

GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA E RIPRISTINO



 SOSTELIA Società del Gruppo Hera	Politica P - Gestione degli Incidenti di Sicurezza Informatica e Ripristino	Rev. 00 del 09/06/2026
	Modello Organizzativo NIS 2	

Tabella di revisione:

Controllo del documento	
Autore	Lucrezia Lodi
Data di creazione	09/06/2026
Data di ultima revisione	09/06/2026

Versione	Data	Approvato da	Descrizione delle modifiche
00	09/06/2026	Direzione	Prima emissione

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di **Sostelia S.p.A. A Socio Unico**

SOMMARIO:

PREMESSA	4
SCOPO E AMBITO DI APPLICAZIONE	4
RIFERIMENTI NORMATIVI	4
DEFINIZIONI	5
RUOLI E RESPONSABILITÀ	6
CLASSIFICAZIONE DEGLI INCIDENTI SIGNIFICATIVI	7
PROCESSO DI GESTIONE DEGLI INCIDENTI	8
Preparazione	8
Rilevamento	8
Risposta	9
Ripristino	9
Miglioramento	9
PIANO DI GESTIONE DEGLI INCIDENTI E NOTIFICA AL CSIRT ITALIA	9
COMUNICAZIONE AI DESTINATARI DEI SERVIZI E AL PUBBLICO	11
COORDINAMENTO CON LA GESTIONE DEI DATA BREACH (GDPR)	11
PLAYBOOK – SCENARI DI INCIDENTE	11
Scenario 1 – Attacco Ransomware	11
Scenario 2 – Compromissione di Account e Credenziali	12
Scenario 3 – Indisponibilità Prolungata di un Servizio Critico	12
Scenario 4 – Incidente su Sistemi di un Fornitore Esterno	12
REGISTRO DEGLI INCIDENTI	12
COMUNICAZIONI	13
ENTRATA IN VIGORE	13

PREMESSA

La gestione degli incidenti di sicurezza informatica rappresenta una capacità essenziale per garantire la continuità operativa dei servizi, la protezione delle informazioni e la resilienza dell'organizzazione. Un incidente, se non rilevato e gestito tempestivamente, può determinare impatti significativi sulle attività di Sostelia S.p.A. A Socio Unico (di seguito "la Società") in termini operativi, finanziari e reputazionali.

La gestione degli incidenti è ricompresa tra le misure di gestione del rischio che i soggetti NIS sono tenuti ad adottare ai sensi dell'articolo 24 del D.Lgs. 4 settembre 2024, n. 138 (di seguito "Decreto NIS" o "decreto"), che recepisce in Italia la Direttiva (UE) 2022/2555 (NIS 2). Inoltre, ai sensi dell'articolo 25 del medesimo decreto, la Società è tenuta a notificare al CSIRT Italia ogni incidente che ha un impatto significativo sulla fornitura dei propri servizi.

La presente Politica costituisce il piano per la gestione degli incidenti di sicurezza informatica richiesto dalla misura RS.MA-01 della Determinazione ACN n. 379907 del 19 dicembre 2025, e dà attuazione, per l'ambito "p) Gestione degli incidenti, ivi inclusi la risposta e ripristino", ai requisiti delle misure RS.MA-01, RS.CO-02 e RC.RP-01 indicati nella Tabella 1 in Appendice all'Allegato 1 della medesima Determinazione.

Sostelia è classificata quale soggetto importante ai sensi del Decreto NIS; conseguentemente si applicano i requisiti contrassegnati per i soggetti importanti (colonna S_I) e le tipologie di incidente significativo di cui all'Allegato 3 della Determinazione ACN (IS-1, IS-2, IS-3).

La presente Politica è approvata dagli organi di amministrazione e direttivi della Società ed è resa nota alle articolazioni competenti, tenuto conto della necessità di conoscere (need to know).

SCOPO E AMBITO DI APPLICAZIONE

La presente Politica si applica a Sostelia S.p.A. A Socio Unico.

In attuazione della misura RS.MA-01, la Politica definisce il piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, che comprende almeno:

- le fasi e le procedure di gestione e notifica degli incidenti con l'indicazione dei relativi ruoli e delle responsabilità;
- le procedure per la predisposizione e la trasmissione delle relazioni di cui all'articolo 25, comma 5, lettere c), d) ed e) del Decreto NIS;
- le informazioni di contatto per la segnalazione degli incidenti;
- le modalità di comunicazione interna, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna;
- la reportistica da utilizzare per la documentazione dell'incidente.

