrazione e gli organi direttivi esercitano la responsabilità di indirizzo e sovrintendenza prevista dalla disciplina NIS. In particolare:

- approvano la presente politica e le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica;
- sovrintendono all'attuazione degli obblighi applicabili, inclusi gli adempimenti verso ACN e CSIRT Italia, e verificano lo stato dei piani di adeguamento;
- assegnano ruoli, responsabilità, autorità e risorse adeguate, assicurando l'indipendenza e l'accesso alle informazioni necessari alle funzioni di controllo;
- seguono una formazione in materia di sicurezza informatica e promuovono una formazione periodica e coerente per dipendenti e collaboratori;
- ricevono informazioni periodiche e, quando opportuno, tempestive sui rischi, sugli incidenti, sulle notifiche, sulle carenze e sulle azioni correttive;
- approvano i criteri di accettazione del rischio e accettano formalmente i rischi residui che eccedono le soglie delegate;
- assicurano l'integrazione del SGSI e degli obblighi NIS nella strategia, nei processi, negli investimenti e nella gestione dei fornitori.

L'attribuzione di compiti operativi o deleghe non elimina le responsabilità previste dalla legge in capo agli organi di amministrazione e direttivi.

RESPONSABILE SGSI / FUNZIONE DI SICUREZZA INFORMATICA

Il Responsabile SGSI o la funzione incaricata della sicurezza informatica coordina l'attuazione della politica, mantiene il sistema documentale e il quadro dei controlli, supporta la valutazione e il trattamento dei rischi, monitora vulnerabilità e minacce, coordina la risposta agli incidenti, cura metriche, audit, formazione e reporting e propone alla Direzione le azioni necessarie. Opera in raccordo con IT, process owner, Risorse Umane, Acquisti, Legale/Privacy e con le altre funzioni interessate.

PUNTO DI CONTATTO NIS E RUOLI PER LE NOTIFICHE

Quando applicabile, la Direzione designa e mantiene aggiornati il Punto di contatto NIS, il relativo sostituto, le persone fisiche responsabili ai sensi dell'articolo 38, comma 5, del decreto NIS e il referente incaricato delle interlocuzioni e notifiche al CSIRT Italia, con adeguate sostituzioni e reperibilità. I ruoli sono formalizzati, comunicati internamente e dotati delle necessarie autorizzazioni di accesso ai Servizi NIS.

Il Punto di contatto assicura la correttezza e l'aggiornamento dei dati comunicati tramite la piattaforma ACN e coordina gli adempimenti periodici. Le modifiche alle informazioni trasmesse sono comunicate tempestivamente e, ove previsto dall'articolo 7 del decreto NIS, entro quattordici giorni.

RESPONSABILI DI PROCESSO, SERVIZIO E ASSET

Ogni processo, attività, servizio, informazione e asset rilevante ha un responsabile identificato. I responsabili contribuiscono alla classificazione, alla valutazione dei rischi, alla definizione dei requisiti di continuità e sicurezza, alla validazione degli accessi, alla gestione delle modifiche e al monitoraggio delle dipendenze e dei fornitori.

PERSONALE, COLLABORATORI E TERZE PARTI

Tutti i destinatari rispettano la presente politica e le procedure collegate, proteggono credenziali e asset, partecipano alla formazione, segnalano immediatamente eventi, anomalie, vulnerabilità, sospetti o violazioni e cooperano nelle attività di risposta e verifica. I soggetti terzi sono vincolati da obblighi contrattuali coerenti con il rischio e con gli obblighi NIS applicabili.

GESTIONE DEL RISCHIO E ATTIVITÀ E SERVIZI NIS

La gestione del rischio è un processo continuo, documentato e basato su un approccio multirischio. Essa considera almeno attività e servizi, processi, informazioni, sistemi informativi e di rete, ambiente fisico, persone, dipendenze interne ed esterne, fornitori diretti e subfornitori rilevanti, minacce, vulnerabilità, probabilità, conseguenze operative, economiche, sociali, legali e reputazionali.

