DELIBERAZIONE DEL DIRETTORE GENERALE

Deliberazione n.ro	Data di Adozione
0000001	08/01/2026

OGGETTO: UOSVD Cybersicurezza - Adozione della Politica di Gestione degli incidenti di Cybersicurezza in adempimento alla direttiva UE 2022/2555 così come recepita in Italia dal D.Lgs. n. 138/2024

PROPOSTA DI DELIBERAZIONE DEL DIRETTORE GENERALE N.RO 20250003049 DEL 30/12/2025
COMPOSTA COMPLESSIVAMENTE DA 5 (cinque) PAGINE
DI 1 (uno) ALLEGATI SOGGETTI A PUBBLICAZIONE PER UN TOTALE DI 35 (trentacinque) PAGINE
DI 0 (zero) ALLEGATI NON SOGGETTI A PUBBLICAZIONE PER UN TOTALE DI 0 (zero) PAGINE
DI 1 (uno) DOCUMENTI ISTRUTTORI NON ALLEGATI PER UN TOTALE DI 39 (trentanove) PAGINE

Con la sottoscrizione in calce, i Direttori dichiarano di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, l. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/2013, vigente codice di comportamento aziendale e art. 1, c. 9, lett. e), l. 190/2012 – quest'ultimo come recepito, a livello aziendale, della vigente sezione Anticorruzione e Trasparenza del PIAO – tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, D.L.gs. 165/2001.

Parere della Direttrice Amministrativa	Parere della Direttrice Sanitaria
Firmato Digitalmente il 08/01/2026 14:33 Rachele POPOLIZIO	*Firmato Digitalmente il 08/01/2026 15:22* Rosella SQUICCIARINI

Il Segretario	Il Direttore Generale
Firmato Digitalmente il 08/01/2026 17:28 Filomena BAVARO	*Firmato Digitalmente il 08/01/2026 17:20* Luigi FRUSCIO

ATTESTAZIONE DI AVVENUTA PUBBLICAZIONE

Si attesta che il presente provvedimento viene pubblicato all'Albo pretorio *on-line* della ASL BA, ai sensi dell'art. 32, c. 1, l. 69/2009, per la durata di 30 giorni naturali, decorrenti dal **08/01/2026**

Unità Operativa Affari Generali
L'Addetto alla Pubblicazione
Firmato Digitalmente il 08/01/2026 17:29
Filomena BAVARO

OGGETTO:	Adozione della Politica di Gestione degli incidenti di Cybersicurezza in adempimento alla direttiva UE 2022/2555 così come recepita in Italia dal D.Lgs. n. 138/2024

IL DIRETTORE GENERALE

Vista la Deliberazione del Direttore Generale n. 329 del 17/02/2025, con l'assistenza del Segretario, sulla base della proposta formulata dalla U.O.S.V.D. Cybersicurezza che ne attesta la regolarità formale del procedimento ed il rispetto della legittimità, considera e determina quanto segue:

Premesso che:

- l'Azienda Sanitaria Locale di Bari rientra tra i soggetti obbligati di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90, ed è qualificabile come Soggetto Essenziale ai sensi della Direttiva (UE) 2022/2555 (Direttiva NIS 2), così come recepita nell'ordinamento nazionale dal D.Lgs. n. 138/2024;

- la Direttiva (UE) 2022/2555 e il D.Lgs. n. 138/2024 impongono ai soggetti essenziali l'adozione di misure organizzative, tecniche e procedurali finalizzate alla gestione dei rischi per la sicurezza informatica, inclusa la gestione e la notifica degli incidenti di cybersicurezza;

- l'art. 24 del D. Lgs. n. 138/2024 prevede l'obbligo, per i Soggetti interessati (tra i quali, l'A.S.L. Bari), di adottare misure per "gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26";

- la determinazione ACN n. 164179 del 14/04/2025, la quale all'art. 3, comma 2, fissa il termine per l'adempimento dell'obbligo di notifica degli incidenti significativi in nove mesi dall'inserimento nell'elenco dei soggetti NIS, rendendo necessaria l'adozione di una Procedura e delle connesse azioni sia organizzative che tecniche per la gestione dell'*incident reporting*, coincidente con la data del 31 dicembre 2025;

- al fine di assicurare il rispetto del quadro normativo vigente e di rafforzare la resilienza dell'Ente, si rende necessario adottare una Politica di Gestione degli Incidenti di Cybersicurezza, quale strumento organizzativo di riferimento per la prevenzione, la gestione e la comunicazione degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici.

Richiamati:

- il D.L. n. 82/2021, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), convertito con modificazioni dalla Legge nazionale del 4 agosto 2021, n. 109;

- la Direttiva UE n. 2022/2555 (Direttiva NIS 2) relativa alle misure per un livello comune elevato di cybersicurezza nell'Unione, che all'art. 21, lett. b), prevede un obbligo per i soggetti essenziali e importanti di adottare misure tecniche operative e organizzative adeguate e proporzionate per gestire gli incidenti di sicurezza e che all'art. 23 prevede gli obblighi in tema di segnalazione dei predetti incidenti;

- la Legge nazionale del 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici;

- il D.Lgs. n. 138/2024 avente ad oggetto: "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148";

Dato atto che, l'Azienda Sanitaria Locale rientra tra i soggetti obbligati agli adempimenti in materia di cybersicurezza ai sensi dell'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90 e, in quanto Soggetto Essenziale NIS, è soggetta alle previsioni di cui all'articolo 23 della Direttiva (UE) 2022/2555 e agli articoli 24 e 25 del D.Lgs. n. 138/2024, in materia di obblighi di gestione e notifica degli incidenti di cybersicurezza;

Rilevato che:

- La Direttiva (UE) 2022/2555 (NIS 2) e il D.Lgs. n. 138/2024 impongono ai soggetti obbligati l'adozione di misure organizzative e procedurali per la gestione degli incidenti di cybersicurezza, ivi incluse la rilevazione, la risposta, la notifica e il ripristino degli stessi;

- L'ASL rientra tra i soggetti essenziali di cui alla normativa vigente ed è pertanto tenuta a dotarsi di una politica formalizzata di gestione degli incidenti di cybersicurezza applicabile ai propri sistemi informativi e di rete;

- Risulta necessario definire ruoli, responsabilità e modalità operative per assicurare una gestione tempestiva ed efficace degli incidenti di cybersicurezza, nonché il rispetto degli obblighi di notifica previsti dalla normativa;

Ritenuto,

- Di dover adottare la "Politica_Gestione_Incidenti_ASL_Bari" di Cybersicurezza, allegata al presente provvedimento, per il rafforzamento della resilienza dell'Ente (ASL Bari) secondo la legge n. 90/2024, la Direttiva UE n. 2022/2555 (Direttiva NIS2) e per il D. Lgs. N. 138/2024;

- Di dover demandare alla U.O.S.V.D. Cybersicurezza la struttura competente per il coordinamento, l'attuazione e l'aggiornamento della suddetta Politica;

- Di dover dare atto che la Politica di Gestione degli Incidenti di Cybersicurezza si applica a tutti i sistemi informativi e di rete dell'Azienda;

Assunto il parere favorevole del Direttore Amministrativo e del Direttore Sanitario, reso ai sensi dell'art. 3, d. lgs. 502/1992

Tutto ciò premesso, perché costituisca parte integrante e sostanziale del presente provvedimento

