MANUALE DI GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

Laboratori Italiani riuniti Campania S.p.A

REGISTRO DELLE MODIFICHE

Versione	Scritto da	Revisionato da	Approvato da	Data
1	Aegister S.p.A.	Cesareo Mangiacapre	Cesareo Mangiacapre	29/12/2025

Avvertenza: l'emanazione del presente manuale come copia non controllata non obbliga l'azienda a mantenere aggiornato il documento.

Classificazione: USO INTERNO

Indice

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente Manuale definisce le procedure operative per l'identificazione, la comunicazione, la valutazione e la notifica degli incidenti di sicurezza informatica in conformità alla Direttiva NIS2 e al D.lgs. 138/24 e nello specifico all'art.25 del d.lgs 138/24 che sancisce l'obbligo di notifica degli incidenti.

Questo documento si applica a:

- Tutti i dipendenti di Laboratori Italiani Riuniti Campania S.p.A
- Collaboratori esterni e consulenti
- Fornitori e partner che operano con accesso ai sistemi aziendali
- Tutti i soggetti che hanno accesso alle risorse IT e ai dati aziendali

L'obiettivo del presente manuale è quello di:

- Garantire la tempestiva **identificazione**, **comunicazione e segnalazione degli incidenti** di sicurezza
- Assicurare la conformità agli obblighi normativi di notifica
- Minimizzare l'impatto degli incidenti sull'operatività aziendale
- Proteggere la riservatezza, l'integrità e la disponibilità delle informazioni

2. DEFINIZIONI E RIFERIMENTI NORMATIVI

Evento di Sicurezza: Qualsiasi occorrenza identificata che può indicare una possibile violazione della sicurezza o un malfunzionamento delle misure di protezione.

Incidente di Sicurezza Informatica: Qualsiasi evento che comprometta la riservatezza, l'integrità o la disponibilità dei sistemi informatici, delle reti o dei dati.

Incidente Significativo: Incidente che causa o può causare una grave perturbazione operativa, perdite finanziarie o ripercussioni su persone fisiche o giuridiche.

Referente CSIRT: Soggetto designato da Laboratori Italiani Riuniti Campania S.p.A responsabile della gestione degli incidenti e delle comunicazioni con l'Agenzia per la Cybersicurezza Nazionale.

Pre-notifica: Comunicazione iniziale all'ACN da effettuarsi entro 24 ore dalla rilevazione dell'incidente.

Notifica: Comunicazione dettagliata all'ACN da effettuarsi entro 72 ore dalla rilevazione dell'incidente.

Riferimenti normativi:

- Direttiva (UE) 2022/2555 (Direttiva NIS2)
- D.lgs. 138/2024 (Recepimento Direttiva NIS2)
- Determina ACN n. 164179/2025

3. RUOLI E RESPONSABILITÀ

3.1 Tutto il Personale

Responsabilità:

- **Identificare e comunicare** immediatamente qualsiasi evento sospetto o anomalia
- Seguire le procedure operative indicate nel presente manuale
- Cooperare con il Referente CSIRT durante la gestione degli incidenti
- Preservare le evidenze e non alterare lo stato dei sistemi compromessi

3.2 Referente CSIRT

Nome: Cesareo Mangiacapre	
Contatti: 349 0911161	Contatti: incidenti@lirspa.com

Responsabilità:

- Ricevere e registrare tutte le comunicazioni di eventi di sicurezza informatica
- Valutare e classificare gli eventi di sicurezza
- Coordinare le attività di risposta agli incidenti
- Predisporre e inviare le notifiche all'ACN nei termini previsti
- Interfacciarsi con le autorità competenti
- Documentare tutte le fasi di gestione dell'incidente

3.3 CISO (Chief Information Security Officer)

Nome: Cesareo Mangiacapre	
Contatti: 349 0911161	Contatti: ict@lirspa.com

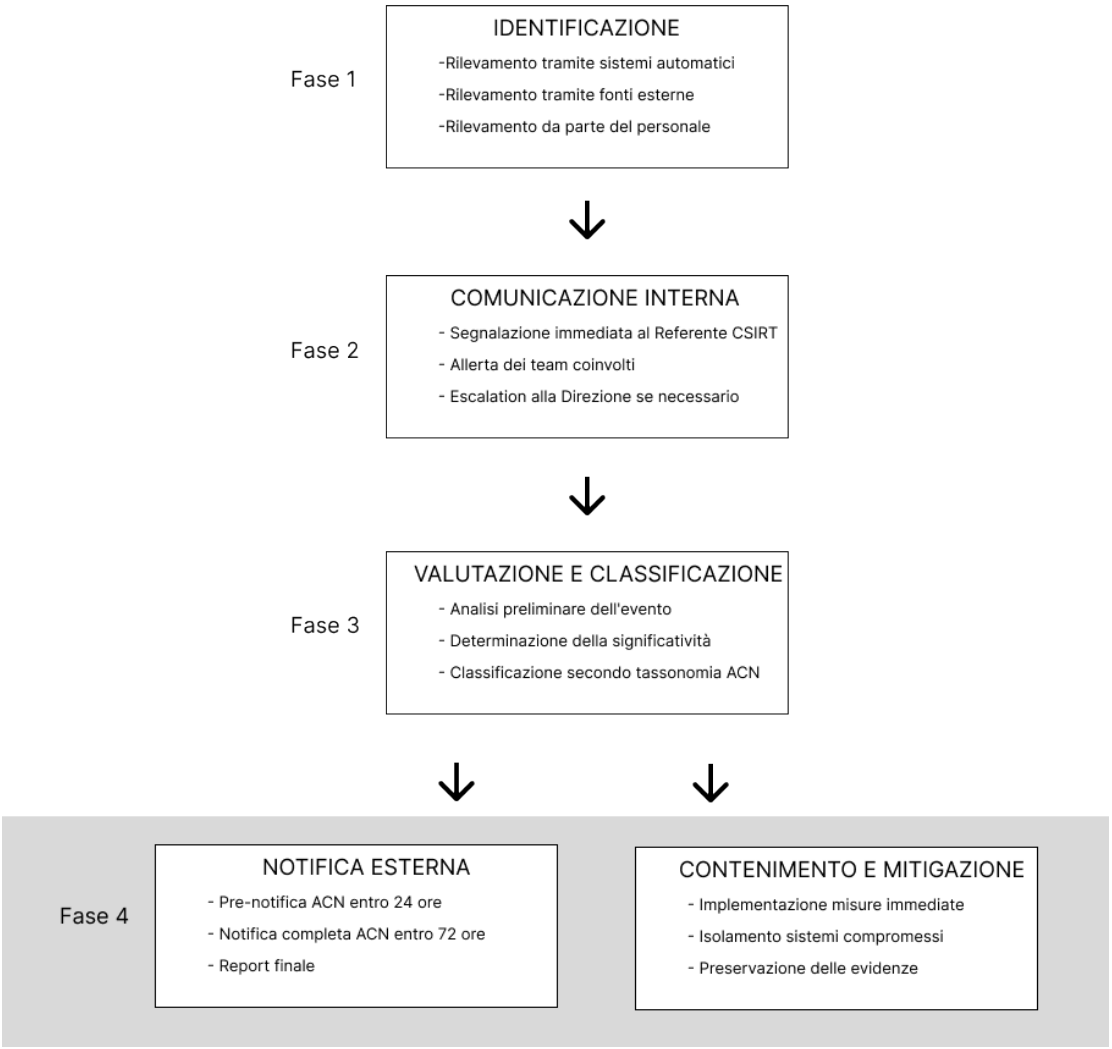
Responsabilità:

