

ALLEGATO 2. CYBER INCIDENT RESPONSE: “MANUALE OPERATIVO VISIVO PER LA RISPOSTA ALLE EMERGENZE CYBER”

Azienda Socio-Sanitaria Locale n.2 della Gallura

Sede Legale: via Bazzoni-Sircana, 2/2A – 07026 Olbia (SS)

Tel. 0789/552305 - www.aslgallura.it

Posta certificata: protocollo@pec.aslgallura.it

Codice Fiscale e Partita IVA: 02891650901

Revisione 00

Sommario

1	Descrizione e Oggetto del Documento	3
---	---	---

1 DESCRIZIONE E OGGETTO DEL DOCUMENTO

Il presente documento costituisce la **Procedura Operativa: Gestione e Notifica Incidenti Informatici** dell'**ASL Gallura** e di **ARES Sardegna**, concepita come manuale operativo visivo (*playbook*) per la risposta e la gestione standardizzata delle emergenze cyber.

Nello specifico, la procedura definisce:

- **Architettura Normativa e Matrice di Compliance:** Il quadro di adeguamento alla Direttiva NIS2 (D.Lgs. 138/2024) e alle linee guida dell'Agenzia per la Cybersicurezza Nazionale (ACN), con il dettaglio delle misure di sicurezza e dei requisiti richiesti per i soggetti essenziali e importanti, integrando la mappatura dei fornitori della *supply chain*.
- **Ecosistema Istituzionale e Modello Operativo "a Due Mani":** L'interazione integrata tra l'**ASL Gallura** (responsabile formale della compliance, della notifica e della valutazione dell'impatto clinico/amministrativo), **ARES Sardegna** (erogatore dei servizi di sicurezza centralizzati SOC, gestione tecnica dell'infrastruttura e contenimento) e il **CSIRT Italia** (struttura nazionale di coordinamento e unico interlocutore per le notifiche legali).
- **Organigramma e Matrice delle Responsabilità (RACI):** L'attribuzione dei ruoli interni dell'ASL 2 Gallura per l'operatività sul portale ACN:
 - **Punto di Contatto (PdC):** Referente primario, *owner* dell'attivazione tempestiva delle notifiche e dell'invio formale dei dati.
 - **Sostituto PdC (SPdC):** Figura vicaria per garantire continuità all'accesso operativo e all'inserimento dati in caso di assenza del PdC.
 - **Segreteria (SG):** Gestione documentale, supporto amministrativo e *owner* del monitoraggio delle scadenze legali.
- **Tassonomia e Timeline Perentorie di Notifica:** La classificazione degli incidenti ai sensi del DPCM 81/2021 (criticità ICP-B entro 1 ora, ICP-A entro 6 ore) e l'iter procedurale di legge in 3 step: *Minuto Zero* (\$T_0\$), *Segnalazione Iniziale / Early Warning* entro 24 ore (\$T+24h\$) e *Notifica Completa* entro 72 ore (\$T+72h\$).
- **Fasi CSIRT e Protocollo Tecnico per i Malware:** Le 4 fasi operative del CSIRT Italia (Raccolta metriche, Notifica su piattaforma, *Incident Handling* con report entro 5 giorni, Chiusura formale) e la procedura di trasmissione in sicurezza di campioni malevoli tramite archivio ZIP protetto da password standard (infectedacn) all'indirizzo dedicato.
- **Scadenze e Postura Continuativa:** La pianificazione degli adempimenti ricorrenti, tra cui la scadenza annuale del 31 maggio (aggiornamento anagrafica ACN), la scadenza del 30 giugno (mappatura *supply chain* e categorizzazione ex Art. 30 D.Lgs. 138/2024) e l'avvio dell'Ufficio della Cyber Sicurezza aziendale.



Procedura Operativa: Gestione e Notifica Incidenti Informatici

Linee Guida ACN, Compliance NIS2 e Modello ARES-ASL

UN MANUALE OPERATIVO VISIVO PER LA RISPOSTA ALLE EMERGENZE CYBER

Architettura Normativa e Modello Regionale



Direttiva NIS2 & D.Lgs 138/2024

Recepimento nazionale per garantire un livello comune elevato di cybersicurezza.



ACN (Agenzia per la Cybersicurezza Nazionale)

Autorità nazionale competente. Emanazione delle specifiche di base e gestione operativa del CSIRT Italia.



Modello Regionale ARES-ASL

Gestione centralizzata dei servizi ICT e di cybersicurezza regionale (Servizi SOC integrati via Consip ID 2296).

Soggetti Essenziali

43

Misure di
Sicurezza

116

Requisiti

Applicazione rigorosa per infrastrutture
ad altissima criticità.

