

PROCEDURA OPERATIVA: GESTIONE E NOTIFICA INCIDENTI INFORMATICI

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

Redatto:

Dott. Ing. Martino Ruiu

PROCEDURA OPERATIVA: GESTIONE E NOTIFICA INCIDENTI INFORMATICI

Approvato con Delibera del Direttore Generale n. ____ del ____ .08.2026

Dipartimento Area Amministrativa

Edizione:
01/2026

Revisione: 00

Sommario

1	ACRONIMI E DEFINIZIONI.....	3
2	CANALI DI SEGNALAZIONE E OBBLIGHI PER TERZE PARTI	3
3	ORGANIZZAZIONE DE TURNI E REGIME DI PRONTA DISPONIBILITA'	4
4	REQUISITI MINIMI DI SICUREZZA (MISURE TECNICHE E ORGANIZZATIVE.....	4
5	MATRICE DELLE RESPONSABILITA' (RACI)	5
6	DISPOSIZIONI FINALI, APPROVAZIONE E PUBBLICITÀ.....	6
6.1	MODALITÀ DI APPROVAZIONE E REVISIONE.....	6
6.2	PUBBLICITÀ E DIFFUSIONE	6
7	ALLEGATI	6

1 ACRONIMI E DEFINIZIONI

In conformità al quadro normativo vigente, in particolare il D.lgs. 138/2024 (Decreto NIS2) e il D.L. 82/2021, si definiscono i seguenti termini e acronimi:

Acronimo	Definizione
ACN	Agenzia per la Cybersicurezza Nazionale: Autorità nazionale competente e punto di contatto unico in materia di cybersicurezza ai sensi dell'Art. 7 del D.L. 82/2021.
ASL	Azienda Socio Sanitaria Locale: Nello specifico, la ASL Gallura (Azienda Socio Sanitaria Locale n. 2).
ARES	Azienda Regionale della Salute: Ente di supporto tecnico-operativo per il coordinamento della sanità regionale e dei dati anagrafici (NSIS).
CSIRT	Computer Security Incident Response Team: Gruppo di intervento per le emergenze informatiche preposto alla prevenzione, monitoraggio e risposta agli incidenti.
NIS	Network and Information Security: Riferito alla Direttiva (UE) 2022/2555 e al relativo decreto di recepimento D.Lgs. 138/2024.
PdC	Punto di Contatto: Referente primario per l'interlocuzione con l'ACN e responsabile della validazione delle dichiarazioni sulla piattaforma NIS.
SPdC	Sostituto Punto di Contatto: Figura che supporta il PdC e ne assume le funzioni in caso di assenza per garantire la continuità operativa (Art. 7, c. 4, D.Lgs. 138/2024).
RTD	Responsabile per la Transizione Digitale: Dirigente preposto alla gestione della trasformazione digitale (SC Tecnologia e Transizione Digitale).
SL	Soggetto Legittimato: Ente riconosciuto come "Soggetto Incluso" negli elenchi NIS o nel Perimetro di Sicurezza Nazionale Cibernetica.
MFA	Multi-Factor Authentication: Sistema di autenticazione a più fattori obbligatorio per l'accesso ai portali istituzionali e alla piattaforma ACN.

2 CANALI DI SEGNALAZIONE E OBBLIGHI PER TERZE PARTI

È fatto obbligo inderogabile a tutti i fornitori esterni, collaboratori e consulenti operanti presso le sedi della ASL di segnalare senza indugio ogni potenziale incidente informatico, anomalia di sistema o sospetta violazione della sicurezza rilevata sulle infrastrutture della ASL Gallura.

La segnalazione dovrà essere inoltrata esclusivamente attraverso i seguenti canali ufficiali:

Canale Tecnico Operativo (CSIRT): tecnologia.transizionedigitale@aslgallura.it;

Canale Formale (Protocollo): protocollo@pec.aslgallura.it (da inviare per conoscenza);

La mancata osservanza dei canali indicati o il ritardo nella comunicazione costituiscono una grave violazione procedurale, soggetta all'attivazione delle clausole sanzionatorie previste dai contratti in essere o alla risoluzione degli stessi per inadempimento.

PROCEDURA OPERATIVA: GESTIONE E NOTIFICA INCIDENTI INFORMATICI

3 ORGANIZZAZIONE DE TURNI E REGIME DI PRONTA DISPONIBILITA'

Al fine di assicurare un presidio permanente e la resilienza dei servizi essenziali, l'articolazione oraria dei referenti della cybersicurezza è stabilita come segue:

1. Orario Operativo Ordinario:

- Lunedì – Giovedì: ore 08:00 – 18:00;
- Venerdì: ore 08:00 – 14:00;
- In questa fase l'operatività è garantita dal personale interno turnante della SC Tecnologia e Transizione Digitale.

2. Regime di Pronta Disponibilità:

- Dal Venerdì alle ore 14:00 al Lunedì alle ore 08:00;
- Copertura h24 per i giorni festivi e prefestivi;

Durante il regime di reperibilità, è garantito un presidio congiunto tra i tecnici interni della ASL Gallura e i referenti del **CSIRT ARES**. Tale sinergia è finalizzata alla gestione immediata delle criticità e al tempestivo riscontro alle richieste dell'Autorità Nazionale (ACN).

4 REQUISITI MINIMI DI SICUREZZA (MISURE TECNICHE E ORGANIZZATIVE

Il processo di gestione e notifica deve seguire rigorosamente la timeline definita dalla Guida ACN, pena l'irrogazione della sanzioni amministrative previste dalla legge.