- Supervisionare l'intero processo di gestione degli incidenti
- Autorizzare le comunicazioni esterne
- Decidere sulle misure di contenimento e ripristino
- Interfacciarsi con la Direzione aziendale

4. PROCESSO DI GESTIONE DEGLI INCIDENTI

Il processo di gestione degli incidenti si articola nelle seguenti fasi:

Section 2



5. IDENTIFICAZIONE DEGLI EVENTI DI SICUREZZA

5.1 Fonti di Identificazione

Gli eventi di sicurezza possono essere identificati attraverso:

Strumenti Interni di Monitoraggio:

- SIEM (Security Information and Event Management): Alert generati dai sistemi di correlazione eventi
- Antivirus/EDR: Rilevamento di malware, comportamenti sospetti o tentativi di intrusione
- Firewall e IDS/IPS: Rilevamento di traffico anomalo o tentativi di accesso non autorizzato
- Log Analysis: Analisi dei log di sistema, applicativi e di rete

- DLP (Data Loss Prevention): Rilevamento di tentativi di esfiltrazione dati
- Vulnerability Scanner: Identificazione di vulnerabilità critiche sfruttate

Strumenti Esterni:

- Security Vendor Alerts: Notifiche da fornitori di soluzioni di sicurezza
- Dark Web Monitoring: Rilevamento di dati aziendali esposti nel dark web
- CERT/CSIRT Nazionali: Bollettini di sicurezza e segnalazioni
- ACN: Comunicazioni dell'Agenzia per la Cybersicurezza Nazionale
- Partner e Clienti: Segnalazioni da terze parti

Rilevazione del Personale:

- Osservazione diretta di comportamenti anomali
- Ricezione di e-mail di phishing o comunicazioni sospette
- Rilevamento di accessi non autorizzati
- Malfunzionamenti inspiegabili dei sistemi

5.2 Principio della comunicazione immediata

REGOLA FONDAMENTALE: In caso di dubbio, il personale deve comunicare sempre.

- Non è richiesta la certezza assoluta che si tratti di un incidente
- Non tentare di risolvere autonomamente l'evento
- Non ritardare la comunicazione per effettuare verifiche personali
- La tempestività è essenziale per una gestione efficace

6. TIPOLOGIE DI INCIDENTI DI SICUREZZA

6.1 Incidenti relativi alla riservatezza (confidentiality)

6.1.1 Data Breach - Perdita di Riservatezza dei Dati

Descrizione: Accesso, divulgazione o esposizione non autorizzata di dati riservati. Esempi specifici:

• Esfiltrazione di dati tramite malware: Sottrazione di database clienti, dati finanziari o proprietà intellettuale
• Accesso non autorizzato a documenti riservati: Dipendente o terzo accede a informazioni al di fuori delle proprie autorizzazioni
• Esposizione pubblica di dati sensibili: Configurazione errata di database o storage cloud che rende accessibili dati riservati
• Data leak via e-mail: Invio accidentale di documenti riservati a destinatari non autorizzati
• Furto di credenziali: Sottrazione di username/password che permettono accesso a sistemi aziendali

• Divulgazione dati nel dark web: Pubblicazione di credenziali, dati personali o informazioni aziendali in forum o marketplace del dark web
• Screen scraping: Acquisizione non autorizzata di informazioni visualizzate su schermi aziendali

6.1.2 Phishing e Social Engineering

Descrizione: Tentativi di ottenere informazioni riservate attraverso l'inganno.

Esempi specifici:

• Spear phishing: E-mail mirate a specifici dipendenti per ottenere credenziali o informazioni sensibili
• Business E-mail Compromise (BEC): Compromissione di account e-mail aziendali per frodi o furto informazioni
• Vishing (Voice Phishing): Telefonate fraudolente per ottenere credenziali o informazioni
• Smishing (SMS Phishing): SMS fraudolenti con link malevoli o richieste di informazioni
• Whaling: Attacchi mirati a dirigenti e figure di alto livello
• Pretexting: Creazione di scenari fittizi per ottenere informazioni riservate
• Baiting: Distribuzione di dispositivi USB o altri media infetti per compromettere sistemi

6.2 Incidenti relativi all'integrità (integrity)

6.2.1 Manipolazione di Dati

Descrizione: Modifica non autorizzata di dati che compromette l'accuratezza e l'affidabilità delle informazioni.