DELIBERA

- DI ADOTTARE la "Politica_Gestione_Incidenti_ASL_Bari" di Cybersicurezza, allegata al presente provvedimento, per il rafforzamento della resilienza dell'Ente (ASL Bari) secondo la legge n. 90/2024, la Direttiva UE n. 2022/2555 (Direttiva NIS2) e per il D. Lgs. N. 138/2024;

- Di DEMANDARE alla U.O.S.V.D. Cybersicurezza la struttura competente per il coordinamento, l'attuazione e l'aggiornamento della suddetta Politica;

- Di DARE ATTO che la Politica di Gestione degli Incidenti di Cybersicurezza si applica a tutti i sistemi informativi e di rete dell'Azienda;

- DI TRASMETTERE il presente provvedimento alla UOC Analisi e Sviluppo del Sistema Informatico Aziendale, alla UOS Affari Generali e alla UOS Privacy;

- La pubblicazione del corrente provvedimento in Amministrazione Trasparente nella sottosezione di primo livello "Provvedimenti", sottosezione di secondo livello "Provvedimenti organi indirizzo politico", riferimento normativo art. 23, comma 1, D.Lgs n. 33/2013 e art. 1, comma 16 della L. n. 190/2012;

Tutti i firmatari del presente atto attestano di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, L. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/2013, ai sensi del vigente codice di comportamento aziendale e art. 1, c. 9, lett. e), L. 190/2012- quest'ultimo come recepito, a livello aziendale, dalla Sezione Anticorruzione e Trasparenza del vigente PIAO - tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35- bis, D. Lgs 165/2001.

Politica di Gestione degli Incidenti di Sicurezza Informatica

Azienda Sanitaria Locale della Provincia di Bari

Versione	1.0
Stato	Bozza
Classificazione	Uso Interno
Data di emissione	19/12/2025
Proprietario	U.O.S.V.D. Cybersicurezza
Approvato da	[Direzione Strategica Aziendale]
Atto	[Da definire]

Registro delle Revisioni

Versione	Data	Autore	Descrizione	Diffusione
1.0	19/12/2025	U.O.S.V.D. Cybersicurezza	Prima emissione	**TLP:CLEAR**

Indice

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

1. Introduzione e Obiettivi

La presente Politica definisce il quadro di riferimento per la gestione degli incidenti di sicurezza informatica dell'Azienda Sanitaria Locale della Provincia di Bari (ASL Bari).

L'ASL Bari, in qualità di **Soggetto Essenziale** ai sensi della Direttiva NIS2, adotta la presente Politica in conformità all'art. 24 del D.Lgs. 138/2024.

1.1 Obiettivi

- garantire una risposta tempestiva e proporzionata agli incidenti di sicurezza;
- minimizzare l'impatto sulla continuità dei servizi sanitari e sulla sicurezza dei dati;
- assicurare la conformità agli obblighi di notifica (ACN, CSIRT Italia, Garante Privacy);
- preservare le evidenze per analisi forensi e procedimenti legali;
- favorire il miglioramento continuo delle capacità di risposta.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

2. Ambito di Applicazione

2.1 Perimetro Organizzativo

La presente Politica si applica a:

- tutte le strutture organizzative dell'ASL Bari;
- tutto il personale dipendente;
- collaboratori esterni, consulenti, stagisti e tirocinanti;
- fornitori e partner che accedono ai sistemi informativi aziendali o trattano dati per conto dell'Azienda.

2.2 Perimetro Tecnologico

La Politica copre gli incidenti di sicurezza relativi a:

- sistemi informativi clinici e amministrativi;
- infrastrutture di rete (LAN, WAN, Wi-Fi, VPN);
- dispositivi medici connessi e sistemi IoT sanitari;
- postazioni di lavoro, dispositivi mobili e supporti rimovibili;
- servizi cloud e applicazioni SaaS;
- sistemi di posta elettronica e collaborazione.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

3. Riferimenti Normativi e Documentali

3.1 Riferimenti Normativi Primari

Riferimento	Descrizione
Direttiva (UE) 2022/2555	Direttiva NIS2 sulla sicurezza delle reti e dei sistemi informativi
Regolamento di esecuzione (UE) 2024/2690	Requisiti tecnici e metodologici delle misure di gestione dei rischi di cybersicurezza
D.Lgs. 138/2024	Recepimento della Direttiva NIS2 nell'ordinamento italiano
Legge n. 90/2024	Disposizioni in materia di rafforzamento della cybersicurezza nazionale
Regolamento (UE) 2016/679	Regolamento Generale sulla Protezione dei Dati (GDPR)

3.2 Determinazioni e Linee Guida ACN

Riferimento	Descrizione
Determinazione ACN n. 164179/2025	Categorie di incidenti significativi (IS-1/IS-2/IS-3/IS-4) e obblighi di notifica
TC-ACN	Tassonomia Cyber dell'Agenzia per la Cybersicurezza Nazionale - Framework per la categorizzazione degli eventi cyber
Documentazione ACN	Linee Guida, Circolari e Determinazioni emanate dall'Agenzia per la Cybersicurezza Nazionale

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

3.3 Standard e Framework di Riferimento

Riferimento	Descrizione
FNCDP 2025	Framework Nazionale per la Cybersicurezza e la Data Protection - Edizione 2025
ISO/IEC 27001:2022	Sistemi di gestione della sicurezza delle informazioni
ISO/IEC 27002:2022	Controlli per la sicurezza delle informazioni
ISO/IEC 27035-1/2/3	Gestione degli incidenti di sicurezza delle informazioni
NIST CSF 2.0	Cybersecurity Framework 2.0 - Funzioni Govern, Identify, Protect, Detect, Respond, Recover
NIST SP 800-61r3	Incident Response Recommendations and Considerations for Cybersecurity Risk Management (aprile 2025)
ENISA NIS2 Guidelines	Technical Guidance for the implementation of NIS2 - Incident Handling

3.4 Riferimenti per la Protezione dei Dati Personali

Riferimento	Descrizione
GPDP	Linee Guida, Provvedimenti e Pareri del Garante per la Protezione dei Dati Personali
EDPB	Linee Guida dell'European Data Protection Board

3.5 Documenti Aziendali Correlati

Documento	Relazione
Piano di Continuità Operativa (PCO)	Attivazione in caso di incidenti con impatto sulla continuità dei servizi

