# NOTIFICA INCIDENTE DI SICUREZZA

**Titolo documento:** Notifica di incidente di sicurezza
**Versione:** 1.0
**Data:** _____
**Referente della segnalazione:** _____
**Ruolo/Unità organizzativa:** _____
**Contatti:** _____

---

1. **Informazioni generali sull'incidente**
   - **ID incidente:** _____
   - **Data/Ora del rilevamento:** _____
   - **Data/Ora del presunto inizio:** _____
   - **Stato dell'incidente:** ☐ Aperto ☐ In corso ☐ Mitigato ☐ Chiuso
   - **Segnalato da:** ☐ Persona interna ☐ Sistema di monitoraggio ☐ Terza parte ☐ Altro: _____

---

2. **Modalità di rilevamento (selezionare una o più opzioni):**
   ☐ Alert da sistemi di sicurezza (SIEM/IDS/IPS/EDR, ecc.)
   ☐ Anomalia rilevata dal SOC interno/esterno
   ☐ Segnalazione interna (utente/reparto/IT)
   ☐ Segnalazione da fornitore/terza parte
   ☐ Analisi di log/attività di monitoraggio periodico
   ☐ Attività di audit/vulnerability assessment
   ☐ Altro: _____

**Descrizione iniziale dell'evento osservato:**

- Data e ora del primo evento sospetto (se note): _____
- Sistema/servizio coinvolto: _____
- Sintomi osservati: _____
- Prime evidenze tecniche disponibili (log, IoC, screenshot, sample): _____
- Soggetto che ha effettuato il rilevamento: _____

---

## 3. Acquisizione e registrazione delle informazioni

**Informazioni tecniche disponibili al momento della rilevazione:**

- Host/Server coinvolti: _____
- Utenti coinvolti: _____
- Applicazioni/Servizi impattati: _____
- IP/MAC/Domini/Hash/IOC: _____
- Log/Timestamp chiave: _____
- Evidenze digitali: _____ (invio zip password "infectedacn")

**Azioni preliminari di raccolta dati:**
☐ Salvataggio log
☐ Snapshot sistemi
☐ Raccolta segnalazioni
☐ Isolamento asset
☐ Analisi IOC
☐ Altro: _____

---

## 4. Classificazione dell'incidente

**Tipologia (codice tassonomia ACN):**
☐ _____

**Livello gravità: ☐ Basso ☐ Medio ☐ Alto ☐ Critico**

Impatto stimato:

- Continuità: _____
- Reputazione: _____
- Altro:_____

---

**5. Gestione dell'incidente**

- **Azioni intraprese per contenere l'incidente:**

- **Misure di mitigazione attuate:**

- **Unità coinvolte nelle attività di risposta:**

---

**6. Raccolta evidenze e analisi forense**

- **Evidenze raccolte:**
  ☐ Log di sistema
  ☐ Log firewall / IDS / IPS
  ☐ Immagini forensi/snapshot/memory dump
  ☐ Testimonianze / segnalazioni
  ☐ Backup pre/post-incidente
  ☐ Altro: _____

- **Stato dell'analisi forense:**
  ☐ Avviata
  ☐ In corso
  ☐ Completata
  ☐ Non necessaria

- **Risultati preliminari dell'analisi:**

---

**7. Comunicazioni dell'incidente**

- **Comunicazioni interne effettuate:**
  ☐ Direzione
  ☐ IT / SOC
  ☐ DPO
  ☐ HR
  ☐ Ufficio legale
  ☐ Altro: _____
- **Comunicazioni esterne effettuate:**
  ☐ CSIRT Italia
  ☐ Fornitori / partner
  ☐ Autorità Garante (se applicabile)
  ☐ Clienti / utenti (se applicabile)
  ☐ Altro: _____
- **Data e modalità della comunicazione al CSIRT:**

---

**8. Gestione post-incidente**

- **Ripristino della piena operatività:**
  - Data/Ora conclusione ripristino: _____
  - Sistemi reintegrati: _____
- **Analisi delle cause radice**
  - Root Cause: _____
  - Contributori: _____
- **Update CSIRT:**

  ☐ Report finale inviato
- **Misure correttive e preventive suggerite:**
  ☐ Introduzione nuove policy
  ☐ Miglioramento configurazioni di sicurezza
  ☐ Aggiornamento sistemi
  ☐ Formazione personale
  ☐ Revisione procedure
  ☐ Altro: _____

- **Lezioni apprese:**

---

**9. Allegati**

- ☐ Log di sistema
- ☐ Report tecnico SOC
- ☐ Evidenze forensi
- ☐ Comunicazioni interne
- ☐ Comunicazioni esterne
- ☐ Diagrammi / timeline
- ☐ Altro: _____

---

**Firma del referente**

Nome e cognome: _____
Data: _____