Esempi specifici:

• Alterazione di database: Modifica fraudolenta di record in database aziendali (es. transazioni finanziarie, ordini)
• Manomissione di documenti: Modifica non autorizzata di contratti, report o documenti ufficiali
• Corruzione di dati di backup: Compromissione dell'integrità dei backup che impedisce il ripristino affidabile
• Modifica di configurazioni di sistema: Alterazione di parametri critici di sistemi operativi o applicazioni
• Sabotaggio di codice sorgente: Inserimento di backdoor o codice malevolo in repository di sviluppo
• Falsificazione di log: Cancellazione o modifica di log per nascondere attività malevole

6.2.2 Defacement

Descrizione: Modifica non autorizzata di contenuti visibili, in particolare siti web e interfacce pubbliche.

Esempi specifici:

• Defacement di siti web: Sostituzione della home page o di sezioni del sito aziendale
• Modifica di contenuti social media: Compromissione di account aziendali su piattaforme social
• Alterazione di comunicazioni pubbliche: Manomissione di newsletter, comunicati stampa o messaggi ufficiali

6.3 Incidenti relativi alla disponibilità (availability)

6.3.1 Denial of Service (DoS) e Distributed Denial of Service (DDoS)

Descrizione: Attacchi volti a rendere indisponibili servizi, sistemi o risorse di rete.

Esempi specifici:

• DDoS volumetrico: Saturazione della banda con traffico malevolo
• DDoS applicativo: Esaurimento delle risorse applicative (es. HTTP flood, Slowloris)
• DDoS a livello protocollo: Sfruttamento di vulnerabilità nei protocolli di rete (SYN flood, Ping of Death)
• Resource exhaustion: Esaurimento di risorse di sistema (CPU, memoria, storage)

6.3.2 Ransomware

Descrizione: Malware che cripta i dati e richiede un riscatto per il ripristino.

Esempi specifici:

• Ransomware con crittografia: Cifratura di file e sistemi con richiesta di pagamento
• Ransomware con esfiltrazione: Doppia estorsione con minaccia di pubblicazione dati sottratti
• Wiper ransomware: Malware che cancella i dati anziché cifrarli
• Ransomware-as-a-Service (RaaS): Attacchi ransomware condotti tramite piattaforme criminali

6.3.3 Malfunzionamenti e Interruzioni di Servizio

Descrizione: Indisponibilità di servizi critici dovuta a cause tecniche o attacchi. Esempi specifici:

• Interruzione servizi e-mail: Impossibilità di inviare/ricevere e-mail aziendali
• Crash di ERP/CRM: Indisponibilità di sistemi gestionali critici
• Downtime di server critici: Arresto di server che ospitano applicazioni essenziali

• Interruzione connettività di rete: Perdita di connessione Internet o della rete interna
• Failure di sistemi di produzione: Arresto di sistemi SCADA, ICS o altri sistemi operativi
• Indisponibilità di servizi cloud: Problemi di accesso a servizi cloud critici

6.4 Incidenti da malware

6.4.1 Tipologie di Malware

Esempi specifici:

- Trojan: Software malevolo mascherato da applicazione legittima
- Worm: Malware che si auto-replica attraverso la rete
- Spyware: Software che raccoglie informazioni senza consenso
- Keylogger: Registrazione delle battiture della tastiera per rubare credenziali
- Rootkit: Malware che nasconde la propria presenza e mantiene accesso privilegiato
- Botnet: Rete di dispositivi compromessi controllati da un attaccante
- Cryptominer: Software che utilizza risorse di sistema per mining di criptovalute non autorizzato
- Fileless malware: Malware che opera in memoria senza scrivere file su disco

6.5 Incidenti di accesso non autorizzato

6.5.1 Intrusioni e Compromissioni

Esempi specifici:

- Compromissione di account utente: Accesso non autorizzato tramite credenziali rubate o indovinate
- Privilege escalation: Ottenimento di privilegi superiori sfruttando vulnerabilità
- Accesso tramite backdoor: Utilizzo di punti di accesso nascosti lasciati da attaccanti
- Bypass di autenticazione: Sfruttamento di vulnerabilità per eludere meccanismi di login
- Lateral movement: Movimento dell'attaccante all'interno della rete dopo la compromissione iniziale
- Persistenza: Installazione di meccanismi per mantenere l'accesso nel tempo
- Command and Control (C2): Comunicazione tra sistemi compromessi e server dell'attaccante

6.5.2 Insider Threat

Esempi specifici:

- Abuso di privilegi: Dipendente che utilizza i propri accessi per scopi non autorizzati
- Sabotaggio interno: Danneggiamento intenzionale di sistemi o dati da parte di personale interno
- Furto di informazioni da dipendente: Sottrazione di proprietà intellettuale o dati sensibili
- Negligenza: Violazione di policy di sicurezza che causa incidenti

6.6 Incidenti fisici e ambientali

Esempi specifici:

- Furto di dispositivi: Smarrimento o furto di laptop, smartphone, tablet, hard disk esterni
- Accesso fisico non autorizzato: Intrusione in locali riservati (server room, data center, uffici)
- Manomissione di dispositivi: Installazione di hardware malevolo (USB, keylogger hardware)
- Distruzione fisica: Danni a infrastrutture IT causati da incendi, allagamenti, sabotaggi
- Intercettazione fisica: Installazione di dispositivi di intercettazione su cavi di rete o linee telefoniche

6.7 Incidenti da vulnerabilità

Esempi specifici:

- Exploit di vulnerabilità zero-day: Sfruttamento di vulnerabilità non ancora note o patchate
- Exploit di vulnerabilità note: Attacchi a sistemi non aggiornati con patch disponibili
- SQL Injection: Inserimento di codice SQL malevolo in input applicativi
- Cross-Site Scripting (XSS): Iniezione di script malevoli in pagine web
- Remote Code Execution (RCE): Esecuzione remota di codice su sistemi vulnerabili
- Buffer overflow: Sfruttamento di errori di gestione della memoria
- Misconfiguration: Sfruttamento di configurazioni errate di sistemi o applicazioni

6.8 Incidenti relativi alla supply chain

Esempi specifici:

- Compromissione di fornitori: Attacco tramite fornitori o partner con accesso ai sistemi aziendali
- Software supply chain attack: Inserimento di codice malevolo in software di terze parti
- Compromissione di aggiornamenti: Distribuzione di aggiornamenti software infetti
- Attacco tramite servizi cloud: Compromissione di servizi cloud utilizzati dall'azienda