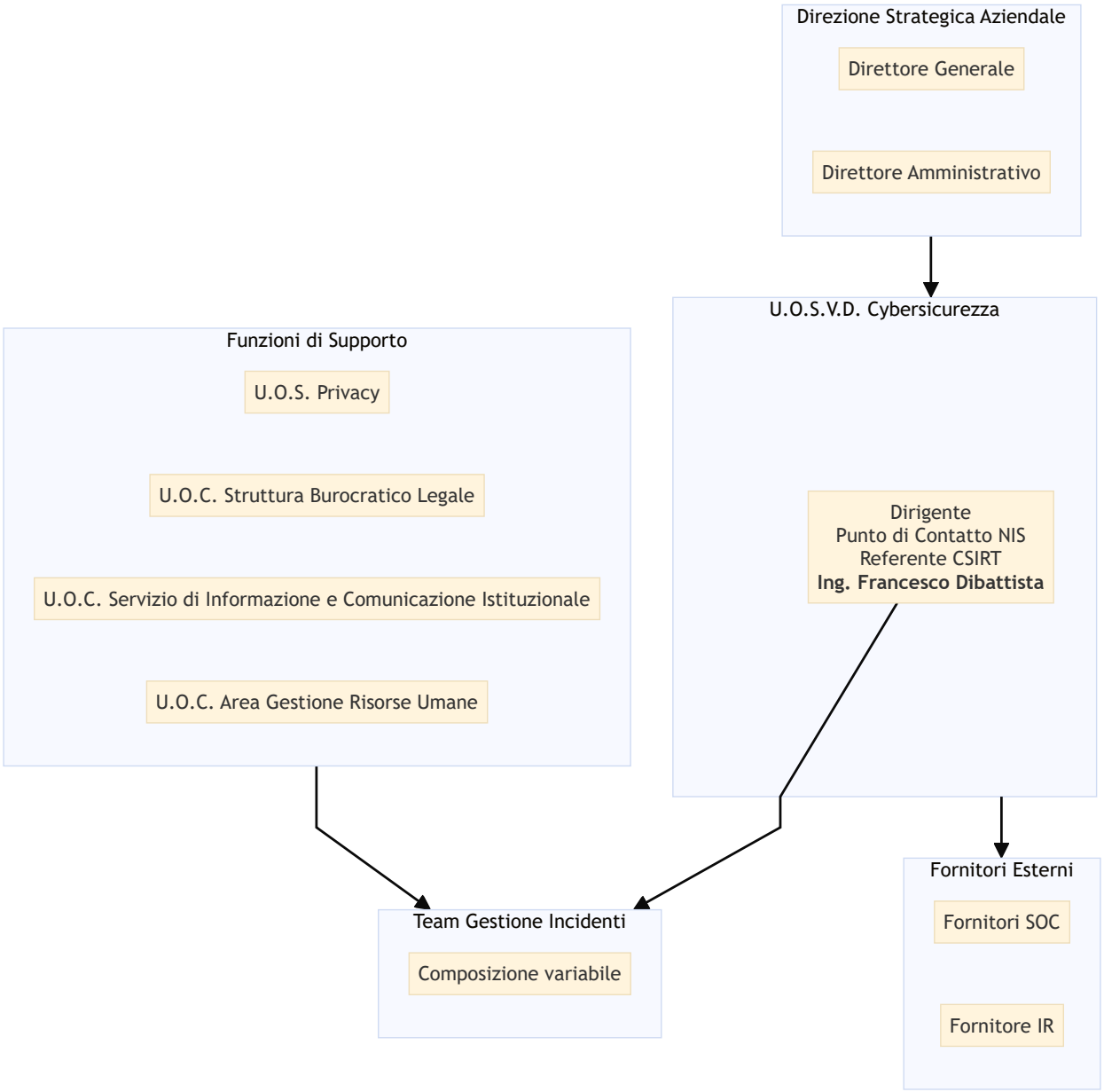
Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

Documento	Relazione
Piano di Disaster Recovery (DR)	Procedure di ripristino dei sistemi critici
Procedura di Gestione delle Violazioni dei Dati Personali (Data Breach)	Coordinamento per incidenti con impatto su dati personali
Procedura Operativa di Incident Response (Fornitore IR)	Dettaglio operativo delle attività di risposta - Allegato A
Registro dei Trattamenti	Identificazione dei dati personali coinvolti

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

4. Ruoli e Responsabilità

4.1 Struttura Organizzativa per la Gestione degli Incidenti



Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

4.2 Direzione Strategica Aziendale

La Direzione Strategica Aziendale (Direttore Generale e Direttore Amministrativo):

- approva la presente Politica e i suoi aggiornamenti;
- garantisce l'allocazione delle risorse necessarie per la gestione degli incidenti;
- è informata tempestivamente sugli incidenti significativi e costantemente aggiornata sull'andamento;
- assume le decisioni strategiche in caso di incidenti ad alto impatto;
- approva le comunicazioni esterne relative a incidenti gravi.

4.3 Responsabile per la Cybersicurezza

L'**Ing. Francesco Dibattista** ricopre i seguenti ruoli:

Dirigente U.O.S.V.D. Cybersicurezza:

- dirige l'unità organizzativa preposta alla sicurezza informatica.

Responsabile per la Cybersicurezza / Referente ex L. 90/2024:

- è il proprietario della presente Politica e ne cura l'aggiornamento;
- coordina le attività di gestione degli incidenti di sicurezza informatica;
- attiva e coordina il Team di Gestione Incidenti per eventi complessi;
- autorizza le azioni di contenimento ed eradicazione;
- valida la classificazione degli incidenti e le eventuali riclassificazioni;
- supervisiona le attività dei Fornitori SOC e del Fornitore IR;
- coordina le revisioni post-incidente e monitora l'implementazione delle azioni correttive;
- riferisce periodicamente alla Direzione sullo stato della sicurezza e sugli incidenti gestiti.

Punto di Contatto NIS:

- soggetto designato per le comunicazioni ufficiali con ACN;
- responsabile dell'invio delle notifiche obbligatorie tramite il portale ACN;
- interfaccia principale per le comunicazioni istituzionali in materia NIS2.

Referente CSIRT:

- responsabile delle interazioni tecniche con CSIRT Italia;
- coordina la trasmissione delle pre-notifiche, notifiche e relazioni;
- gestisce le eventuali richieste di informazioni aggiuntive da parte di CSIRT Italia.

È designato **Sostituto Punto di Contatto NIS** l'Ing. Marco Torres, che subentra in caso di assenza o impedimento del titolare.

4.4 U.O.S.V.D. Cybersicurezza

La U.O.S.V.D. Cybersicurezza:

- gestisce operativamente gli incidenti di sicurezza informatica;
- effettua il triage e la classificazione iniziale degli eventi segnalati;
- coordina le attività di analisi, contenimento, eradicazione e ripristino;
- mantiene i rapporti operativi con i Fornitori SOC e con il Fornitore IR;
- cura la documentazione degli incidenti e il registro degli incidenti;
- predispone le notifiche verso le Autorità competenti;
- organizza le esercitazioni periodiche e i programmi di formazione;
- effettua il monitoraggio degli indicatori di performance del processo;
- verifica se gli asset impattati trattano dati personali e attiva, se necessario, la procedura Data Breach.

4.5 Funzioni di Supporto

U.O.S. Privacy (DPO):

- è coinvolta tempestivamente in tutti gli incidenti che possano configurare una violazione di dati personali;
- valuta la necessità di notifica al Garante ai sensi degli artt. 33-34 del GDPR;
- supporta la valutazione dell'impatto sui diritti e le libertà degli interessati;
- coordina le eventuali comunicazioni agli interessati;
- mantiene il registro delle violazioni dei dati personali.

Ufficio Legale:

- fornisce supporto per gli aspetti legali e contrattuali correlati agli incidenti;
- supporta la valutazione di eventuali profili di responsabilità;
- collabora alla gestione di incidenti con implicazioni legali o giudiziarie.

Ufficio Comunicazione:

- gestisce le comunicazioni esterne relative agli incidenti, previa approvazione della Direzione;
- coordina le eventuali comunicazioni ai media;
- supporta la comunicazione verso pazienti e utenti.

Ufficio Risorse Umane:

- coordina le comunicazioni interne al personale riguardo all'incidente;
- fornisce supporto nella gestione di incidenti che coinvolgano comportamenti del personale;

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

- supporta eventuali procedimenti disciplinari correlati a incidenti di sicurezza;
- collabora alle attività di sensibilizzazione e formazione.

