GUIDA RAPIDA GESTIONE INCIDENTI DI SICUREZZA

Aegister SpA

REGOLA FONDAMENTALE: IN CASO DI DUBBIO, COMUNICA SEMPRE

Non è richiesta certezza assoluta • Non tentare risoluzioni autonome • Non ritardare per verifiche personali • La tempestività è essenziale

1. COSA SEGNALARE - PRINCIPALI TIPOLOGIE DI INCIDENTI

RISERVATEZZA

- **Data Breach:** accesso non autorizzato a dati, esfiltrazione database
- **Phishing:** email sospette, BEC, vishing, smishing
- **Furto credenziali:** password sottratte

INTEGRITÀ

- **Manipolazione dati:** modifica database, documenti alterati
- **Defacement:** modifica siti web, contenuti social

DISPONIBILITÀ

- **DDoS:** saturazione risorse, servizi irraggiungibili
- **Ransomware:** crittografia con richiesta riscatto
- **Interruzioni:** crash sistemi, downtime server

MALWARE E ACCESSI

- **Malware:** trojan, worm, spyware, keylogger
- **Accessi non autorizzati:** account compromessi
- **Insider threat:** abuso privilegi, sabotaggio

INCIDENTI FISICI

- Furto/smarrimento dispositivi (laptop, smartphone)
- Accesso non autorizzato a locali
- Manomissione hardware

ALTRI INCIDENTI

- **Vulnerabilità:** exploit, SQL injection
- **Supply chain:** fornitori compromessi
- **Comunicazioni:** intercettazioni, MitM

2. COME SEGNALARE - PROCEDURA IMMEDIATA

CONTATTI EMERGENZA (ATTIVI 24/7)

```
EMAIL:        [incidenti@lirspa.com]
TELEFONO:     [+39 349 0911161] (primario)
              [+39 339 1723907] (alternativo)
```

IMPORTANTE: Utilizzare preferibilmente ENTRAMBI i canali (email E telefono) per garantire ricezione immediata

Template Email di Segnalazione

```
A: incidenti@lirspa.com
Oggetto: [URGENTE] Comunicazione Incidente - [Breve descrizione]
DATI SEGNALANTE:Nome: [Nome Cognome] Ruolo/Reparto: [Ruolo - Reparto] Contatti: [Telefono] | [Email]
DESCRIZIONE EVENTO: [Cosa è stato rilevato, errori, comportamenti anomali]
DATA/ORA RILEVAZIONE:[GG/MM/AAAA - HH:MM]
SISTEMA COINVOLTO:[Nome sistema/dispositivo/applicazione]
AZIONI INTRAPRESE:[Elenco azioni già effettuate o "Nessuna"]
EVIDENZE:[Indicare screenshot/log allegati]
```

La mancanza di una o più informazioni NON deve in alcun modo ritardare la comunicazione

3. COSA FARE E NON FARE

AZIONI CONSENTITE (DO's)

- **Segnalare immediatamente** anche in caso di dubbio
- **Isolare dispositivo:** disconnettere rete (NO spegnere)
- **Conservare evidenze:** screenshot, annotare data/ora
- **Documentare:** tracciare azioni con timestamp
- **Seguire istruzioni** del team sicurezza
- **Mantenere riservatezza:** non divulgare esternamente

AZIONI VIETATE (DON'Ts)

- **Spegnere/riavviare:** perdita RAM ed evidenze forensi
- **Cliccare link sospetti:** aggrava compromissione
- **Modificare/cancellare file:** compromette evidenze
- **Risolvere autonomamente:** causa perdita evidenze
- **Divulgare esternamente:** solo via Direzione/CISO
- **Pagare riscatti:** solo con autorizzazione Direzione
- **Usare sistemi compromessi:** non proseguire attività

GUIDA RAPIDA GESTIONE INCIDENTI DI SICUREZZA

Aegister SpA

REGOLA FONDAMENTALE: IN CASO DI DUBBIO, COMUNICA SEMPRE

Non è richiesta certezza assoluta • Non tentare risoluzioni autonome • Non ritardare per verifiche personali • La tempestività è essenziale

4. COMPORTAMENTI SPECIFICI PER TIPOLOGIA DI INCIDENTE

EMAIL SOSPETTE / PHISHING

DA FARE:

- Non cliccare link o allegati
- Non fornire credenziali
- Inoltrare email al Referente CSIRT
- Segnalare immediatamente

NON FARE:

- Rispondere all'email
- Cancellare prima della segnalazione
- Avvisare colleghi via email compromessa

MALWARE / RANSOMWARE

DA FARE:

- Disconnettere rete immediatamente
- Fotografare messaggi di riscatto
- Lasciare dispositivo acceso
- Segnalare subito

NON FARE:

- Rimuovere malware autonomamente
- Pagare riscatti
- Formattare o pulire disco
- Riconnettere alla rete

FURTO / SMARRIMENTO DISPOSITIVI

DA FARE:

- Segnalare subito: tipo/data/ora/luogo/dati
- Modificare password aziendale
- Collaborare per blocco remoto

NON FARE:

- Ritardare per cercare autonomamente
- Tentare recupero se rubato (rischio personale)

ACCESSO NON AUTORIZZATO

DA FARE:

- Disconnettere account se possibile
- Cambiare password (solo su istruzione)
- Verificare attività recenti
- Segnalare immediatamente

NON FARE:

- Modificare dati per "ripulire"
- Cancellare log o cronologie
- Continuare a usare account compromesso

5. CHECKLIST RAPIDA PRIMO INTERVENTO

✓ **A ALLEGARE ALLA MAIL:**

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

☐ **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

CONTATTI REFERENTI

Referente CSIRT Primario
Nome: Cesareo Mangiacapre
Email: incidenti@lirpa.com
Tel: 349 0911161
Reperibilità: 24/7

Sostituto CSIRT
Nome: Vincenzo Forino
Email: v.forino@lirspa.com
Tel: 339 1723907
Reperibilità: 24/7

CISO
Nome: Cesareo Mangiacapre
Email: incidenti@lirpa.com
Tel: 349 0911161

La tempestività è essenziale per una gestione efficace degli incidenti. Meglio una segnalazione con informazioni parziali che un ritardo per raccogliere dettagli completi.