6.9 Incidenti relativi alle comunicazioni

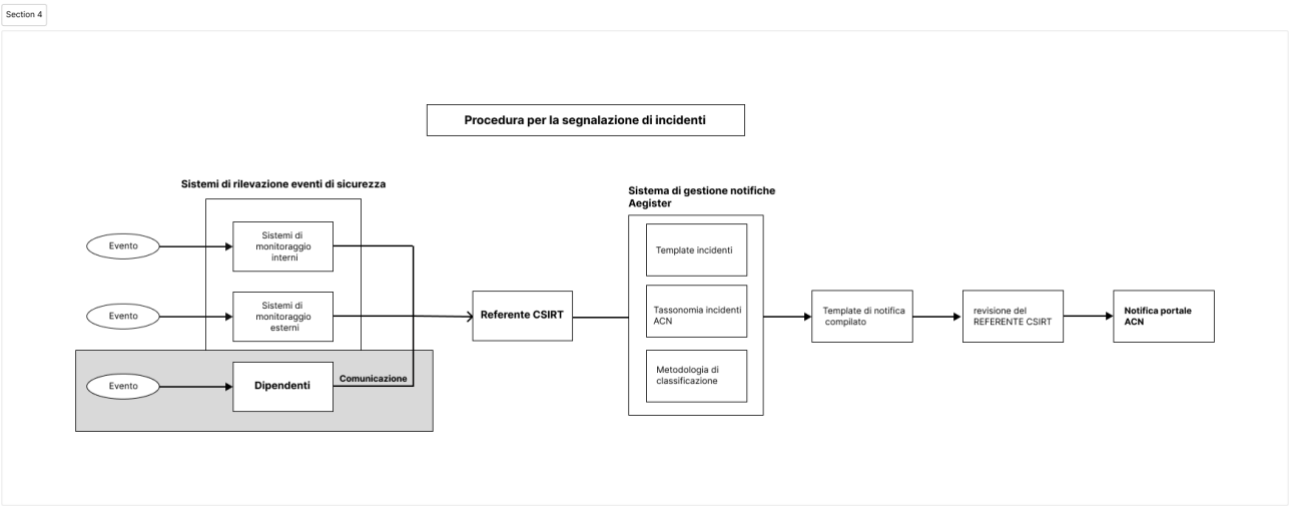
Esempi specifici:

- Man-in-the-Middle (MitM): Intercettazione di comunicazioni tra due parti
- DNS Spoofing/Hijacking: Manipolazione di risoluzioni DNS per reindirizzare traffico
- Session hijacking: Sottrazione di sessioni autenticate
- E-mail spoofing: Invio di e-mail falsificate che sembrano provenire da fonti legittime
- Intercettazione di comunicazioni: Ascolto non autorizzato di comunicazioni aziendali

7. COMUNICAZIONE DELL'EVENTO AL REFERENTE CSIRT

Il processo di comunicazione da parte del personale segue questi passaggi:

1. **Verifica dell'Evento:** Tutto ha inizio con il verificarsi di un **"Evento"**.
2. **Rilevazione Umana:** A differenza dei flussi superiori (gestiti da sistemi di monitoraggio automatici), in questo caso l'evento viene intercettato o notato direttamente dai **dipendenti**.
3. **Comunicazione:** Una volta identificato l'evento, il dipendente attiva una procedura di **"Comunicazione"**.
4. **Comunicazione al Responsabile:** La comunicazione viene indirizzata e inoltrata direttamente al **"Referente CSIRT"**, che funge da punto centrale di raccolta per tutte le notifiche di incidente, sia automatiche che umane.



7.1 Canali di Comunicazione

La comunicazione deve essere effettuata immediatamente utilizzando i seguenti canali, attivi 24/7:

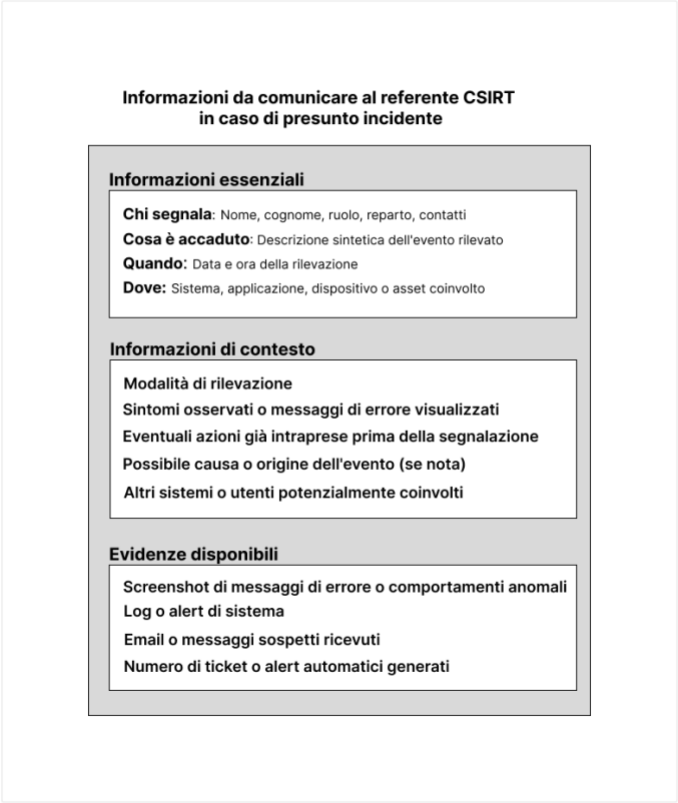
Canale	Informazioni
E-mail di emergenza	[email.incidenti@azienda.it]
Telefono diretto	[+39 XXX XXXXXXX]
Telefono alternativo	[+39 XXX XXXXXXX]
Piattaforma interna	[URL piattaforma di ticketing/segnalazione se disponibile]

IMPORTANTE: Utilizzare preferibilmente **entrambi i canali** (e-mail E telefono) per garantire la ricezione immediata della segnalazione.

7.2 Informazioni da Fornire

Nel comunicare l'evento, fornire il maggior numero possibile delle seguenti informazion

Section 5



ATTENZIONE: La mancanza di una o più informazioni **NON** deve in alcun modo ritardare la comunicazione. È preferibile segnalare immediatamente con informazioni parziali piuttosto che ritardare per raccogliere dettagli completi.