Soggetti Importanti

37

Misure di
Sicurezza

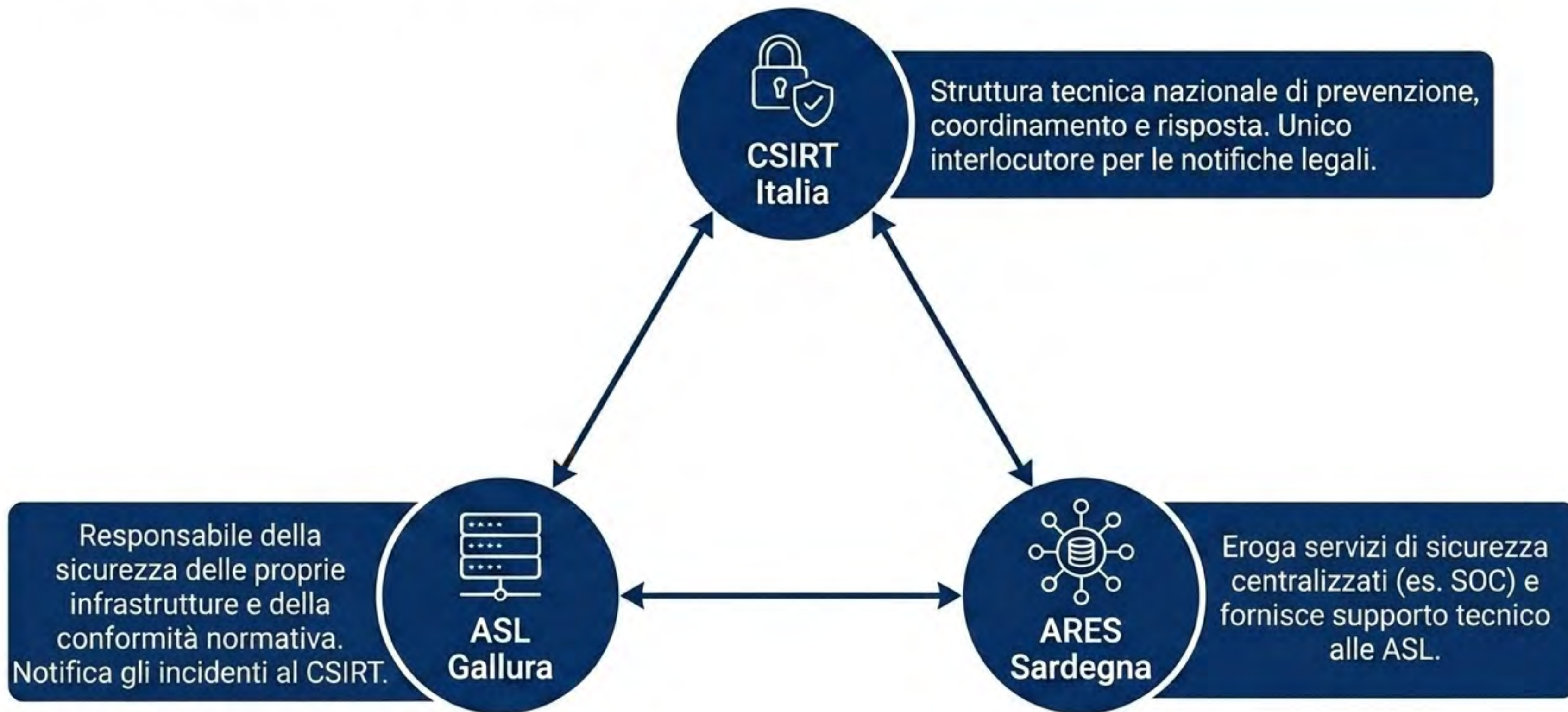
87

Requisiti

Conformità richiesta per entità sistemiche
della catena di approvvigionamento.

ASL Gallura ha attivato in accorso e con il supporto di ARES la mappatura dei propri fornitori rilevanti per garantire la sicurezza lungo tutta la supply chain.

L'Ecosistema Istituzionale: Ruoli e Relazioni



Designazione Ufficiale ASL 2 Gallura (D.Lgs. 138/2024)



Punto di Contatto (PdC)

Referente primario per l'interlocuzione formale e tecnica con l'Autorità Nazionale ACN.



Sostituto PdC (SPdC)

Supporta il PdC e ne assume integralmente le funzioni in caso di assenza o impedimento per garantire continuità.



Segreteria (SG)

Supporto tecnico-amministrativo, gestione documentale e monitoraggio stringente delle scadenze istituzionali.

Matrice Operativa delle Responsabilità (RACI)

Attività	PdC	SPdC	SG
Aggiornamento Portale ACN	Valida e Invia	Inserimento Dati	Gestione Documentale
Notifica Incidenti Informatici	Attivazione Tempestiva (Owner)	Subentro in Assenza	Supporto
Monitoraggio Scadenze Legali	Supervisione	Allineamento	Owner (es. 31 Maggio)
Integrazione Informativa ACN	Coordinamento Generale	Verifica Completezza Dati	Archiviazione