4.6 Team di Gestione Incidenti

Il Team di Gestione Incidenti è un gruppo multidisciplinare attivato per la gestione di incidenti complessi o ad alto impatto. La composizione è definita dal Responsabile per la Cybersicurezza in base alla natura dell'incidente e può includere:

- personale della U.O.S.V.D. Cybersicurezza (coordinamento);
- referenti dei sistemi informativi coinvolti;
- Asset Owner degli asset impattati;
- referenti delle aree cliniche o amministrative impattate;
- U.O.S. Privacy, Ufficio Legale, Ufficio Comunicazione, Ufficio Risorse Umane (in base alle necessità);
- personale del Fornitore IR;
- altri specialisti.

4.7 Responsabili delle Strutture Organizzative e Asset Owner

Responsabili delle Strutture Organizzative (Direttori di Dipartimento, Distretto, UOC/UOSD):

- promuovono la cultura della segnalazione degli eventi sospetti;
- garantiscono che il personale conosca le procedure di segnalazione;
- collaborano con la U.O.S.V.D. Cybersicurezza nella gestione degli incidenti;
- autorizzano, per quanto di competenza, le azioni di contenimento che impattano sull'operatività della struttura.

Asset Owner:

- forniscono informazioni sulla criticità e sul contesto operativo dell'asset;
- collaborano alla valutazione dell'impatto dell'incidente;
- autorizzano, per quanto di competenza, le azioni di contenimento sull'asset;
- supportano le attività di ripristino e verifica.

4.8 Tutto il Personale

Tutto il personale dell'ASL Bari:

- è tenuto a segnalare tempestivamente qualsiasi evento sospetto;

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

- deve seguire le istruzioni ricevute durante la gestione di un incidente;
- deve preservare le potenziali evidenze, evitando azioni che possano alterarle;
- deve partecipare alle attività formative sulla sicurezza informatica.

4.9 Fornitori Esterni

Fornitori SOC (es. hyperSOC Regione Puglia, clinicalSOC Regione Puglia, servizi MDR):

- effettuano il monitoraggio continuo degli eventi di sicurezza;
- eseguono la rilevazione e l'analisi iniziale delle minacce;
- escalano gli eventi rilevanti alla U.O.S.V.D. Cybersicurezza secondo le procedure concordate;
- supportano le attività di contenimento e risposta secondo gli SLA contrattuali.

Fornitore IR:

- fornisce supporto specialistico per la risposta agli incidenti complessi;
- esegue attività di analisi forense quando richiesto;
- supporta le attività di eradicazione e ripristino;
- opera secondo la Procedura Operativa di Incident Response (Allegato A).

5. Monitoraggio e Logging

5.1 Obiettivi

Le attività di monitoraggio e logging sono finalizzate a:

- rilevare tempestivamente eventi che possano costituire incidenti di sicurezza;
- supportare le attività di analisi, risposta e forensics;
- verificare la conformità alle politiche di sicurezza;
- identificare anomalie comportamentali e pattern sospetti.

5.2 Architettura

Il monitoraggio è realizzato attraverso:

- **fornitori SOC esterni**: monitoraggio continuo 24x7 con capacità di rilevazione e risposta gestita;
- **strumenti interni**: soluzioni di monitoraggio e logging integrate nell'infrastruttura aziendale.

L'architettura garantisce **continuità operativa e ridondanza**: i sistemi di raccolta e correlazione log sono configurati con adeguati livelli di ridondanza, i servizi SOC esterni costituiscono un livello indipendente, i log critici sono replicati su storage separato.

5.3 Perimetro del Logging

Sono soggetti a logging, in relazione alla criticità determinata dall'analisi dei rischi:

- traffico di rete in ingresso e in uscita;
- eventi di autenticazione e variazioni dei privilegi;
- creazione, modifica, eliminazione di utenze;
- attività degli account privilegiati e amministrativi;
- accessi e modifiche a configurazioni critiche;
- log degli strumenti di sicurezza (antivirus, EDR, firewall, IDS/IPS);
- accessi fisici alle aree tecnologiche;
- attivazione, arresto e modifica delle configurazioni di logging.

5.4 Requisiti Tecnici

Metadati dei log: timestamp sincronizzato (ISO-8601), identificativo univoco, sorgente, livello di severità, descrizione, utente ed esito (ove applicabili).

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

Sincronizzazione temporale: tutti i sistemi sono sincronizzati con sorgente temporale affidabile (NTP autenticato).

Soglie di allarme: sono definite soglie che generano notifiche automatiche (tentativi autenticazione falliti, escalation privilegi, volumi anomali traffico, rilevazione malware, accessi inusuali, modifiche configurazioni critiche). Le soglie sono oggetto di **ottimizzazione continua** per minimizzare falsi positivi e falsi negativi.

5.5 Conservazione e Protezione

I log sono conservati secondo i requisiti normativi applicabili e le esigenze di analisi incidenti.

La protezione è garantita attraverso: controllo accessi basato su ruoli, memorizzazione su sistemi dedicati, meccanismi di protezione dell'integrità, backup su storage separato.

5.6 Revisione

Le procedure di monitoraggio e logging e l'elenco degli asset soggetti a logging sono rivisti almeno annualmente, a seguito di incidenti significativi o di cambiamenti rilevanti nell'infrastruttura.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

6. Segnalazione degli Eventi

6.1 Obbligo di Segnalazione

Tutto il personale dell'ASL Bari è tenuto a segnalare tempestivamente qualsiasi evento sospetto che possa indicare un incidente di sicurezza, inclusi:

- comportamenti anomali dei sistemi (rallentamenti, blocchi, messaggi inusuali);
- e-mail sospette (phishing, allegati inattesi, richieste anomale);
- accessi o attività non autorizzate;
- perdita o furto di dispositivi o credenziali;
- richieste sospette di informazioni;
- qualsiasi altra situazione che appaia anomala rispetto al normale funzionamento.

La segnalazione deve avvenire **indipendentemente dalla certezza** che si tratti di un incidente: il triage sarà effettuato dal personale competente.

6.2 Canali di Segnalazione

Sono disponibili i seguenti canali per la segnalazione degli eventi:

Canale	Modalità	Disponibilità
E-mail dedicata	sicurezza.informatica@asl.bari.it	24x7 (lettura in orario lavorativo)
Telefono	080 5842 218	Orario lavorativo
Modulo di segnalazione	Allegato B - Modulo di segnalazione incidenti	Sempre disponibile
Numero di emergenza	347 0849 354	24x7 (in casi critici e per impossibilità di utilizzo degli altri canali)

Per eventi critici o in orari extra-lavorativi, sono attivi i Fornitori SOC che garantiscono la rilevazione automatica e l'escalation verso i referenti aziendali secondo le procedure concordate.

6.3 Contenuto della Segnalazione

La segnalazione deve contenere, ove possibile:

- data e ora dell'evento;

- descrizione dell'avvenimento;
- asset aziendali colpiti;
- tipologia di informazioni aziendali impattate;
- eventuali persone/enti coinvolti;
- eventuali screenshot, messaggi di errore o altre evidenze;
- azioni già intraprese;
- dati di contatto del segnalante per eventuali approfondimenti.

Il **Modulo di segnalazione incidenti** (Allegato B) fornisce un formato standardizzato per la raccolta delle informazioni.

6.4 Segnalazioni da Fornitori e Soggetti Esterni

I fornitori e i soggetti esterni che abbiano accesso ai sistemi aziendali o che trattino dati per conto dell'Azienda sono tenuti a segnalare tempestivamente eventuali eventi di sicurezza attraverso i canali concordati contrattualmente.