7.3 Modello di Segnalazione E-mail

In caso di incidente, inviare immediatamente una e-mail utilizzando il seguente template. Copiare e incollare il testo sottostante per garantire che tutte le informazioni critiche vengano trasmesse.

A: incidenti@lirspa.com **Oggetto:** [URGENTE] Comunicazione Incidente di Sicurezza – [Breve descrizione]

DATI DEL SEGNALANTE:

- **Nome e Cognome:** [Inserire Nome Cognome]
- **Ruolo/Reparto:** [Inserire Ruolo – Reparto]
- **Contatti:** [Telefono] | [E-mail]

DESCRIZIONE EVENTO: [Descrizione sintetica di cosa è stato rilevato, errori visibili, comportamenti anomali]

DATA E ORA RILEVAZIONE: [GG/MM/AAAA – HH:MM]

SISTEMA/ASSET COINVOLTO: [Nome sistema, hostname, dispositivo o applicazione]

AZIONI GIÀ INTRAPRESE: [Elencare eventuali azioni di contenimento già effettuate, oppure scrivere "Nessuna"]

EVIDENZE DISPONIBILI: [Indicare se sono stati allegati screenshot o log]

NOTE AGGIUNTIVE: [Qualsiasi altra informazione rilevante]

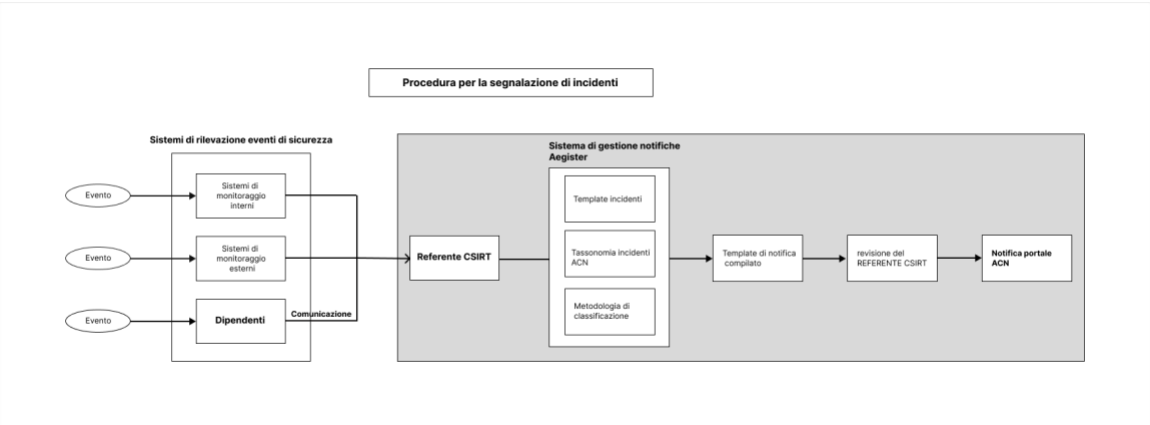
7.4 Conferma di Ricezione

Il Referente CSIRT confermerà la ricezione della comunicazione e fornirà:

- Prime indicazioni operative
- Richiesta di eventuali informazioni aggiuntive necessarie

8. GESTIONE DELLA NOTIFICA DI INCIDENTE DA PARTE DEL REFERENTE CSIRT

Section 6



Il Referente CSIRT, una volta ricevuta la comunicazione:

1. Registra l'incidente nel sistema di gestione incidenti con:
    - Timestamp di rilevazione
    - Informazioni del segnalante
    - Descrizione preliminare
2. Effettua una valutazione preliminare per determinare:
    - Gravità e urgenza
    - Necessità di escalation alla Direzione
    - Obbligo di notifica all'ACN
3. Si mette in contatto con le figure tecniche deputate alla risposta agli incidenti fornendo informazioni riguardo l'accaduto

8.1 Determinazione della Significatività

Un incidente è classificato come significativo se soddisfa uno dei seguenti criteri previsti dal D.lgs. 138/24:

a) Ha causato o può causare una grave perturbazione operativa dei servizi o perdite finanziarie per Laboratori Italiani Riuniti Campania S.p.A

b) Ha avuto o può avere ripercussioni su persone fisiche o giuridiche, determinando perdite materiali o immateriali considerevoli

8.2 Incidenti Significativi Soggetti a Notifica Obbligatoria

8.2.1 Per Soggetti Importanti (Allegato III Determina ACN)

- IS-1: Perdita di riservatezza verso l'esterno di dati digitali
- IS-2: Perdita di integrità con impatto verso l'esterno di dati
- IS-3: Violazione dei livelli di servizio attesi

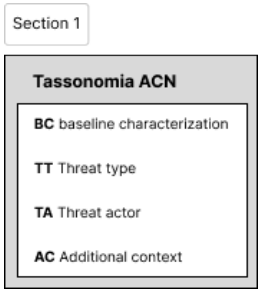
8.2.2 Per Soggetti Essenziali (Allegato IV Determina ACN)

- IS-1: Perdita di riservatezza verso l'esterno di dati digitali
- IS-2: Perdita di integrità con impatto verso l'esterno di dati
- IS-3: Violazione dei livelli di servizio attesi
- IS-4: Accesso non autorizzato o con abuso di privilegi a dati digitali

Nota: Laboratori Italiani Riuniti Campania S.p.A è classificata come Soggetto Essenziale ai sensi della normativa NIS2.