La Politica disciplina inoltre le procedure di comunicazione ai destinatari dei servizi e al pubblico (misura RS.CO-02) e le procedure di ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti dagli incidenti (misura RC.RP-01).

La Politica si applica a tutti i sistemi informativi e di rete rilevanti ai sensi della normativa NIS 2, ivi compresi i sistemi di tecnologia operativa (OT) a supporto dei servizi erogati dalla Società, e coinvolge tutto il personale dipendente, i collaboratori, i consulenti esterni e i fornitori che gestiscono o hanno accesso ai sistemi della Società. Ciascun fornitore, nell'eventuale regolamentazione della gestione degli incidenti con proprie procedure, deve rispettare i criteri definiti nel presente documento.

RIFERIMENTI NORMATIVI

- Direttiva (UE) 2022/2555 (NIS 2), artt. 21 e 23 – obblighi di gestione del rischio e di notifica degli incidenti.
- D.Lgs. 4 settembre 2024, n. 138 – artt. 23, 24, 25 e 26 – organi di amministrazione, misure di gestione del rischio, obblighi di notifica degli incidenti e notifica volontaria.
- Determinazione ACN n. 379907 del 19 dicembre 2025 – Misure di sicurezza di base. Misure applicabili alla presente Politica (Tabella 1, ambito p): RS.MA-01 (punti 1, 2 e 3), RS.CO-02 (punti 1 e 2), RC.RP-01 (punto 1).

- Determinazione ACN n. 379907 del 19 dicembre 2025 – Allegato 3: tipologie di incidente significativo per i soggetti importanti (IS-1, IS-2, IS-3).
- Linee Guida ACN – “Definizione del processo di gestione degli incidenti di sicurezza informatica”, dicembre 2025.
- FAQ ACN – “Domande frequenti NIS – Misure di sicurezza e notifica di incidenti”.
- Regolamento (UE) 2016/679 (GDPR), artt. 33 e 34 – notifica delle violazioni di dati personali, per il coordinamento con la Procedura di gestione dei Data Breach della Società.
- NIST SP 800-61r3 – Incident Response Recommendations and Considerations for Cybersecurity Risk Management.
- UNI CEI EN ISO/IEC 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni – Requisiti.
- ISO/IEC 27035 – Information security incident management (Parti 1, 2 e 3) – principi e linee guida per la gestione e la risposta agli incidenti.

DEFINIZIONI

Le definizioni principali utilizzate nella presente Politica sono conformi all’art. 2 del Decreto NIS e alla Determinazione ACN n. 379907/2025:

- **Incidente di sicurezza informatica:** evento che compromette la disponibilità, l’autenticità, l’integrità o la riservatezza di dati conservati, trasmessi o elaborati, ovvero dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi.
- **Incidente significativo:** incidente che ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per la Società, oppure che ha avuto o può avere ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli (art. 25, comma 4, Decreto NIS).
- **Quasi-incidente:** evento che avrebbe potuto configurare un incidente senza che quest’ultimo si sia tuttavia verificato.
- **Minaccia informatica significativa:** minaccia informatica che, in base alle sue caratteristiche tecniche, si può presumere possa avere gravi ripercussioni sui sistemi informativi e di rete della Società o sugli utenti dei suoi servizi.
- **Evidenza dell’incidente:** disponibilità di elementi oggettivi dai quali si evince che si è verificato un incidente di sicurezza informatica; l’acquisizione dell’evidenza determina il momento dal quale decorrono i termini per la pre-notifica (24 ore) e la notifica (72 ore).
- **CSIRT Italia:** Gruppo nazionale di risposta agli incidenti di sicurezza informatica operante all’interno dell’Agenzia per la Cybersicurezza Nazionale (ACN), ai sensi dell’art. 15 del Decreto NIS.
- **Punto di Contatto NIS2 (PdC):** figura designata dalla Società ai sensi dell’art. 7 del Decreto NIS, responsabile dei rapporti istituzionali con l’ACN.
- **Referente CSIRT:** figura tecnica designata tramite il Portale ACN, incaricata di interfacciarsi con il CSIRT Italia e di effettuare le notifiche degli incidenti significativi, le notifiche volontarie e le informazioni pertinenti di cui all’art. 26 del Decreto NIS.
- **Livelli di servizio attesi (SL):** obiettivi, indicati in termini misurabili, che definiscono le prestazioni attese dei servizi e delle attività della Società, definiti ai sensi della misura DE.CM-01; non necessariamente coincidono con i livelli di servizio contrattuali (SLA).
- **RTO (Recovery Time Objective):** intervallo di tempo entro cui sono disponibili le risorse di backup per il ripristino del livello essenziale di attività.
- **RPO (Recovery Point Objective):** tempo massimo che intercorre tra la produzione di un dato e la sua messa in sicurezza; misura la massima quantità di dati che può essere persa a causa di un incidente.