- mantenere l'elenco aggiornato e, quando richiesto, la caratterizzazione e categorizzazione delle attività e dei servizi NIS secondo il modello ACN;
- mappare gli asset, i flussi informativi, le dipendenze e i responsabili, classificando informazioni e sistemi in base a criticità e impatto;
- definire criteri di rischio, soglie di accettazione e metodologie coerenti con il SGSI e con le specifiche ACN;
- predisporre e mantenere un piano di trattamento con responsabili, priorità, risorse, scadenze e stato di avanzamento;
- approvare e monitorare i rischi residui, incluse le eventuali eccezioni ai requisiti di sicurezza;
- riesaminare le valutazioni almeno annualmente e a seguito di incidenti, modifiche significative, nuove minacce o vulnerabilità, cambiamenti nei servizi o nella catena di approvvigionamento e aggiornamenti normativi;
- adottare senza indebito ritardo misure correttive appropriate e proporzionate quando sia rilevata una non conformità o un livello di rischio non accettabile.

MISURE DI GESTIONE DEI RISCHI PER LA SICUREZZA INFORMATICA

Le misure tecniche, operative e organizzative sono definite, attuate, mantenute e documentate in modo proporzionato ai rischi e comprendono almeno i seguenti ambiti.

POLITICHE DI ANALISI DEI RISCHI E SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE

L'organizzazione mantiene un insieme coerente di politiche, standard e procedure, configurazioni di base sicure e controlli per la protezione di reti, sistemi, endpoint, applicazioni, dati e ambienti fisici. Sono previsti, in funzione del rischio, segmentazione, hardening, protezione da codice malevolo, gestione delle configurazioni, logging, monitoraggio, rilevamento degli eventi e conservazione delle evidenze.

GESTIONE DEGLI INCIDENTI E NOTIFICHE

È mantenuto un processo documentato per preparazione, rilevamento, registrazione, analisi, classificazione, contenimento, eradicazione, ripristino, comunicazione e miglioramento post-incidente. Il processo definisce ruoli, sostituzioni, canali protetti, reperibilità, criteri di escalation, conservazione delle evidenze, coordinamento con fornitori e gestione delle crisi.

- tutto il personale e i fornitori segnalano immediatamente gli eventi o i sospetti di sicurezza attraverso i canali autorizzati;
- gli incidenti sono valutati rispetto ai criteri di significatività previsti dal decreto NIS e dalle specifiche ACN applicabili al soggetto essenziale o importante;
- gli organi di amministrazione e direttivi sono informati periodicamente e, per gli eventi rilevanti, tempestivamente;
- per gli incidenti significativi soggetti a notifica, sono garantite al CSIRT Italia, senza indebito ritardo, la pre-notifica entro 24 ore dalla conoscenza, la notifica entro 72 ore, le relazioni intermedie richieste e la relazione finale entro un mese dalla notifica; se la gestione è ancora in corso, sono forniti gli aggiornamenti previsti e la relazione finale entro un mese dalla conclusione;
- sono gestite, ove applicabili, le comunicazioni ai destinatari dei servizi e gli ulteriori adempimenti verso autorità, interessati, clienti, assicuratori e forze dell'ordine, coordinando gli obblighi NIS con quelli in materia di protezione dei dati personali e con gli obblighi contrattuali;
- sono svolte esercitazioni periodiche e sono documentate le lezioni apprese e le azioni correttive.

CONTINUITÀ OPERATIVA, BACKUP, RIPRISTINO E GESTIONE DELLE CRISI

I servizi e i processi critici sono oggetto di analisi di impatto, strategie di continuità, piani di risposta e ripristino e procedure di gestione delle crisi. Sono definiti obiettivi di ripristino, priorità, responsabilità, comunicazioni, risorse alternative e dipendenze. I backup sono

protetti, separati dai sistemi operativi quando opportuno, verificati e sottoposti a prove di ripristino. Piani ed esercitazioni sono riesaminati con frequenza proporzionata alla criticità.