8.2.3 Classificazione secondo Tassonomia ACN

L'incidente viene classificato secondo quattro dimensioni identificate all'interno della tassonomia ACN:



8.2.4 Determinazione della Significatività

Il Referente CSIRT verifica se l'incidente soddisfa i criteri di significatività per:

- IS-1: Perdita di riservatezza di dati verso l'esterno
- IS-2: Perdita di integrità di dati con impatto verso l'esterno

- IS-3: Violazione dei livelli di servizio attesi
- IS-4 (solo soggetti essenziali): Accesso non autorizzato o abuso di privilegi

8.3 Utilizzo della Aegister Cyber Console®

Laboratori Italiani Riuniti Campania S.p.A utilizza la piattaforma Aegister per la gestione delle notifiche di incidenti. Il Referente CSIRT:

1. Accede alla sezione dedicata alla gestione delle notifiche
2. Avvia una nuova segnalazione tramite l'apposita funzionalità
3. Inserisce il timestamp di rilevamento da cui decorrono le tempistiche di notifica
4. Compila il titolo e il riepilogo dell'incidente
5. Seleziona il template appropriato (se disponibile) per la tipologia di incidente
6. Utilizza il supporto IA per:
    - Classificazione secondo tassonomia ACN
    - Valutazione preliminare dell'impatto (CIA)
    - Suggerimenti su azioni di mitigazione
    - Verifica delle tempistiche di notifica

La piattaforma offre al Referente CSIRT un insieme completo di strumenti per semplificare la gestione degli incidenti:

- Generazione automatica bozze: Le informazioni inserite vengono elaborate e strutturate secondo i campi richiesti dal modulo ACN
- Analisi IA: Supporto alla classificazione e alla valutazione dell'impatto
- Monitoraggio tempistiche: Contatori che indicano il tempo residuo per pre-notifica e notifica
- Link diretto al Portale ACN: Per procedere rapidamente all'invio ufficiale
- Esportazione report: Possibilità di scaricare la documentazione completa per archiviazione
- Funzione di archivio storico degli incidenti ai fini della compliance NIS 2

8.4 Predisposizione della Documentazione

Il Referente CSIRT prepara la documentazione necessaria che include:

8.4.1 Documentazione per la Notifica ACN

- Modulo di pre-notifica (entro 24 ore)
- Modulo di notifica completa (entro 72 ore)
- Eventuali aggiornamenti successivi
- Report finale dell'incidente

8.5 Coordinamento delle Attività di Risposta

Il Referente CSIRT coordina:

- Team IT/Security: Per contenimento tecnico e analisi forense
- Team Legale: Per valutazione obblighi normativi e implicazioni legali
- Team Comunicazione: Per gestione comunicazioni interne ed esterne (se autorizzate)
- CISO/Direzione: Per decisioni strategiche e autorizzazioni
- DPO (Data Protection Officer): In caso di coinvolgimento di dati personali
- Fornitori/Partner: Se l'incidente coinvolge sistemi o servizi di terze parti

9. SEGNALAZIONE ALL'ACN

Laboratori Italiani Riuniti Campania S.p.A, in qualità di Soggetto Essenziale ai sensi della Direttiva NIS2 e del D.lgs. 138/24, è tenuta a notificare all'Agenzia per la Cybersicurezza Nazionale (ACN) tutti gli incidenti qualificati come significativi.

La procedura di notifica si attiva nel momento in cui Laboratori Italiani Riuniti Campania S.p.A ha evidenza dell'avvenimento dell'incidente.

Evidenza significa che l'organizzazione dispone di elementi oggettivi dai quali si evince che si è verificato un incidente di sicurezza informatica, provenienti da:

- Rilevazioni interne (alert SIEM, EDR, antivirus, log analysis)
- Fonti esterne (segnalazioni CERT, partner, dark web monitoring)
- Rilevazioni del personale

IMPORTANTE: L'evidenza è tipicamente successiva al verificarsi effettivo dell'incidente. Le tempistiche di notifica decorrono dal momento dell'evidenza, non dal momento in cui l'incidente si è effettivamente verificato.

9.1 Processo di Notifica in Due Fasi

9.1.1 PRE-NOTIFICA (entro 24 ore dall'evidenza)

Obiettivo: Comunicazione iniziale rapida all'ACN

Contenuti minimi:

- Identificativo del soggetto notificante
- Data e ora di rilevazione dell'incidente
- Breve descrizione dell'evento
- Tipologia di incidente (secondo codici IS-1, IS-2, IS-3, IS-4)
- Classificazione secondo tassonomia ACN (contesto business, tipo minaccia, azioni, conseguenze)
- Indicazione preliminare della gravità
- Sistemi, servizi e dati coinvolti

- Misure di contenimento e mitigazione adottate
- Stima dei danni e delle conseguenze
- Indicazione di eventuali altri soggetti coinvolti
- Presenza di impatti transfrontalieri

Modalità: Tramite Portale ACN dedicato

Responsabile: Referente CSIRT

Strumenti: Aegister Cyber Console® supporta la compilazione guidata della pre-notifica

9.1.2 NOTIFICA COMPLETA (entro 72 ore dall'evidenza)

Obiettivo: Fornire informazione dettagliata dell'incidente

Contenuti richiesti:

- Descrizione dettagliata dell'incidente
- Classificazione secondo tassonomia ACN (contesto business, tipo minaccia, azioni, conseguenze)
- Timeline degli eventi
- Sistemi, servizi e dati coinvolti
- Valutazione dell'impatto (CIA triad)
- Misure di contenimento e mitigazione adottate
- Misure di rimedio pianificate
- Stima dei danni e delle conseguenze
- Indicazione di eventuali altri soggetti coinvolti
- Presenza di impatti transfrontalieri
- Coinvolgimento di infrastrutture critiche

Responsabile: Referente CSIRT

Approvazione: CISO/Direzione prima dell'invio

9.2 Accesso al Portale segnalazioni

URL: [https://segnalazioni.acn.gov.it/]

Autenticazione: [SPID / CIE / CNS] + [eventuale secondo fattore]

9.3 Aggiornamenti Successivi

Oltre alla pre-notifica e alla notifica completa, Laboratori Italiani Riuniti Campania S.p.A deve fornire:

9.3.1 Aggiornamenti Intermedi

- In caso di evoluzione significativa dell'incidente
- Su richiesta specifica dell'ACN
- Se emergono nuove informazioni rilevanti
- In caso di aggravamento della situazione

9.3.2 Report Finale

- Da inviare entro 30 giorni dalla risoluzione completa dell'incidente
- Include: analisi root cause, misure correttive implementate, lessons learned
- Chiusura formale dell'incidente

9.4 Conservazione della Documentazione

Tutta la documentazione relativa all'incidente e alle notifiche effettuate deve essere conservata per 5 anni e include:

- Comunicazione iniziale ricevuta
- Log ed evidenze tecniche
- Analisi e valutazioni effettuate
- Copie delle notifiche inviate all'ACN
- Comunicazioni ricevute dall'ACN
- Report finale dell'incidente
- Documentazione delle azioni correttive implementate

10. COMPORTAMENTI DA ADOTTARE E DA EVITARE

In questo capitolo sono elencate in modo esemplificativo le azioni che il personale dell'organizzazione deve e non deve compiere in caso di rilevazione di un evento di sicurezza che potrebbe potenzialmente essere etichettato come incidente.