- **Sistemi OT (Operational Technology):** sistemi di tecnologia operativa – quali sistemi di controllo industriale, SCADA, PLC e apparati di telecontrollo – utilizzati per il monitoraggio e il controllo di processi fisici e impianti a supporto dei servizi della Società.
- **Incidente operativo:** incidente di sicurezza ICT originato da guasti, errori o anomalie non riconducibili ad eventi malevoli e/o minacce informatiche.
- **Incidente cyber:** incidente di sicurezza ICT associato ad attività malevole, vulnerabilità sfruttate o compromissioni di sicurezza.
- **SOC (Security Operation Center):** struttura, anche in outsourcing, preposta al monitoraggio continuo degli eventi di sicurezza, all'analisi preliminare delle segnalazioni e al supporto nelle attività di contenimento e risposta.
- **Severità:** parametro che esprime il livello di gravità di un incidente, determinato in base all'impatto sui servizi, al numero di utenti e sistemi coinvolti, alla durata del disservizio e al rischio per la continuità operativa; consente di definire priorità di intervento ed escalation.

RUOLI E RESPONSABILITÀ

Ai fini di una gestione efficace e coordinata degli incidenti, sono individuati i seguenti ruoli con le relative responsabilità. L'organizzazione per la sicurezza informatica e i relativi ruoli sono approvati dagli organi di amministrazione e direttivi e resi noti alle articolazioni competenti.

Ruolo	Nominativo	Responsabilità principali
Organi di amministrazione e direttivi	Giuliano Fontanesi	Approvano la presente Politica (RS.MA-01 punto 2). Ricevono informazione sugli incidenti significativi. Approvano il piano di adeguamento e le azioni correttive.
Punto di Contatto NIS2	Francesco Riccò	Supervisione degli adempimenti NIS 2. Decisione finale sulla notifica al CSIRT Italia. Coordinamento delle comunicazioni verso ACN e stakeholder istituzionali.
Referente CSIRT (e sostituto)	Francesco Riccò / Andrea Milioli Paolo Beiato	Trasmissione delle notifiche al CSIRT Italia tramite Portale ACN. Interlocazione tecnica con il CSIRT durante la gestione dell'incidente.
Responsabile IT	Francesco Riccò / Paolo Beiato (Ufficio IT – informatica@sostelia.com, int. 900)	Coordinamento tecnico della risposta. Triage, contenimento, investigazione, eradicazione e ripristino. Gestione degli strumenti di monitoraggio e del Registro Incidenti.
SOC (in outsourcing)	Punto com srl (security@puntocomgroup.com, tel. 030 77 044 89)	Monitoraggio continuo degli eventi di sicurezza; rilevazione e analisi preliminare delle segnalazioni; supporto al contenimento e al ripristino, secondo le procedure concordate con la Società.
Referente Privacy	Lucrezia Lodi	Coordinamento del doppio binario NIS 2 + GDPR per gli incidenti che coinvolgono dati personali. Notifica al Garante entro 72 ore ove dovuta.

Ruolo	Nominativo	Responsabilità principali
Personale, collaboratori e fornitori	Tutti	Segnalazione immediata al Responsabile IT di qualsiasi evento anomalo o sospetto. Cooperazione nelle attività di risposta e nella raccolta delle informazioni per le notifiche.

I nominativi indicati devono essere formalizzati dagli organi di amministrazione e direttivi prima dell'entrata in vigore della presente Politica. I ruoli e le responsabilità sono riesaminati e, se opportuno, aggiornati almeno ogni due anni, nonché a fronte di incidenti significativi o variazioni organizzative.

CLASSIFICAZIONE DEGLI INCIDENTI SIGNIFICATIVI

Ai fini dell'obbligo di notifica al CSIRT Italia, l'Allegato 3 della Determinazione ACN n. 379907/2025 definisce, per i soggetti importanti, le seguenti tipologie di incidente significativo:

Codice	Compromissione	Descrizione
IS-1	Riservatezza	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Integrità	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Disponibilità	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi (SL) dei suoi servizi e/o delle sue attività, stabiliti ai sensi della misura DE.CM-01.