I contratti con i fornitori devono prevedere:

- l'obbligo di segnalazione tempestiva degli incidenti;
- i canali e i tempi di comunicazione;
- gli obblighi di collaborazione nella gestione degli incidenti.

6.5 Formazione sulla Segnalazione

Il personale è formato periodicamente su:

- cosa costituisce un evento sospetto;
- come effettuare una segnalazione efficace;
- l'importanza della tempestività nella segnalazione;
- i canali disponibili.

La U.O.S.V.D. Cybersicurezza, in collaborazione con l'U.O.S. Formazione, organizza sessioni di sensibilizzazione e campagne informative periodiche.

6.6 Non Ritorsione

L'ASL Bari garantisce che non saranno adottati provvedimenti negativi nei confronti di chi segnala in buona fede eventi sospetti, anche qualora la segnalazione risulti un falso allarme.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

7. Valutazione e Classificazione degli Incidenti

7.1 Principi

La valutazione e classificazione degli incidenti dell'ASL Bari è basata su:

- **Tassonomia Cyber ACN (TC-ACN)**: framework nazionale per la categorizzazione degli eventi cyber;
- **Determinazione ACN n. 164179/2025**: categorie di incidenti significativi (IS-1/IS-2/IS-3/IS-4) e obblighi di notifica;
- **D.Lgs. 138/2024** (art. 25, comma 4): criteri generali di significatività.

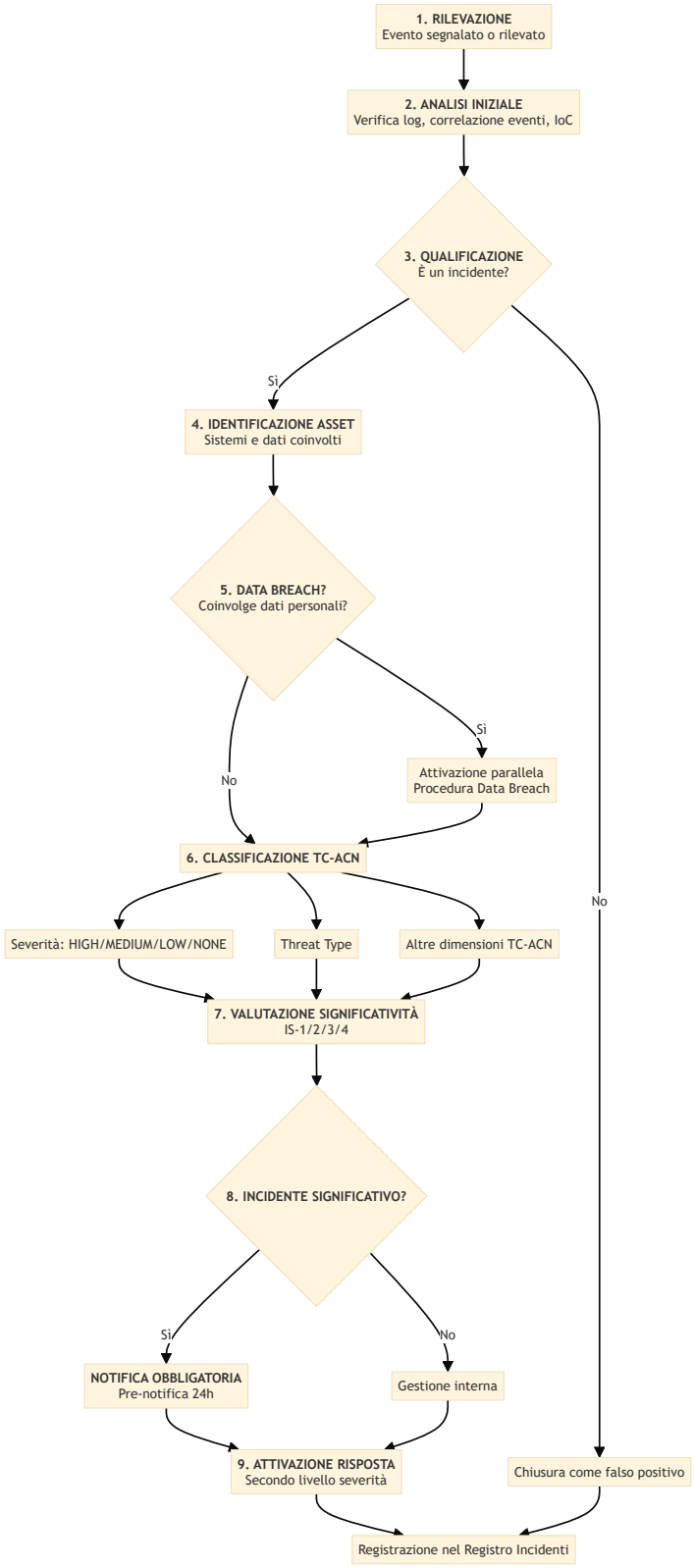
Ogni incidente confermato è soggetto a **doppia classificazione parallela e indipendente**:

Classificazione	Scopo	Framework
Severità	Priorità di risposta e allocazione risorse	TC-ACN (HIGH/MEDIUM/LOW/NONE)
Significatività	Obblighi di notifica alle Autorità	Determinazione ACN (IS-1/IS-2/IS-3/IS-4) + D.Lgs. 138/2024 art. 25 c.4

7.2 Processo di Triage

Il triage è effettuato dalla U.O.S.V.D. Cybersicurezza, con supporto dei Fornitori SOC per gli eventi rilevati automaticamente.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it



Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

7.3 Framework TC-ACN

La TC-ACN è il framework nazionale per la categorizzazione degli eventi cyber, strutturato in quattro macro-categorie:

Macro-categoria	Codice	Contenuto
Baseline Characterization	BC	Impact, Root Cause, Severity, Victim Geography
Threat Type	TT	Tipologie di minaccia (Malicious Code, Social Engineering, Availability, Data Exposure, Vulnerability, ecc.)
Threat Actor	TA	Adversary Type e Motivation
Additional Context	AC	Vector, Involved Asset, Physical Security, ecc.

La TC-ACN completa è disponibile sul sito web dell'Agenzia per la Cybersicurezza Nazionale (https://www.acn.gov.it).

7.4 Livelli di Severità TC-ACN

Severità	Definizione TC-ACN	Tempo Risposta	Escalation
HIGH	L'organizzazione non è più in grado di fornire servizi essenziali; oppure dati sono stati modificati, cancellati o esfiltrati; oppure il recupero non è possibile	≤ 30 min	Direzione + Team Incidenti + Fornitore IR
MEDIUM	L'organizzazione può fornire servizi essenziali solo parzialmente; oppure è stato rilevato accesso ed esfiltrazione di dati; oppure il recupero è possibile ma i tempi sono incerti	≤ 2 ore	Resp. Cybersicurezza

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

Severità	Definizione TC-ACN	Tempo Risposta	Escalation
LOW	L'organizzazione può fornire servizi essenziali ma con efficienza ridotta; oppure è stato rilevato accesso a dati sensibili; oppure il recupero è possibile in tempi noti	≤ 4 ore	U.O.S.V.D. Cybersicurezza
NONE	Nessun effetto sulla capacità di fornire servizi; oppure nessun dato è stato soggetto ad accesso non autorizzato; oppure il recupero è prevedibile con risorse esistenti	≤ 8 ore	U.O.S.V.D. Cybersicurezza

7.5 Significatività NIS2 e Obblighi di Notifica

Categorie di Incidenti Significativi (Determinazione ACN n. 164179/2025)

Un incidente è **significativo** se rientra in almeno una delle seguenti categorie:

Categoria	Criterio	Verifica
IS-1	Perdita di **riservatezza** verso l'esterno di dati digitali	Dati divulgati o accessibili a soggetti esterni non autorizzati?
IS-2	Perdita di **integrità** con impatto verso l'esterno di dati digitali	Dati alterati con conseguenze su soggetti esterni?
IS-3	Violazione dei **livelli di servizio attesi**	SLA violati rispetto ai parametri definiti (DE.CM-01)?
IS-4	**Accesso non autorizzato** o abuso di privilegi a dati digitali	Accesso illegittimo rilevato, anche interno?