10.1 AZIONI CONSENTITE (DO's)

Azione	Istruzioni Operative
Segnalare immediatamente	Contattare il Referente CSIRT senza ritardi, anche in caso di dubbio
Isolare il dispositivo	In caso di sospetta compromissione, disconnettere il cavo di rete o la connessione Wi-Fi. Non spegnere il sistema salvo istruzioni specifiche del team di sicurezza
Conservare le evidenze	Acquisire screenshot di messaggi di errore, alert o comportamenti anomali. Annotare data, ora e circostanze precise

Documentare le azioni	Tenere traccia di tutte le azioni intraprese, con timestamp precisi
Seguire le istruzioni	Attenersi rigorosamente alle indicazioni fornite dal Referente CSIRT o dal team di sicurezza
Collaborare attivamente	Fornire tutte le informazioni richieste e rendersi disponibili per chiarimenti
Mantenere la riservatezza	Trattare l'incidente come informazione riservata, da non divulgare all'esterno

10.2 AZIONI VIETATE (DON'Ts)

Azione Vietata	Motivazione
Spegnere o riavviare il dispositivo	Rischio di perdita di informazioni volatili (memoria RAM), log ed evidenze forensi essenziali per l'analisi. Il riavvio può anche attivare meccanismi di persistenza del malware
Cliccare su link o allegati sospetti	Può aggravare l'incidente, causare ulteriore compromissione o esfiltrazione dati
Modificare, cancellare o spostare file	Compromette le evidenze necessarie per l'analisi forense e può ostacolare le indagini
Tentare di risolvere autonomamente	Può causare perdita di evidenze, aggravamento dell'incidente o diffusione della compromissione
Divulgare informazioni all'esterno	È severamente vietato comunicare l'incidente a soggetti esterni, inclusi media, social media, forum online o altre organizzazioni. Le comunicazioni ufficiali sono gestite esclusivamente dalla Direzione e/o dal CISO
Pagare eventuali riscatti	In caso di ransomware, non effettuare pagamenti senza autorizzazione esplicita della Direzione e consultazione con le autorità competenti
Utilizzare dispositivi personali per attività aziendali	Durante o dopo un incidente, evitare di utilizzare dispositivi non controllati dall'azienda

Continuare a utilizzare sistemi compromessi	Non proseguire attività lavorative su sistemi sospetti o confermati come compromessi

10.3 Comportamenti Specifici per Tipologia di Incidente

10.3.1 In caso di **Phishing/E-mail Sospette**

DA FARE	**DA NON FARE**
Non cliccare su link o allegati	Rispondere all'email
Non fornire credenziali o informazioni	cancellare l'e-mail prima della segnalazione
Inoltrare l'e-mail al Referente CSIRT	Avvisare altri colleghi tramite lo stesso sistema e-mail (potrebbe essere compromesso)
Segnalare immediatamente	

10.3.2 In caso di **Malware/Ransomware**

DA FARE	**DA NON FARE**
Disconnettere immediatamente dalla rete (Wi-Fi o cavo)	Tentare di rimuovere il malware autonomamente
Fotografare eventuali messaggi di riscatto	Pagare riscatti
Lasciare il dispositivo acceso (salvo istruzioni diverse)	Formattare o pulire il disco
Segnalare immediatamente	Riconnettere alla rete

10.3.3 In caso di **Furto/Smarrimento Dispositivi**

DA FARE	**DA NON FARE**
Segnalare immediatamente specificando: tipo di dispositivo, data/ora/luogo dell'evento, dati potenzialmente contenuti	Ritardare la segnalazione per cercare autonomamente il dispositivo
Modificare password di accesso aziendale	Tentare di recuperare il dispositivo se rubato (rischio personale)
Collaborare per eventuale blocco remoto del dispositivo	

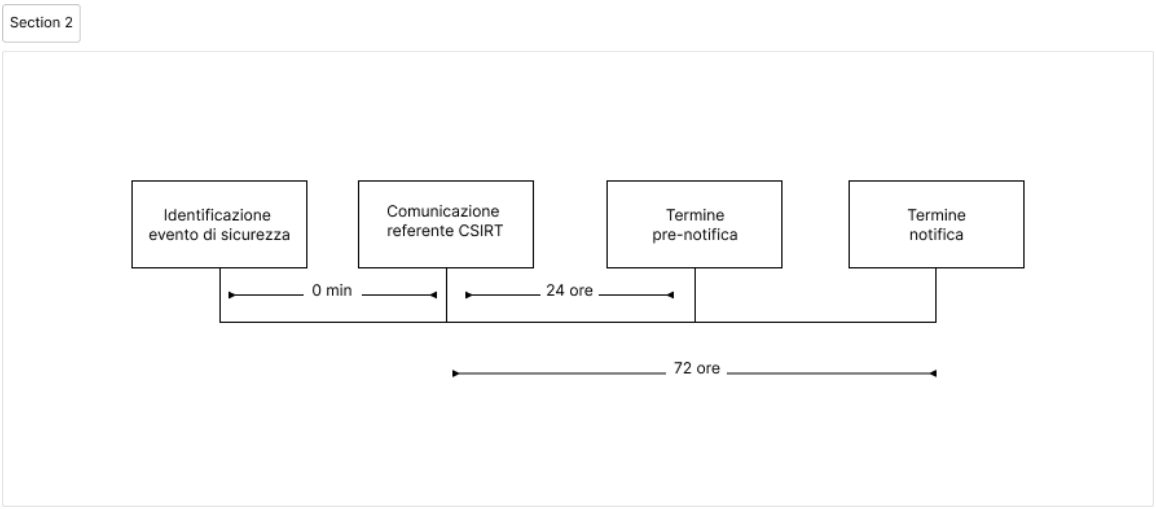
10.3.4 In caso di **Accesso Non Autorizzato**

DA FARE	DA NON FARE
Disconnettere l'account se possibile	Non modificare dati o configurazioni per "ripulire"
Cambiare le password (solo su istruzione del team di sicurezza)	Non cancellare log o cronologie
Verificare attività recenti dell'account	Non continuare a utilizzare l'account compromesso
Segnalare immediatamente	

11. TEMPISTICHE E SCADENZE

11.1 Timeline del Processo di Gestione Incidenti

Il diagramma illustra la **procedura operativa per la segnalazione degli incidenti di sicurezza**.