Ciò che rileva ai fini dell'obbligo di notifica è che la Società abbia evidenza dell'incidente, ovvero disponga di elementi oggettivi dai quali si evince che si è verificata una delle fattispecie sopra elencate. La causa dell'incidente – dolosa, accidentale o naturale (ad esempio guasti, errori umani, eventi naturali) – non è rilevante ai fini della notifica.

L'evidenza dell'incidente si acquisisce tipicamente tramite l'analisi di segnalazioni di attori esterni (ad esempio il CSIRT Italia), di segnalazioni di attori interni (ad esempio un utente che riporta un malfunzionamento all'help desk) o degli eventi di sicurezza rilevati dai sistemi di monitoraggio.

Si precisa che la tipologia IS-4 (accesso non autorizzato o con abuso dei privilegi concessi) è prevista dall'Allegato 4 della Determinazione ACN per i soli soggetti essenziali e pertanto non si applica a Sostelia in quanto soggetto importante.

Livelli di severità. In aggiunta alla classificazione NIS 2 (IS-1, IS-2, IS-3), a ogni incidente è attribuito un livello di severità interno, che ne guida la prioritizzazione e l'escalation. La severità è determinata in base a parametri quali l'estensione dell'incidente, il numero e la tipologia dei sistemi impattati (con indicazione dell'eventuale appartenenza al perimetro NIS 2 e/o OT), il numero di soggetti coinvolti e la tipologia di informazioni interessate.

Livello	Indicazione	Criteri orientativi
Basso	Gestione ordinaria	Impatto contenuto, limitato a un singolo sistema non critico, senza coinvolgimento del perimetro NIS 2.

Livello	Indicazione	Criteri orientativi
Medio	Gestione prioritaria	Impatto significativo su più sistemi o servizi, possibile rilevanza NIS 2 da verificare.
Grave	Escalation immediata	Impatto esteso o su servizi/sistemi critici (NIS 2 e/o OT); attivazione della gestione fast track e valutazione tempestiva della notifica al CSIRT Italia.

PROCESSO DI GESTIONE DEGLI INCIDENTI

Il processo di gestione degli incidenti è strutturato nelle seguenti cinque fasi, ispirate al modello NIST SP 800-61r3 e alle Linee Guida ACN di dicembre 2025. La fase di miglioramento si estende trasversalmente lungo tutto il processo.

- Preparazione – attività propedeutiche di governo, identificazione e protezione.
- Rilevamento – individuazione tempestiva del verificarsi di un incidente.
- Risposta – segnalazione, investigazione, contenimento ed eradicazione.
- Ripristino – ripristino dei sistemi informativi e di rete oggetto di compromissione.
- Miglioramento – individuazione delle azioni di miglioramento sulla base delle lezioni apprese.

Preparazione

La fase di preparazione comprende le attività propedeutiche volte a garantire una gestione strutturata ed efficace degli incidenti. La Società mantiene aggiornati:

- l'inventario dei sistemi informativi e di rete rilevanti ai fini NIS 2, con indicazione di criticità e responsabili;
- i livelli di servizio attesi (SL) per i servizi e le attività rilevanti, quale base per il rilevamento tempestivo degli incidenti significativi (misura DE.CM-01);
- gli strumenti tecnici per il rilevamento degli incidenti, adeguatamente aggiornati, mantenuti e configurati;
- i playbook operativi per gli scenari di incidente più probabili (cfr. sezione dedicata);
- il piano di formazione del personale, comprensivo delle modalità di segnalazione degli incidenti.

Strumenti tecnici a supporto. La Società, anche tramite il SOC in outsourcing, si avvale di strumenti tecnici per il rilevamento e la gestione degli incidenti, tra cui:

- soluzioni di raccolta e correlazione dei log (log collection / SIEM);
- soluzioni di protezione e rilevamento sugli endpoint (EDR/XDR);
- sonde e sistemi di rilevamento/prevenzione delle intrusioni di rete (IDS/IPS);
- soluzioni di monitoraggio dei sistemi OT a supporto dei servizi, ove presenti;
- sistema documentale per l'archiviazione della documentazione relativa all'incidente.