SICUREZZA DELLA CATENA DI APPROVVIGIONAMENTO

I fornitori e i servizi esternalizzati sono selezionati e governati secondo il rischio. La valutazione considera le vulnerabilità specifiche del fornitore, la qualità dei prodotti e delle pratiche di sicurezza, ove applicabile le pratiche di sviluppo sicuro adottate dal fornitore, le dipendenze, la concentrazione e il ricorso a subfornitori. I contratti includono, secondo necessità, requisiti di sicurezza, riservatezza, continuità, gestione delle vulnerabilità, tempi di segnalazione degli incidenti compatibili con gli obblighi NIS, cooperazione nelle indagini e notifiche, diritto di verifica, livelli di servizio, gestione delle modifiche, restituzione o cancellazione dei dati e condizioni di uscita. Le prestazioni e le evidenze dei fornitori critici sono monitorate e riesaminate.

ACQUISIZIONE, MANUTENZIONE E GESTIONE DELLE VULNERABILITÀ

I requisiti di sicurezza delle informazioni sono definiti prima dell'acquisizione, dell'introduzione o della modifica di sistemi, applicazioni, servizi, infrastrutture e componenti tecnologici e sono verificati durante il relativo ciclo di vita.

L'Organizzazione applica criteri di configurazione sicura, separazione degli ambienti ove pertinente, controllo delle modifiche, verifica delle forniture, gestione degli aggiornamenti, delle patch e delle dipendenze tecnologiche, nonché procedure per la dismissione sicura dei sistemi e dei componenti.

Le vulnerabilità tecniche individuate o segnalate sono registrate, valutate e classificate in funzione del livello di rischio, trattate secondo priorità definite e monitorate fino alla loro risoluzione o all'accettazione formale del rischio residuo.

VALUTAZIONE DELL'EFFICACIA DELLE MISURE

È definito e documentato un piano per valutare l'efficacia delle misure di gestione del rischio mediante indicatori, controlli di secondo livello, audit, riesami, test di ripristino, esercitazioni, vulnerability assessment o altre verifiche proporzionate al rischio. I risultati sono comunicati ai responsabili e alla Direzione, registrati e tradotti in azioni correttive monitorate.

IGIENE INFORMATICA E FORMAZIONE

Sono stabilite pratiche di igiene informatica che includono, in funzione del rischio, gestione sicura delle credenziali, aggiornamenti, protezione dei dispositivi, uso corretto di posta e web, gestione dei supporti, lavoro remoto, prevenzione del phishing e segnalazione degli eventi. La formazione è differenziata per ruolo, erogata all'ingresso e periodicamente, verificata nell'efficacia e aggiornata rispetto alle minacce. Gli organi di amministrazione e direttivi seguono una formazione specifica e documentata.

CRITTOGRAFIA E CIFRATURA

Sono mantenute politiche e procedure per l'uso appropriato della crittografia e, ove necessario, della cifratura dei dati in transito e a riposo. Algoritmi, protocolli, certificati, chiavi e segreti sono scelti secondo lo stato dell'arte, gestiti lungo il ciclo di vita, protetti da accessi non autorizzati e riesaminati periodicamente.

SICUREZZA DEL PERSONALE, CONTROLLO DEGLI ACCESSI, ASSET E SICUREZZA FISICA

L'organizzazione mantiene inventari aggiornati di informazioni, sistemi, dispositivi, software, servizi e relativi responsabili. Gli accessi sono autorizzati secondo necessità, minimo privilegio e separazione dei compiti, con procedure di ingresso, variazione e cessazione, riesami periodici e controlli rafforzati per account privilegiati. Sono previsti obblighi di riservatezza, verifiche pre-impiego ove lecite e proporzionate, misure disciplinari e protezioni fisiche e ambientali contro accessi, danni, manomissioni, guasti e indisponibilità.

AUTENTICAZIONE A PIÙ FATTORI E COMUNICAZIONI PROTETTE

Sono utilizzate soluzioni di autenticazione a più fattori con priorità per accessi remoti, privilegiati, cloud e a sistemi o servizi critici.