Criteri Generali di Significatività (D.Lgs. 138/2024 art. 25, comma 4)

Indipendentemente dalle categorie IS, un incidente è significativo se:

a) ha causato o è in grado di causare una **grave perturbazione operativa dei servizi** o **perdite finanziarie** per il soggetto interessato;

b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su **altre persone fisiche o giuridiche** causando **perdite materiali o immateriali considerevoli**.

Se l'incidente è significativo (categoria IS o criteri art. 25 c.4): **pre-notifica CSIRT ≤24h, notifica ≤72h, relazione finale ≤1 mese**.

7.6 Registrazione

Tutti gli eventi sono registrati nel **Registro degli Incidenti** (Allegato B):

Campo	Descrizione
ID	Identificativo univoco
Data/ora rilevazione	Timestamp della prima rilevazione
Data/ora segnalazione	Timestamp della segnalazione (se diversa)
Fonte	Fornitori SOC / Segnalazione utente / Altro
Esito triage	Incidente / Falso positivo / Evento non di sicurezza
Classificazione TC-ACN	Severity, Threat Type, Impact, Root Cause, Vector
Significatività	IS-1/2/3/4 o Non significativo
Asset coinvolti	Elenco sistemi/dati impattati
Data breach	Sì/No
Stato	Aperto / In gestione / Chiuso
Riferimento fascicolo	Link al fascicolo incidente

Incidenti Ricorrenti

Su base trimestrale, la U.O.S.V.D. Cybersicurezza analizza il registro per identificare pattern ricorrenti e possibili incidenti significativi derivanti dall'aggregazione di eventi minori.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

8. Risposta agli Incidenti

8.1 Modello di Riferimento

Il ciclo di vita della gestione degli incidenti è allineato al **NIST Cybersecurity Framework 2.0** (SP 800-61r3) e alle linee guida **ENISA** per l'implementazione della NIS2:

Fase	Funzione CSF 2.0	Riferimento ENISA	Sezione Politica
Preparazione	Govern, Identify, Protect	3.1, 3.2	Sez. 4-6
Rilevazione e Analisi	**Detect**	3.3, 3.4	Sez. 7
Contenimento	**Respond**	3.5.2(a)	Sez. 8.3
Eradicazione	**Respond**	3.5.2(b)	Sez. 8.4
Ripristino	**Recover**	3.5.2(c)	Sez. 8.5
Post-incidente	Identify (Improvement)	3.6	Sez. 10

Le attività operative di dettaglio sono descritte nella **Procedura Operativa di Incident Response** (Allegato A), comprensiva dei playbook per tipologia di incidente.

8.2 Attivazione della procedura di risposta

La risposta è attivata secondo i tempi definiti per ciascun livello di severità (sezione 7.4):

- assegnazione di un incident handler;
- apertura del fascicolo dell'incidente;
- attivazione delle escalation previste;
- comunicazione alla Direzione.

Per incidenti HIGH o MEDIUM, il Responsabile per la Cybersicurezza valuta l'attivazione del Team di Gestione Incidenti e il coinvolgimento del Fornitore IR.

8.3 Contenimento

Obiettivo: prevenire l'espansione dell'incidente e limitarne l'impatto.

Preservazione evidenze (prima del contenimento): acquisire e preservare log, artefatti malevoli, IoC. Per ogni evidenza documentare: data/ora, fonte, operatore, hash SHA-256. Garantire la catena di custodia.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

Azioni di contenimento: isolamento sistemi compromessi, blocco account/traffico malevolo, disabilitazione servizi compromessi. Le azioni sono autorizzate dal Responsabile per la Cybersicurezza.

8.4 Eradicazione

Obiettivo: eliminare le cause dell'incidente e le componenti malevole dall'ambiente.

Azioni di eradicazione: rimozione malware, chiusura vulnerabilità sfruttate, rimozione accessi non autorizzati, reset credenziali compromesse, eliminazione meccanismi di persistenza.

8.5 Ripristino

Obiettivo: ripristinare i sistemi alle normali operazioni in modo sicuro.

Azioni di ripristino: ripristino da backup verificati (previa verifica integrità), riconfigurazione sistemi, verifica funzionamento, riattivazione graduale servizi, monitoraggio intensivo post-ripristino.

Per incidenti che lo richiedano, coordinamento con il Piano di Disaster Recovery.

Verifica efficacia: test delle azioni di remediation prima del ripristino completo. Se negativi, iterare contenimento/eradicazione.

8.6 Gestione dei Conflitti e Documentazione

Conflitti tra obiettivi: in caso di conflitto tra attività forensi, risposta e continuità operativa, il Responsabile per la Cybersicurezza definisce le priorità considerando rischio residuo, impatto su servizi essenziali e obblighi normativi.

Documentazione: per ogni incidente mantenere cronologia eventi, azioni intraprese, decisioni e motivazioni, comunicazioni, evidenze, IoC, tempi, impatto, root cause analysis e raccomandazioni.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

9. Comunicazione e Notifiche Obbligatorie

9.1 Principi della Comunicazione

La comunicazione relativa agli incidenti di sicurezza è governata dai seguenti principi:

- **tempestività**: le comunicazioni devono avvenire nei tempi previsti dagli obblighi normativi e dalle esigenze operative;
- **accuratezza**: le informazioni comunicate devono essere verificate e aggiornate;
- **coerenza**: i messaggi devono essere coerenti tra i diversi canali e destinatari;
- **appropriatezza**: il livello di dettaglio è calibrato in base al destinatario;
- **riservatezza**: le informazioni sensibili sono condivise solo con soggetti autorizzati.

9.2 Comunicazione Interna

9.2.1 Escalation verso la Direzione

La Direzione Strategica Aziendale è informata:

- **immediatamente**: per incidenti di severità HIGH;
- **entro 4 ore**: per incidenti di severità MEDIUM;
- **attraverso reporting periodico**: per incidenti di severità LOW e NONE.

La U.O.S.V.D. Cybersicurezza garantisce un **flusso costante di aggiornamento e informazione** alla Direzione durante tutta la gestione dell'incidente.

9.2.2 Comunicazione alle Strutture Impattate

I Responsabili delle strutture organizzative impattate da un incidente sono informati tempestivamente dal Responsabile per la Cybersicurezza o dalla U.O.S.V.D. Cybersicurezza riguardo a:

- natura dell'incidente (nei limiti della riservatezza);
- impatti previsti o in corso;
- azioni richieste al personale;
- tempistiche previste per il ripristino.