Rilevamento

La fase di rilevamento si attiva con l'identificazione di un evento anomalo che potenzialmente configura un incidente. L'evento può essere rilevato automaticamente dagli strumenti di monitoraggio, ovvero tramite segnalazione interna (dipendenti, collaboratori, fornitori) o esterna (CSIRT Italia, partner, clienti).

Chiunque rilevi o sia a conoscenza di un evento anomalo o sospetto è tenuto a segnalarlo immediatamente al Responsabile IT. Quest'ultimo procede alla registrazione e all'analisi preliminare (triage) per determinare se l'evento si configura come incidente di sicurezza informatica e, in caso affermativo, per valutarne la potenziale rilevanza ai fini NIS 2.

In sede di triage il Responsabile IT, con il supporto del SOC, classifica preliminarmente l'evento come incidente operativo (guasti, errori o anomalie non malevoli) o incidente cyber (attività malevole, vulnerabilità sfruttate o compromissioni), instradandolo verso il percorso di gestione più appropriato. La classificazione è provvisoria e può essere rivista a seguito di analisi più approfondite.

Risposta

La fase di risposta inizia nel momento in cui è stato dichiarato l'incidente e si articola nelle seguenti sotto-fasi, che possono procedere in parallelo e in modo iterativo:

- **Segnalazione:** il Responsabile IT informa il Punto di Contatto NIS2 e, ove siano coinvolti dati personali, il Referente Privacy; viene avviata la compilazione del Dossier Incidente. In caso di incidente significativo si attivano le notifiche al CSIRT Italia (cfr. sezione dedicata).
- **Investigazione:** analisi tecnica volta a determinare la causa originale (root cause), l'estensione della compromissione, i sistemi e i dati coinvolti, gli indicatori di compromissione (IoC) e la cronologia degli eventi.
- **Contenimento:** adozione delle misure tecniche urgenti per limitare la propagazione dell'incidente, quali l'isolamento dei sistemi coinvolti, la revoca degli accessi compromessi, il blocco delle trasmissioni in corso e la preservazione dei log a fini di analisi forense.
- **Eradicazione:** rimozione di ogni capacità di controllo e persistenza dell'attaccante (bonifica delle credenziali, rimozione degli artefatti malevoli, risoluzione o mitigazione delle vulnerabilità sfruttate, installazione degli aggiornamenti di sicurezza).

Gestione fast track degli incidenti gravi. In caso di evidenza immediata di un'anomalia grave (ad esempio presenza e diffusione di malware), è attivato un percorso accelerato in cui le azioni di contenimento immediato (es. isolamento dei sistemi dalla rete) hanno priorità rispetto alla documentazione, che può essere completata al primo momento utile dopo la messa in sicurezza. La gestione dell'emergenza segue la catena di escalation definita, coinvolgendo il SOC, il Responsabile IT e il Punto di Contatto NIS2.

Ripristino

RC.RP-01 (punto 1). Nell'ambito del piano per la gestione degli incidenti, sono adottate e documentate procedure per il ripristino con riguardo almeno al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidenti di sicurezza informatica, ivi compresi quelli oggetto di obbligo di notifica ai sensi dell'articolo 25 del Decreto NIS.

La parte del piano relativa al ripristino viene eseguita una volta avviata dal processo di risposta. Le attività comprendono, a titolo esemplificativo: la creazione di immagini pulite (golden/clean image), la reinstallazione dei sistemi a partire da immagini pulite o da backup verificati, il ricollegamento in rete dei sistemi bonificati e il monitoraggio intensificato per verificarne l'efficacia. Il ripristino persegue gli obiettivi di RTO e RPO definiti per ciascun servizio rilevante nei piani di continuità operativa e di ripristino in caso di disastro.

Al fine di garantire tracciabilità e coerenza, sono documentate almeno le seguenti informazioni: sistemi impattati, obiettivi e attività di ripristino con le relative motivazioni, strutture tecniche e organizzative coinvolte, modalità di verifica dell'efficacia ed esiti attesi.

Miglioramento

Al termine della gestione dell'incidente viene condotta un'analisi delle lezioni apprese (lesson learned), con la partecipazione di tutti i soggetti coinvolti. Gli esiti alimentano l'aggiornamento delle procedure e dei playbook, delle logiche di rilevamento, del piano di formazione e dei piani di continuità operativa, ripristino e gestione delle crisi. Il Punto di Contatto NIS2 riferisce agli organi di amministrazione e direttivi sugli esiti degli incidenti significativi e sulle azioni correttive intraprese.