ADEMPIMENTI VERSO ACN E CSIRT ITALIA

PH Facility S.r.l. rientrando nell'ambito del decreto NIS, mantiene un calendario di conformità con responsabili, scadenze ed evidenze, assicurando almeno:

- registrazione e aggiornamento delle informazioni tramite i Servizi NIS, inclusi Punto di contatto, sostituto, recapiti, domini, indirizzamento IP e responsabili richiesti;
- comunicazione tempestiva delle variazioni e rispetto delle finestre annuali e delle modalità definite dal decreto e dalle determinazioni ACN;
- elencazione, caratterizzazione e categorizzazione periodica delle attività e dei servizi NIS e aggiornamento delle relative dipendenze;
- attuazione delle misure di sicurezza di base applicabili alla qualifica di soggetto essenziale entro i termini comunicati;
- notifica degli incidenti significativi di base e conservazione delle ricevute, delle comunicazioni e della documentazione a supporto;
- cooperazione con ACN, CSIRT Italia e Autorità di settore nelle attività di vigilanza, verifica, richiesta di informazioni e gestione degli incidenti.

COMUNICAZIONI E CONDIVISIONE DELLE INFORMAZIONI

La comunicazione e diffusione di informazioni verso l'esterno è consentita esclusivamente per finalità legittime, da personale autorizzato e nel rispetto della classificazione delle informazioni, degli obblighi di riservatezza e delle norme applicabili. In caso di incidente o minaccia significativa, le comunicazioni verso clienti, utenti, partner, autorità o pubblico sono coordinate tra Direzione, sicurezza informatica, Legale/Privacy e Comunicazione, garantendo tempestività, accuratezza, coerenza e protezione delle indagini.

DOCUMENTAZIONE, EVIDENZE E DOCUMENTI ATTUATIVI

Politiche, procedure, piani, registri, decisioni, eccezioni e risultati delle verifiche sono soggetti a controllo documentale, approvazione, versionamento, accesso autorizzato, conservazione e riesame. Le evidenze devono consentire di dimostrare l'effettiva attuazione delle misure e il rispetto delle scadenze.

La presente politica è attuata almeno mediante i seguenti documenti o processi documentati:

- metodologia di analisi del rischio e piano di trattamento;
- inventario e classificazione di informazioni, asset, attività e servizi, dipendenze e responsabili;
- gestione delle identità, degli accessi e degli account privilegiati;
- gestione delle configurazioni, modifiche, patch, vulnerabilità e sviluppo/acquisizione sicuri;
- logging, monitoraggio, rilevamento e gestione degli eventi;
- piano di gestione e risposta agli incidenti e procedura di notifica NIS/CSIRT Italia;
- piani di continuità operativa, disaster recovery, backup, ripristino e gestione delle crisi;
- processo di sicurezza dei fornitori e clausole contrattuali minime;
- programma di formazione, consapevolezza e igiene informatica;
- politica crittografica e gestione delle chiavi e dei segreti;
- piano di verifica dell'efficacia, audit, test, metriche e reporting alla Direzione;
- registro degli adempimenti ACN, delle comunicazioni e delle scadenze.

NON CONFORMITÀ, ECCEZIONI E VIOLAZIONI

Le non conformità e le carenze sono registrate, valutate e corrette senza indebito ritardo con azioni proporzionate al rischio. Ogni eccezione a un requisito deve essere motivata, sottoposta ad analisi del rischio, approvata dall'autorità competente, limitata nel tempo, accompagnata da misure compensative e riesaminata prima della scadenza.

La violazione intenzionale o negligente della presente politica e delle procedure collegate può comportare misure disciplinari, contrattuali o legali, nel rispetto della normativa e degli accordi applicabili. Le violazioni da parte di terzi possono determinare sospensione degli accessi, azioni correttive, applicazione di penali o risoluzione del rapporto.

RIESAME E MIGLIORAMENTO CONTINUO

La politica è riesaminata almeno annualmente e ogniqualvolta intervengano cambiamenti significativi nell'organizzazione, nei servizi, nei sistemi, nelle minacce, nei fornitori, nel quadro normativo o nelle specifiche ACN, nonché a seguito di incidenti rilevanti, audit o verifiche. Il riesame considera l'efficacia delle misure, lo stato dei rischi, degli obiettivi e delle azioni, le risorse, le competenze, le lezioni apprese e le esigenze degli stakeholder.

Gli esiti del riesame sono documentati e includono decisioni, responsabilità, priorità, risorse e tempi per il miglioramento. Ogni revisione della politica è approvata dall'organo di amministrazione o dalla Direzione competente e comunicata ai destinatari.

Genova, lì 31/07/2026

DGE