ICP-B

Impatto ICT Critico

**Notifica ENTRO 1 ORA
dal rilevamento**

ICP-A

Impatto ICT

**Notifica ENTRO 6 ORE
dal rilevamento**

ICP-C

Diversi da beni ICT

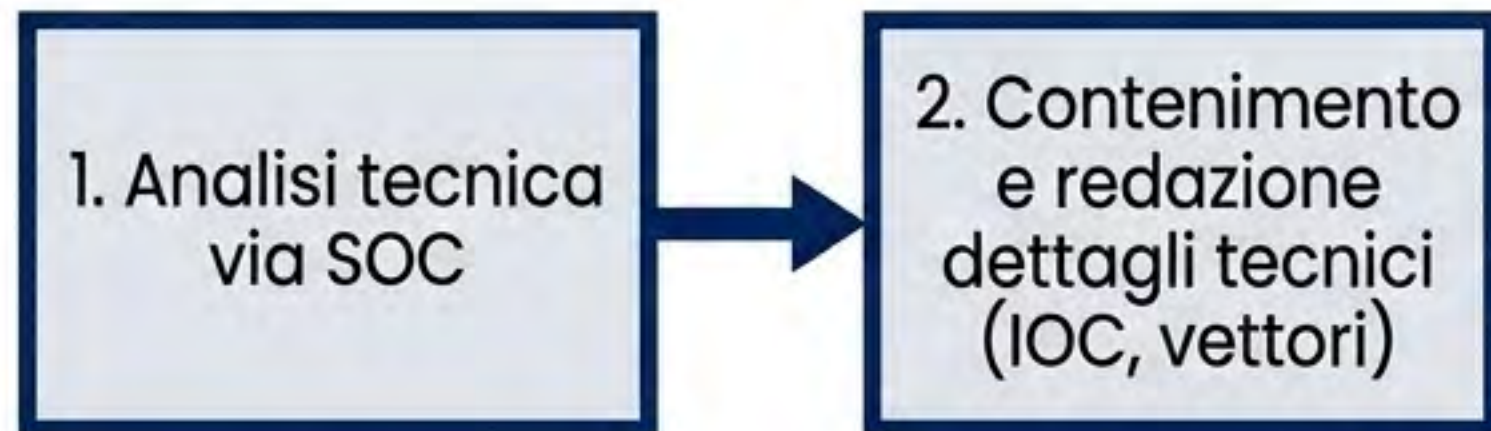
Nessuna tempistica perentoria
iniziale, **ma soggetto a
monitoraggio continuo.**

Il Modello a Due Mani: Flusso di Risposta ASL-ARES

Corsia ASL Gallura (Azione Locale)



Corsia ARES Sardegna (Azione Centralizzata)





1

Fase 1: Raccolta Metriche d'Impatto

- ☐ - Numero stimato di utenti impattati
- ☐ - Durata stimata dell'incidente
- ☐ - Diffusione geografica del disservizio
- ☐ - Mappatura degli asset compromessi

2

Fase 2: Notifica Piattaforma ACN

csirt.gov.it/segnalazione

- Data e ora esatta del rilevamento
- Vettori d'attacco identificati
- Misure di rientro intraprese
- Indicatori di Compromissione (IOC)

3

Fase 3: Gestione della Notifica (Incident Handling)

Il CSIRT Italia valuta il livello di gravità della segnalazione e fornisce supporto tecnico diretto (da remoto o in loco).

Requisito di Legge: Piena collaborazione e accesso tempestivo ai sistemi da parte dell'amministrazione. Report tecnico
tecnopito¹
obbligatorio entro 5 giorni.

4

Fase 4: Chiusura dell'Incidente

Fase finale successiva alla mitigazione.

- Risoluzione della criticità tecnica
- Ripristino completo e certificato dei servizi erogati
- Certificazione di chiusura formale del ticket di sicurezza con il CSIRT

PROTOCOLLO DI TRASMISSIONE CAMPIONI MALEVOLI

STEP 1: Isolare l'evidenza digitale (es. file eseguibili malware, email di phishing in formato .msg o .eml, file testuali di ransom note).

STEP 2: Inserire tutti i file probatori in un archivio compresso (formato ZIP).

STEP 3 (CRITICO): Proteggere l'archivio ZIP esclusivamente con la password standard imposta dall'Autorità:

infectedacn

STEP 4: Trasmettere l'archivio protetto all'indirizzo sicuro:
infected@csirt.gov.it

ATTENZIONE: NON ALLEGARE MAI MALWARE IN CHIARO NELLE COMUNICAZIONI E-MAIL.

Scadenza Perentoria (30 Giugno)

Categorizzazione definitiva delle attività e dei servizi (Art. 30 decreto NIS) e mappatura completa e validata dei fornitori rilevanti per la sicurezza della Supply Chain regionale.

Scadenza Annuale (31 Maggio)

Aggiornamento ricorrente sulla Piattaforma ACN dei Dati Organizzazione, Utenti, Domini e IP (a cura esclusiva del PdC e della Segreteria).

Le date sopra riportate sono le scadenze ad oggi imposte alla data di stesura di questo documento e che possono avere variazioni secondo gli aggiornamenti di ACN



L'integrazione strutturale tra ASL Gallura e ARES Sardegna garantisce una postura cibernetica resiliente, trasformando la mera compliance normativa in vera sicurezza operativa.

È in corso la costituzione formale dell'Ufficio della Cyber Sicurezza (d'intesa con ARES) per dettagliare ulteriormente le procedure di resilienza aziendale.