PIANO DI GESTIONE DEGLI INCIDENTI E NOTIFICA AL CSIRT ITALIA

RS.MA-01 (punto 1). La presente Politica costituisce il piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, in accordo all'articolo 25 del Decreto NIS. Il piano comprende le fasi e le procedure di gestione e notifica (sezioni precedenti), i ruoli e le responsabilità, le procedure per le relazioni di cui all'art. 25 comma 5, le informazioni di contatto, le modalità di comunicazione interna ed esterna e la reportistica per la documentazione dell'incidente.

RS.MA-01 (punto 2). Il piano è approvato dagli organi di amministrazione e direttivi della Società.

RS.MA-01 (punto 3). Il piano è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi – integrando le relative lezioni apprese – o mutamenti dell’esposizione alle minacce e ai relativi rischi.

In presenza di un incidente significativo (IS-1, IS-2 o IS-3), la Società trasmette al CSIRT Italia le seguenti comunicazioni tramite il Portale segnalazioni ACN (<https://segnalazioni.acn.gov.it/>), secondo le modalità e i termini di cui all’articolo 25 del Decreto NIS:

Tipo di segnalazione	Tempistica	Responsabile	Contenuto minimo
Pre-notifica	Entro 24 ore dall’evidenza dell’incidente	Francesco Riccò	Indicazione se l’incidente possa ritenersi il risultato di atti illegittimi o malevoli o avere un impatto transfrontaliero.
Notifica	Entro 72 ore dall’evidenza dell’incidente	Francesco Riccò Andrea Milioli Paolo Beiato	Aggiornamento della pre-notifica e valutazione iniziale dell’incidente, comprensiva di gravità, impatto e, ove disponibili, indicatori di compromissione.
Relazione intermedia	Su richiesta del CSIRT Italia	Francesco Riccò Andrea Milioli Paolo Beiato	Aggiornamenti pertinenti sullo stato dell’incidente.
Relazione finale	Entro 1 mese dalla notifica	Francesco Riccò Andrea Milioli Paolo Beiato	Descrizione dettagliata dell’incidente; tipo di minaccia o causa originale; misure di attenuazione adottate e in corso; impatto transfrontaliero ove noto.
Relazione mensile sui progressi	Mensile, se l’incidente è in corso al momento della relazione finale	Francesco Riccò Andrea Milioli Paolo Beiato	Progressi e aggiornamenti sino alla relazione finale entro un mese dalla conclusione della gestione.

La notifica non espone la Società a una maggiore responsabilità rispetto a quella derivante dall’incidente stesso (art. 25, comma 3, Decreto NIS). Senza ingiustificato ritardo e ove possibile entro 24 ore dalla pre-notifica, il CSIRT Italia fornisce un riscontro iniziale e, su richiesta, orientamenti sulle misure di mitigazione. Qualora si sospetti il carattere criminale dell’incidente, il CSIRT Italia fornisce orientamenti per la segnalazione alle Autorità di contrasto.

Nel caso in cui l’incidente si sia verificato su un sistema gestito da un fornitore esterno, è onere del referente che si avvale di tale fornitore raccogliere tutte le informazioni necessarie all’espletamento delle segnalazioni all’Autorità nei termini previsti. L’obbligo di notifica al CSIRT Italia resta in capo alla Società in quanto soggetto NIS cliente.

Catena di escalation operativa. Operativamente, l’evento sospetto rilevato dall’utente o dal SOC (Punto com srl) viene segnalato all’Ufficio IT, che ne verifica la natura; confermato l’incidente, il Referente CSIRT effettua la segnalazione al CSIRT Italia tramite il Portale segnalazioni ACN e, quale coordinamento di

Gruppo, la comunicazione al canale cyber del Gruppo Hera (cybersec-op@gruppohera.it). Le attività di contenimento e ripristino sono condotte con il supporto del SOC.

Oltre agli obblighi di notifica, la Società può trasmettere su base volontaria al CSIRT Italia notifiche relative a incidenti non significativi, quasi-incidenti e minacce informatiche, ai sensi dell'articolo 26 del Decreto NIS. La notifica volontaria non comporta obblighi aggiuntivi.

COMUNICAZIONE AI DESTINATARI DEI SERVIZI E AL PUBBLICO

RS.CO-02 (punto 1). In accordo al piano per la gestione degli incidenti di cui alla misura RS.MA-01, sono documentate e adottate procedure per comunicare senza ingiustificato ritardo, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, ovvero qualora intimato dall'Agenzia per la cybersicurezza nazionale ai sensi dell'articolo 37, comma 3, lettere g) e h), del Decreto NIS:

- ai destinatari dei propri servizi, gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi;
- ai destinatari dei propri servizi potenzialmente interessati da una minaccia informatica significativa, le misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia, nonché la natura della minaccia stessa.