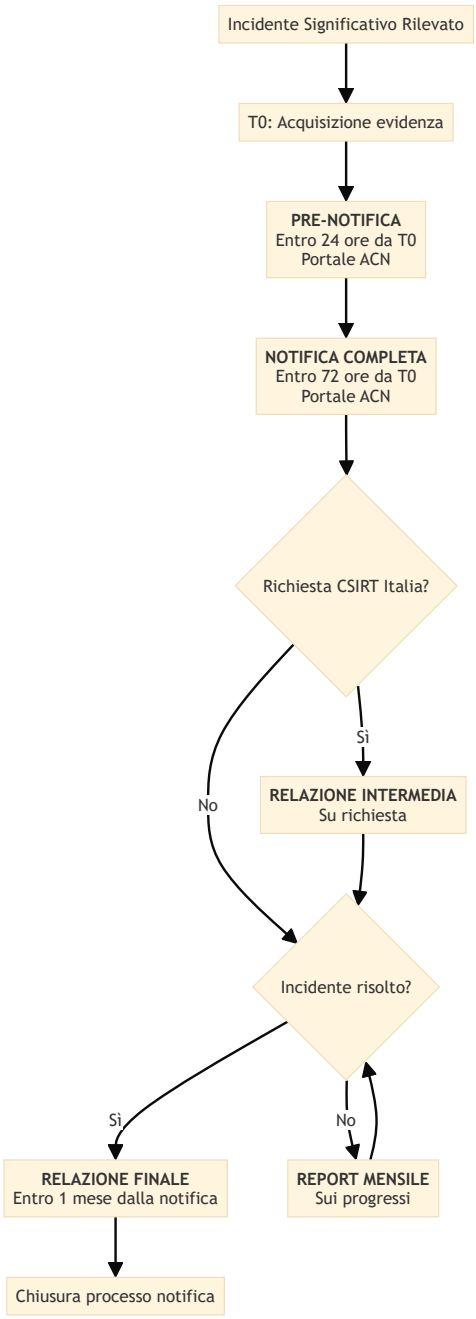
9.2.3 Comunicazione al Personale

In caso di incidenti che richiedano azioni da parte del personale (es. cambio password, verifica dei sistemi), la comunicazione avviene attraverso i canali aziendali (e-mail, intranet) con messaggi validati dalla U.O.S.V.D. Cybersicurezza.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

9.3 Notifiche Obbligatorie

9.3.1 Flusso delle Notifiche



Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

9.3.2 Dettaglio delle Notifiche

Per gli incidenti significativi ai sensi dell'art. 25 del D.Lgs. 138/2024, il **Referente CSIRT** (Ing. Francesco Dibattista) effettua le seguenti notifiche tramite il **Portale Segnalazioni ACN** (https://segnalazioni.acn.gov.it/):

Tipo	Tempistica	Contenuto
Pre-notifica	Entro **24 ore** dalla conoscenza dell'incidente significativo	Informazioni minime sull'accaduto e sistemi coinvolti. Indicazione, ove possibile, se l'incidente possa ritenersi risultato di atti illegittimi o malevoli o possa avere impatto transfrontaliero.
Notifica dell'incidente	Entro **72 ore** dalla conoscenza dell'incidente significativo	Aggiornamento informazioni pre-notifica; valutazione iniziale comprensiva di gravità e impatto; data/ora rilevamento; asset impattati; vettori d'attacco; misure di rientro intraprese e pianificate; IoC; evidenze rilevanti (es. sample malware, ransom note)
Relazione intermedia	Su richiesta di CSIRT Italia	Aggiornamenti pertinenti sulla situazione
Relazione finale	Entro **1 mese** dalla notifica	Descrizione dettagliata dell'incidente (gravità e impatto); tipo di minaccia o root cause; misure di attenuazione adottate e in corso; impatto transfrontaliero (ove noto)
Report mensile	Mensile (se incidente ancora in corso)	Progressi nella gestione, fino a relazione finale entro 1 mese dalla risoluzione

9.3.3 Decorrenza dei Termini

I termini per le notifiche decorrono dal momento in cui l'ASL Bari **viene a conoscenza** dell'incidente significativo, inteso come il momento in cui si dispone di **elementi oggettivi** dai quali si evince che si è verificato un incidente di sicurezza informatica significativo.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

9.4 Notifica al Garante Privacy (GDPR)

In caso di violazione di dati personali (Data Breach), la **U.O.S. Privacy**, nella persona del DPO, in coordinamento con la U.O.S.V.D. Cybersicurezza, valuta la necessità di notifica secondo la **Procedura di Gestione delle Violazioni dei Dati Personali**:

Tipo	Tempistica	Condizione
Notifica al Garante	Entro **72 ore** dalla conoscenza della violazione	Violazione che presenta un rischio per i diritti e le libertà delle persone fisiche
Comunicazione agli interessati	Senza ingiustificato ritardo	Violazione che presenta un rischio elevato per i diritti e le libertà delle persone fisiche

9.5 Riepilogo Obblighi di Notifica

Autorità	Riferimento Normativo	Tempistica	Responsabile
CSIRT Italia (Pre-notifica)	Art. 25, c.5, lett. a) D.Lgs. 138/2024	24 ore	Referente CSIRT
CSIRT Italia (Notifica)	Art. 25, c.5, lett. b) D.Lgs. 138/2024	72 ore	Referente CSIRT
CSIRT Italia (Relazione finale)	Art. 25, c.5, lett. d) D.Lgs. 138/2024	1 mese	Referente CSIRT
Garante Privacy	Artt. 33-34 GDPR	72 ore	DPO

9.6 Comunicazione Esterna - Altri Stakeholder

9.6.1 Comunicazione a Pazienti e Utenti

In caso di incidenti che impattino sui servizi al pubblico o che richiedano comunicazione agli interessati ai sensi del GDPR, la comunicazione è coordinata dall'Ufficio Comunicazione in raccordo con:

- U.O.S.V.D. Cybersicurezza (contenuti tecnici);
- U.O.S. Privacy (aspetti relativi alla protezione dati);
- Direzione Strategica (approvazione).

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

Ai sensi dell'art. 25, comma 2, D.Lgs. 138/2024, l'ASL Bari notifica senza indebito ritardo ai **destinatari dei propri servizi** gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.

9.6.2 Comunicazione ai Fornitori

I fornitori coinvolti in un incidente sono informati nei limiti necessari per la gestione dell'incidente stesso. In particolare:

- i Fornitori SOC e il Fornitore IR ricevono le informazioni necessarie per supportare la risposta;
- i fornitori i cui sistemi o servizi sono coinvolti nell'incidente sono informati secondo le procedure contrattuali.

9.6.3 Comunicazione ai Media

Eventuali comunicazioni ai media sono gestite esclusivamente dall'Ufficio Comunicazione, previa approvazione della Direzione Strategica Aziendale, su contenuti concordati con la U.O.S.V.D. Cybersicurezza.

9.7 Contatti di Emergenza

La U.O.S.V.D. Cybersicurezza mantiene aggiornato l'**Elenco dei Contatti** (Allegato C - documento riservato), includente:

- referenti interni per ruolo e struttura;
- contatti CSIRT Italia;
- contatti Garante Privacy;
- contatti dei fornitori critici (Fornitori SOC, Fornitore IR, altri);
- contatti di fornitori di servizi essenziali.

L'elenco è verificato e aggiornato almeno trimestralmente.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

10. Revisione Post-Incidente

10.1 Obiettivi e Applicabilità

La revisione post-incidente ha l'obiettivo di identificare le cause profonde (root cause analysis), valutare l'efficacia della risposta, documentare le lezioni apprese e definire azioni correttive.