11.2 Responsabilità per il Rispetto delle Tempistiche

Fase	Responsabile	Tempistica
Comunicazione evento	Tutto il personale	Immediata
Conferma ricezione	Referente CSIRT	/
Valutazione preliminare	Referente CSIRT	/
Pre-notifica ACN	Referente CSIRT	Entro 24 ore

Notifica completa ACN	Referente CSIRT	Entro 72 ore
Approvazione notifiche	CISO/Direzione	Prima dell'invio
Report finale	Referente CSIRT	Entro 30 gg da chiusura

11.3 Conseguenze del Mancato Rispetto delle Tempistiche

Il mancato rispetto degli obblighi di notifica nei termini previsti può comportare:

- Sanzioni amministrative secondo quanto previsto dal D.lgs. 138/24
- Responsabilità legali per Laboratori Italiani Riuniti Campania S.p.A. e per i soggetti responsabili
- Danni reputazionali nei confronti di clienti, partner e autorità
- Aggravamento dell'impatto dell'incidente per mancata tempestività

11.4 Gestione Incidenti in Orario Non Lavorativo

Gli obblighi di notifica non si interrompono durante orari non lavorativi, fine settimana o festività.

Procedure per situazioni fuori orario:

- I canali di segnalazione sono attivi 24/7
- Il Referente CSIRT è reperibile tramite e-mail
- In caso di indisponibilità del Referente CSIRT primario, contattare: Vincenzo Forino
- Per incidenti critici rilevati fuori orario, è prevista l'escalation automatica al CISO

12. ALLEGATI

Allegato A - Contatti di Emergenza

Referente CSIRT Primario

- Nome: Cesareo Mangiacapre
- E-mail: incidenti@lirspa.com
- Telefono: 349 0911161
- Reperibilità: 24/7

Sostituto referente CSIRT

- Nome: Vincenzo Forino
- E-mail: v.forino@lirspa.com
- Telefono: 339 1723907

- Reperibilità: 24/7

CISO (Chief Information Security Officer)

- Nome: Cesareo Mangiacapre
- E-mail: ict@lirspa.com
- Telefono: 349 09111161

Ufficio Legale

- E-mail: affarigenerali@azienda.it

Allegato B - Link e Risorse Utili

Portale ACN

- URL: [https://portale.acn.gov.it]
- Documentazione: [https://www.acn.gov.it]

Piattaforma Interna di Gestione Incidenti

- URL: [Aegister Cyber Console]
- Manuale referente CSIRT: [www.lirspa.com/compliance/]

Risorse Esterne

- CSIRT Italia: [https://csirt.gov.it]
- ENISA (European Union Agency for Cybersecurity): [https://www.enisa.europa.eu]

Allegato C - Moduli e Template

Template E-mail di comunicazione Vedi Sezione 7.3

Checklist di Primo Intervento da allegare alla comunicazione al Referente CSIRT

Istruzioni: Questa scheda deve essere utilizzata dal segnalante o dal primo operatore intervenuto per validare le azioni intraprese prima di trasferire la gestione al team specialistico (CSIRT).
SEZIONE A: AZIONI OPERATIVE (Contenimento e Segnalazione)
[ ] **Rilevazione:** L'evento è stato rilevato e i dettagli (data, ora, sintomi) sono stati annotati.
[ ] **Evidenze:** Sono stati acquisiti screenshot, foto dello schermo o log visibili (senza alterare il sistema).
[ ] **Isolamento:** Il dispositivo è stato disconnesso dalla rete (cavo scollegato / Wi-Fi spento) *ove applicabile secondo procedura*.
[ ] **Notifica:** Il Referente CSIRT è stato contattato e la segnalazione (via email o telefono) è stata

effettuata.
SEZIONE B: INTEGRITÀ FORENSE (Divieti)
[ ] **ALIMENTAZIONE:** Confermo che il sistema **NON è stato spento né riavviato** (preservazione RAM).
[ ] **MODIFICHE:** Confermo che **NON sono state apportate modifiche** (nessun file aperto, salvato o software installato/rimosso dopo l'incidente).
[ ] **RISERVATEZZA:** Confermo che **NON sono state effettuate comunicazioni esterne** o non autorizzate in merito all'evento.
SEZIONE C: REPERIBILITÀ
[ ] Il segnalante conferma la propria disponibilità immediata per eventuali richieste di chiarimento o follow-up tecnico.

Allegato D - Glossario

ACN: Agenzia per la Cybersicurezza Nazionale

CERT: Computer Emergency Response Team

CISO: Chief Information Security Officer

CSIRT: Computer Security Incident Response Team

DDoS: Distributed Denial of Service

DPO: Data Protection Officer

EDR: Endpoint Detection and Response

IDS/IPS: Intrusion Detection System / Intrusion Prevention System

Incidente Significativo: Incidente che soddisfa i criteri di gravità previsti dalla normativa NIS2

Malware: Software malevolo (virus, trojan, ransomware, ecc.)

NIS2: Direttiva (UE) 2022/2555 sulla sicurezza delle reti e dei sistemi informativi

Phishing: Tecnica di attacco basata sull'inganno per ottenere credenziali o informazioni

Ransomware: Malware che cripta i dati e richiede un riscatto

SIEM: Security Information and Event Management

Soggetto Essenziale: Organizzazione di particolare importanza secondo NIS2

Soggetto Importante: Organizzazione rilevante secondo NIS2

Allegato E – Do’s and Dont’s