RS.CO-02 (punto 2). Sono documentate e adottate procedure per informare il pubblico sugli incidenti occorsi, qualora intimato dall'Agenzia per la cybersicurezza nazionale ai sensi dell'articolo 37, comma 3, lettera i) del Decreto NIS.

Le comunicazioni verso i destinatari dei servizi e verso il pubblico sono coordinate dal Punto di Contatto NIS2 in raccordo con gli organi di amministrazione e direttivi, previo confronto con il CSIRT Italia ove richiesto.

COORDINAMENTO CON LA GESTIONE DEI DATA BREACH (GDPR)

Quando un incidente di sicurezza informatica comporta anche una violazione di dati personali, si attiva il doppio binario NIS 2 + GDPR:

- NIS 2 (art. 25 Decreto NIS): notifica al CSIRT Italia – pre-notifica entro 24 ore, notifica entro 72 ore;
- GDPR (art. 33 Reg. UE 2016/679): notifica al Garante per la protezione dei dati personali entro 72 ore, se la violazione presenta un rischio per i diritti e le libertà delle persone fisiche;
- GDPR (art. 34): comunicazione agli interessati senza ingiustificato ritardo, se la violazione è suscettibile di presentare un rischio elevato per i loro diritti e libertà.

In presenza di un incidente che coinvolge dati personali, il Responsabile IT attiva immediatamente il Referente Privacy. Le due procedure sono gestite in parallelo con il coordinamento del Punto di Contatto NIS2 e del Referente Privacy, evitando duplicazioni e garantendo la coerenza delle comunicazioni verso le rispettive Autorità. Per le modalità operative degli adempimenti GDPR si rinvia alla Procedura per la gestione delle violazioni di dati personali (Data Breach) adottata dalla Società.

PLAYBOOK – SCENARI DI INCIDENTE

La Società adotta playbook operativi per gli scenari di incidente ad alta probabilità o alto impatto. Per ciascuno sono indicate le azioni prioritarie nella fase di risposta.

Scenario 1 – Attacco Ransomware

Impatto atteso: IS-3 (indisponibilità dei servizi) e/o IS-1 (esfiltrazione di dati preventiva alla cifratura).

- Contenimento: isolamento dalla rete dei sistemi interessati; interruzione delle connessioni VPN e degli accessi remoti attivi; blocco del traffico verso i domini di comando e controllo rilevati.
- Preservazione delle evidenze: acquisizione dei log di sistema, EDR, firewall e Active Directory prima di qualsiasi attività di bonifica.

- Valutazione NIS 2: verifica della violazione degli SL (IS-3) e/o dell'avvenuta esfiltrazione di dati (IS-1); attivazione delle notifiche al CSIRT entro 24/72 ore.
- Ripristino: non procedere al pagamento del riscatto; ripristinare da backup verificati e integri; verificare l'assenza di backdoor residue prima della riconnessione.

Scenario 2 – Compromissione di Account e Credenziali

Impatto atteso: IS-1 (esfiltrazione di dati).

- Contenimento: revoca immediata delle credenziali compromesse; disabilitazione dell'account; invalidazione di tutte le sessioni attive.
- Investigazione: analisi dei log di accesso (Active Directory, posta, VPN, applicativi) per determinare le risorse a cui ha avuto accesso l'attaccante e l'arco temporale.
- Eradicazione: verifica dell'assenza di backdoor e account fantasma; reset forzato delle password degli utenti coinvolti; attivazione dell'autenticazione a più fattori ove non presente.

Scenario 3 – Indisponibilità Prolungata di un Servizio Critico

Impatto atteso: IS-3 (violazione dei livelli di servizio attesi).

- Verifica: accertare che la violazione degli SL sia riconducibile a un incidente di sicurezza e non a un guasto tecnico ordinario; in entrambi i casi documentare l'evento.
- Ripristino: attivazione dei piani di continuità operativa e di ripristino in caso di disastro, con gli RTO/RPO definiti per il servizio interessato.
- Notifica CSIRT: in caso di conferma della rilevanza (IS-3), avvio del processo di notifica entro 24 ore dall'evidenza.