- **T0: Acquisizione Evidenza e Triage Tecnico:** Al rilevamento dell'evento, si procede alla classificazione immediata del livello di gravità:
 - **IS-1 (Informativo):** Anomalie minori o eventi di scansione senza impatto;
 - **IS-2 (Basso):** Incidente con impatto limitato su endpoint isolati;
 - **IS-3 (Medio):** Incidente con parziale interruzione dei servizi sanitari o amministrativi;
 - **IS-4 (Alto/Critico):** Compromissione sistemica, esfiltrazione dati sensibili o blocco totale delle attività.
- **T+24h: Invio Pre-notifica:** Entro 24 ore dall'evidenza, è fatto obbligo di inserire i dati sul Portale ACN secondo la modalità "a due mani":
 - **CSIRT ARES** ha la responsabilità dell'inserimento dei dettagli tecnici, inclusi gli Indicatori di Compromissione (IoC) e le Tattiche, Tecniche e Procedure (TTP) rilevate;
 - **ASL Gallura** deve fornire i dati di contesto organizzativo e la stima dell'impatto

PROCEDURA OPERATIVA: GESTIONE E NOTIFICA INCIDENTI INFORMATICI

- operativo (es. numero di postazioni impattate, servizi interrotti);
 - L'invio finale richiede obbligatoriamente la validazione tramite **firma digitale (CADES/PADES)** da parte del **PdC** o, in sua vece, dello **SPdC**.
 - **T+72h: Invio Notifica Completa:** Entro il termine perentorio di 72 ore dall'evidenza, deve essere trasmessa l'analisi post-incidente dettagliata, comprensiva delle misure di mitigazione adottate e del piano di ripristino (*remediation*).
-

5 MATRICE DELLE RESPONSABILITA' (RACI)

I compiti istituzionali sono assegnati alle seguenti figure, in conformità alle designazioni formali della Direzione Genrale:

- **PdC:**
 - Referente primario per l'Autorità Nazionale NIS.
 - Validazione finale e invio formale delle dichiarazioni sulla piattaforma NIS.
 - Coordinamento delle integrazioni informative richieste da ACN.
- **SPdC:**
 - Supporto operativo nell'inserimento dati sul portale.
 - **Obbligo di verifica periodica delle sezioni:** "Utenti e Ruoli", "Domini e IP", "Dati Organizzazione" e "Fornitori".
 - Garanzia di continuità assoluta degli adempimenti in caso di assenza o impedimento del PdC.
- **SG:**
 - Supporto tecnico-amministrativo e gestione documentale.
 - Monitoraggio delle scadenze istituzionali, con particolare attenzione per la scadenza annuale del 31 maggio per l'aggiornamento anagrafico.
- **CSIRT ARES:**
 - Analisi tecnica di dettaglio e supporto al triage.
 - Inserimento dei parametri tecnici e degli IoC nel portale ACN.

Clausola di Collaborazione Istituzionale: È fatto obbligo ai soggetti designati di mantenere un canale di collaborazione costante con **ARES Sardegna** per l'allineamento dei dati anagrafici (NSIS). In particolare si richiama il rispetto delle procedure per garantire l'efficacia del tavolo tecnico congiunto e la tempestività della risposta agli incidenti.

6 DISPOSIZIONI FINALI, APPROVAZIONE E PUBBLICITÀ

6.1 MODALITÀ DI APPROVAZIONE E REVISIONE

La presente procedura è adottata con deliberazione del Direttore Generale (DG), su proposta del Responsabile per la Transizione Digitale (RTD), che ne cura la coerenza con il Piano Triennale per l'Informatica nella PA.

Considerata la natura transitoria del presente atto, adottato con carattere di urgenza nelle more del completamento delle attività tecnico-documentali coordinate da ARES Sardegna (in attuazione dei Piani Operativi Consip Lotto 2), il documento sarà oggetto di revisione e aggiornamento periodico.

L'aggiornamento della procedura è previsto obbligatoriamente nei seguenti casi:

- **Evoluzione normativa:** recepimento di nuove disposizioni nazionali o europee in materia di cybersicurezza (es. implementazione definitiva del D.Lgs. 138/2024 o modifiche alla L. 90/2024);
- **Armonizzazione regionale:** adozione di procedure definitive e modelli di risposta agli incidenti elaborati d'intesa tra ARES e le Aziende del SSR per garantire uniformità di indirizzo;
- **Miglioramento continuo:** introduzione di nuove pratiche organizzative o tecnologiche volte a incrementare l'efficacia, l'efficienza e la resilienza cibernetica dei servizi sanitari;
- **Esiti di Incident Handling:** qualora l'analisi post-incidente o le attività di monitoraggio e test evidenzino l'inadeguatezza delle procedure vigenti rispetto alle minacce rilevate.

6.2 PUBBLICITÀ E DIFFUSIONE

Al fine di garantire la piena accountability dell'Ente e la conoscenza dei flussi di segnalazione da parte di tutti i soggetti coinvolti, la presente procedura viene:

- Pubblicata sul sito istituzionale dell'Amministrazione, all'interno della sezione "Amministrazione Trasparente", ai sensi del D.Lgs. 33/2013;
- Resa disponibile agli operatori e a tutto il personale dipendente tramite pubblicazione nell'area dedicata della INTRANET aziendale;
- Trasmessa formalmente ai Direttori delle UOR (Unità Organizzative Responsabili) e ai fornitori di servizi ICT rilevanti, affinché ne recepiscano i contenuti nei rispettivi ambiti operativi e contrattuali.

7 ALLEGATI

Allegato: Cyber Incident Response: *“manuale operativo visivo per la risposta alle emergenze cyber”*