Applicabilità:

- tutti gli incidenti HIGH e MEDIUM;
- incidenti LOW con caratteristiche significative o ricorrenti;
- su richiesta del Responsabile per la Cybersicurezza o della Direzione.

Tempistiche: entro 5 giorni lavorativi dalla conclusione del ripristino (HIGH), 10 giorni (MEDIUM), 20 giorni (altri).

10.2 Svolgimento

La revisione è condotta dalla U.O.S.V.D. Cybersicurezza con il coinvolgimento del personale che ha gestito l'incidente, i responsabili delle strutture impattate, la U.O.S. Privacy, il Fornitore IR e gli altri stakeholder rilevanti.

Elementi analizzati: cronologia, efficacia della rilevazione/contenimento/eradicazione/ripristino, adeguatezza delle comunicazioni, root cause, fattori contribuenti, vulnerabilità emerse, punti di forza e aree di miglioramento.

10.3 Report e Azioni Correttive

La revisione produce un report contenente: descrizione e cronologia, impatto effettivo, root cause analysis, valutazione della risposta, lezioni apprese, raccomandazioni, piano di azione con responsabili e tempistiche.

Le raccomandazioni si traducono in azioni correttive riguardanti misure tecniche, procedure, formazione, valutazione rischi o politiche. La U.O.S.V.D. Cybersicurezza traccia l'implementazione e ne verifica l'efficacia.

10.4 Miglioramento Continuo

Le lezioni apprese sono condivise, nei limiti della riservatezza, con il personale interno, i fornitori e altre entità del settore sanitario.

I risultati delle revisioni alimentano il processo di valutazione dei rischi, verificando se il rischio era stato correttamente identificato, se le misure erano adeguate e se sono necessari aggiornamenti.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

11. Test, Revisione e Aggiornamento

11.1 Test delle Procedure

Le procedure di gestione degli incidenti sono testate **almeno annualmente** attraverso:

- esercitazioni tabletop (simulazioni discusse);
- simulazioni operative (attivazione effettiva dei processi);
- red team/blue team;
- walkthrough di incidenti passati.

I test coinvolgono scenari diversificati (ransomware, data breach, DoS, phishing) e includono la Direzione per verificare la comprensione dei ruoli. Possono coinvolgere fornitori e stakeholder esterni.

I risultati sono documentati (scenario, partecipanti, osservazioni, azioni correttive) e le azioni sono tracciate fino all'implementazione.

11.2 Revisione della Politica

La presente Politica è sottoposta a revisione:

- almeno annualmente;
- a seguito di incidenti significativi;
- a seguito di cambiamenti nel contesto organizzativo, tecnologico o normativo.

La revisione considera: risultati dei test, lezioni apprese, evoluzione delle minacce, evoluzioni normative (incluse nuove Determinazioni ACN), modifiche organizzative e infrastrutturali, aggiornamenti agli standard.

Le modifiche significative sono comunicate al personale interessato attraverso i canali aziendali.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

12. Glossario

12.1 Definizioni

Termine	Definizione
Evento di sicurezza	Occorrenza identificata che indica una possibile violazione della politica di sicurezza o un fallimento delle misure di protezione.
Incidente di sicurezza	Evento o serie di eventi che hanno probabilità significativa di compromettere le operazioni aziendali e minacciare la sicurezza delle informazioni.
Incidente significativo	Ai sensi dell'art. 25 c.4 D.Lgs. 138/2024: incidente che causa o può causare grave perturbazione operativa o perdite finanziarie, o che ha ripercussioni su terzi causando perdite considerevoli.
Data Breach	Violazione di sicurezza che comporta distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali.
IoC	Indicatori di Compromissione: artefatti tecnici che indicano una potenziale intrusione.
Triage	Processo di valutazione iniziale per determinare la priorità di gestione di un evento.
RCA	Root Cause Analysis: metodologia per identificare le cause profonde di un incidente.
Pre-notifica	Prima comunicazione al CSIRT Italia entro 24 ore dalla conoscenza di un incidente significativo.
Notifica	Comunicazione completa al CSIRT Italia entro 72 ore.
Relazione finale	Report conclusivo da trasmettere entro 1 mese dalla notifica.
Fornitori SOC	Fornitori di servizi SOC (es. hyperSOC Regione Puglia, clinicalSOC Regione Puglia, servizi MDR).
Fornitore IR	Fornitore del servizio di Incident Response.

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

12.2 Acronimi

Acronimo	Significato
ACN	Agenzia per la Cybersicurezza Nazionale
CSF	NIST Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
DPO	Data Protection Officer
GDPR	General Data Protection Regulation (Regolamento UE 2016/679)
NIS2	Network and Information Security Directive 2
PCO	Piano di Continuità Operativa
SLA	Service Level Agreement
SOC	Security Operations Center
TC-ACN	Tassonomia Cyber ACN

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

13. Allegati

Codice	Titolo	Descrizione
Allegato A	Procedura Operativa di Incident Response	Procedura operativa fornita dal Fornitore IR con dettaglio delle attività tecniche di risposta, comprensiva dei playbook specifici per tipologia di incidente
Allegato B	Moduli e Registro	Modulo di segnalazione incidenti - Registro degli Incidenti
Allegato C	Elenco Contatti	Contatti interni ed esterni per la gestione degli incidenti (documento riservato)

Azienda Sanitaria Locale della Provincia di Bari
Lungomare Starita, 6 – 70123 BARI (BA)
Codice Fiscale/Partita IVA 06534340721
E-Mail: sicurezza.informatica@asl.bari.it - PEC: cybersicurezza.aslbari@pec.rupar.puglia.it

PROFILI CONTABILI

☐ RILEVANTE, a valere su: ☒ NON rilevante

ONERI DI PUBBLICAZIONE OBBLIGATORIA EX D. LGS. 33/2013:

☒ SOGGETTA a pubblicazione ☐ NON soggetta a pubblicazione

Sottosezione di Primo LIvello	Sottosezione di Secondo LIvello	Riferimento Normativo
Provvedimenti	Provvedimenti organi indirizzo politico	Art. 23, c. 1, d.lgs. n. 33/2013 /Art. 1, co. 16 della l. n. 190/2012

ONERI DI RISERVATEZZA:

☐ CONTIENE dati personali da NON pubblicare ☒ NON contiene dati personali

DESTINATARI NOTIFICA/TRASMISSIONE

Sistemi Informativi	U.R.P. e UOS Privacy
Affari Generali	

PROPOSTA N.RO 20250003049 APPROVATA CON DELIBERAZIONE N.RO 20260000001 DEL 08/01/2026

Con la sottoscrizione in calce al presente provvedimento, i firmatari di cui sopra, ciascuno in relazione al proprio ruolo come indicato e per quanto di rispettiva competenza, attestano che il procedimento istruttorio è stato espletato nel rispetto della normativa regionale e nazionale applicabile e che il provvedimento predisposto è conforme alle risultanze istruttorie agli atti d'ufficio.

I medesimi soggetti dichiarano, inoltre, di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, l. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/2013, vigente codice di comportamento aziendale e art. 1, c. 9, lett. e), l. 190/2012 – quest'ultimo come recepito, a livello aziendale, della vigente sezione Anticorruzione e Trasparenza del PIAO – tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, D.L.gs. 165/2001.

RUOLO	NOME E COGNOME	FIRMA
Direttore/Responsabile di Struttura	Dibattista Francesco	*Firmato digitalmente il 31/12/2025 13:08*