Scenario 4 – Incidente su Sistemi di un Fornitore Esterno

Impatto atteso: IS-1, IS-2 o IS-3 a seconda della natura dell'incidente presso il fornitore.

- Raccolta informazioni: il Responsabile IT acquisisce dal fornitore i dettagli su modalità, estensione e impatto dell'incidente sui sistemi della Società.
- Valutazione autonoma: la Società effettua una valutazione indipendente dell'impatto sui propri servizi e dati, senza delegare al fornitore la decisione sulla rilevanza NIS 2.
- Notifica CSIRT: se l'incidente si configura come significativo per la Società, attivazione del processo di notifica entro 24 ore dall'evidenza, ferma restando la titolarità dell'obbligo in capo alla Società.

REGISTRO DEGLI INCIDENTI

Il Responsabile IT mantiene e aggiorna il Registro degli Incidenti di sicurezza informatica, quale repository di tutti gli incidenti gestiti dalla Società e strumento per garantire la tracciabilità delle decisioni, la conservazione delle evidenze e la dimostrazione di conformità agli obblighi NIS 2.

Catena documentale. La documentazione dell'incidente segue tre livelli: la scheda di classificazione (compilata nelle prime fasi per registrare tempistiche, sistemi coinvolti, severità ed eventuale rilevanza NIS 2), il Dossier Incidente (che traccia tutte le attività dalla rilevazione alla chiusura, comprese contenimento, eradicazione, ripristino ed esiti) e il Registro degli Incidenti, nel quale l'incidente chiuso viene censito in via definitiva.

Il Registro contiene, per ciascun evento, almeno le seguenti informazioni:

- codice identificativo, data e ora di rilevamento e di chiusura dell'incidente;
- descrizione sintetica dell'evento e tipologia (IS-1, IS-2, IS-3 o non significativo);
- sistemi e servizi coinvolti, con indicazione dell'eventuale appartenenza al perimetro NIS 2;
- impatto stimato (operativo, finanziario, reputazionale);
- azioni di contenimento, eradicazione e ripristino adottate;
- esito della valutazione di rilevanza NIS 2 e notifiche effettuate al CSIRT Italia;
- eventuale coinvolgimento di dati personali e relative notifiche GDPR;
- lezioni apprese e azioni correttive identificate.

 SOSTELIA Società del Gruppo Hera	Politica P - Gestione degli Incidenti di Sicurezza Informatica e Ripristino	Rev. 00 del 09/06/2026
	Modello Organizzativo NIS 2	

Il Registro è conservato in modo sicuro, con accesso limitato al personale autorizzato, ed è esibito su richiesta dell'ACN o di altre Autorità competenti. Con periodicità almeno annuale sono estratti gli indicatori di prestazione (ad esempio MTTD – tempo medio di rilevazione e MTTR – tempo medio di ripristino) per il riesame del processo da parte degli organi di amministrazione e direttivi.

COMUNICAZIONI

La presente Politica è resa disponibile a tutto il personale della Società mediante pubblicazione sulle bacheche aziendali, invio tramite e-mail istituzionale e, ove presente, caricamento sull'intranet aziendale o su piattaforme di comunicazione interna.

A ogni aggiornamento del documento, il personale è informato tempestivamente attraverso i medesimi canali. È obbligo di ciascun dipendente e collaboratore prendere visione della versione più aggiornata e conformarsi integralmente alle disposizioni contenute.

La mancata osservanza delle disposizioni può comportare l'applicazione di sanzioni disciplinari, oltre all'eventuale segnalazione alle Autorità competenti nei casi di violazioni gravi o reiterate.

ENTRATA IN VIGORE

La presente Politica entra in vigore a partire dal 12/06/2026 e sostituisce integralmente ogni precedente disposizione interna in materia di gestione degli incidenti di sicurezza informatica adottata dalla Società.

Il documento è soggetto a riesame e, se opportuno, ad aggiornamento periodico e comunque almeno ogni due anni ai sensi della misura RS.MA-01 (punto 3), nonché qualora si verificano incidenti significativi, mutamenti rilevanti nel contesto normativo o tecnologico o variazioni nell'esposizione alle minacce e ai relativi rischi.

L'eventuale aggiornamento è comunicato formalmente a tutti i destinatari e la versione aggiornata è resa disponibile secondo le modalità indicate nella sezione "Comunicazioni".

Firmato digitalmente da:
Giuliano Fontanesi
Data: 10/06/2026 18:29:39