



DELIBERAZIONE DEL DIRETTORE GENERALE n. 704 del 23 DIC. 2025

OGGETTO: istituzione del Comitato di Cybersecurity e presa d'atto dell'adozione del piano di gestione degli incidenti di sicurezza informatica

DELIBERAZIONE ADOTTATA DAL DIRETTORE GENERALE DOTT.SSA PAOLA LATTUADA

SU PROPOSTA DEL DIRETTORE DELL'UOC SISTEMI INFORMATIVI AZIENDALI

accertata la competenza procedurale, sottopone in data 23 DIC. 2025 allegata proposta di deliberazione sull'argomento all'oggetto specificato, la cui spesa rientra nel budget assegnato.

Il Responsabile del Procedimento
Direttore UOC Sistemi Informativi Aziendali
Ing. Ponziano A. Ricciardelli

ATTESTAZIONE COPERTURA ECONOMICA

Si attesta la regolarità contabile, la copertura economica e l'imputazione a bilancio degli oneri derivanti dal presente provvedimento con annotazione:

- Il presente provvedimento non comporta oneri diretti a carico del bilancio aziendale

Il Direttore UOC Bilancio, Programmazione finanziaria e Contabilità
Dott.ssa Emilia Martignoni



DELIBERAZIONE DEL DIRETTORE GENERALE n. 704 del 23 DIC. 2025

IL DIRETTORE GENERALE

Viste:

- la DGR n. X/4475 del 10/12/2015 di costituzione, a partire dal 01/01/2016, dell'Azienda Socio Sanitaria Territoriale (ASST) Centro Specialistico Ortopedico Traumatologico Gaetano Pini/CTO;
- la DGR XII/2158 del 15/04/2024 di nomina della Dott.ssa Paola Lattuada quale Direttore Generale dell'Azienda Socio Sanitaria Territoriale (ASST) Gaetano Pini-CTO per il periodo 19/04/2024 - 18/04/2027;
- la deliberazione aziendale n. 198 del 18/04/2024 di presa d'atto della predetta DGR XII/2158/2024 e di insediamento dal 19/04/2024 sino al 18/04/2027 della Dott.ssa Paola Lattuada quale Direttore Generale dell'ASST G. Pini-CTO;

Premesso che:

- la Direttiva (UE) 2022/2555 – NIS2 stabilisce misure per un elevato livello comune di cybersecurity nell'Unione Europea e come primo adempimento da ottemperare entro il 31/12/2025, l'adozione di un Piano di Gestione degli Incidenti di Sicurezza;
- l'Italia ha recepito la direttiva mediante d.lgs. 4 settembre 2024, n. 138 recante il "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*", che recependo la direttiva NIS 2, completa il percorso di adeguamento dell'ordinamento interno alla normativa euro-unitaria già avviato a far data dal 2016, introducendo misure volte a "*garantire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea in modo da migliorare il funzionamento del mercato interno*";
- la Legge del 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", rafforza gli obblighi in materia di sicurezza cibernetica per le infrastrutture critiche e i soggetti essenziali, tra cui le strutture sanitarie;
- la Legge del 28 giugno 2024, n. 90 all'articolo 8 "Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza" prevede l'istituzione da parte dei soggetti di cui all'articolo 1, comma 1 della legge medesima, incluse "*Le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196 [...]*" di una struttura per lo sviluppo delle politiche e delle procedure di sicurezza che provveda:
 - a) allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;
 - b) alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;
 - c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;
 - d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;
 - e) alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d);
 - f) alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;
 - g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza;



DELIBERAZIONE DEL DIRETTORE GENERALE n. 704 del 23 DIC. 2025

- le ASST, quali soggetti essenziali, sono tenute a dotarsi di governance interna, procedure strutturate di gestione degli incidenti di sicurezza e adeguati presidi organizzativi e tecnici;

Considerato che:

- l'elevato rischio cyber per le infrastrutture sanitarie richiede una gestione multidisciplinare e continuativa;
- il coordinamento tra le funzioni tecniche, cliniche, amministrative e legali è indispensabile per garantire una risposta efficace agli incidenti di sicurezza;
- ASST Centro Specialistico Ortopedico Traumatologico Gaetano Pini-CTO, in qualità di Soggetto essenziale deve definire, attuare, aggiornare e documentare un piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, che comprenda almeno:
 - le fasi e le procedure di gestione e notifica degli incidenti con l'indicazione dei relativi ruoli e responsabilità;
 - le procedure per la predisposizione e la trasmissione delle relazioni di cui all'articolo 25, comma 5, lettere c), d) ed e) del decreto NIS;
 - le informazioni di contatto per la segnalazione degli incidenti;
 - le modalità di comunicazione interna, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna;
 - la reportistica da utilizzare per la documentazione dell'incidente;
 - le procedure per comunicare alle parti interne interessate, ivi incluse le articolazioni competenti del soggetto NIS, le attività di ripristino a seguito di un incidente;

Rilevata la necessità di:

- definire un modello organizzativo di gestione della Cybersicurezza, volto a individuare le strutture, le responsabilità e le competenze coinvolte nella protezione dei sistemi informativi aziendali;
- costituire formalmente il Comitato Cybersecurity dell'ASST Gaetano Pini-CTO (Comitato), quale strumento fondamentale per affrontare le nuove esigenze connesse all'implementazione delle misure di sicurezza informatica previste dalla normativa vigente;
- disciplinare le modalità di funzionamento e le responsabilità dei soggetti coinvolti;
- approvare il Piano di Gestione degli Incidenti di Sicurezza Informatica;

Acquisita la proposta del Direttore della UOC Sistemi Informativi Aziendali che propone l'individuazione di Comitato così composto:

- Struttura Cybersecurity ai sensi dell'art.8 della Legge 90/2024:
 - o Direttore UOC Sistemi Informativi Aziendali
 - o Referente Cybersecurity / Punto di Contatto ACN e suo sostituto
 - o Referente CSIRT e suoi sostituti
- Responsabile UOS Ingegneria Clinica
- Referente Privacy
- Data Protection Officer (DPO)
- Direttore UOC Affari Generali e Legali
- Direttore UOC Gestione Acquisti
- Direttore Ufficio Relazioni con il Pubblico
- Responsabile ufficio Comunicazione e relazioni esterne
- Direttore Gestione e sviluppo Risorse Umane
- Direttore Servizio Tecnico Patrimoniale
- Direzioni Mediche di Presidio
- Risk Manager



DELIBERAZIONE DEL DIRETTORE GENERALE n. 704 del 23 DIC. 2025

- Direttore DAPSS
- Capi Dipartimento

Precisato che il Comitato avrà i seguenti compiti principali:

- coordinamento nella gestione degli incidenti e delle crisi cyber;
- monitoraggio dell'attuazione degli obblighi derivanti dalla Direttiva NIS2, dal decreto legislativo di recepimento e dalla Legge n. 90/2024;
- supporto alla Direzione Strategica nelle decisioni relative alla sicurezza cibernetica;

Dato atto che è stato approvato il Piano di gestione degli incidenti di sicurezza Informatica, conservato agli atti e pubblicato sul Sistema di Gestione Qualità aziendale, il quale:

- definisce i livelli di gravità e classificazione degli incidenti;
- disciplina il flusso interno di rilevazione, analisi, contenimento, ripristino e reporting;
- individua le responsabilità operative e decisionali;
- stabilisce le modalità di notifica ai soggetti esterni previsti dalla normativa (CSIRT Italia, ACN, autorità competenti, Garante Privacy in caso di data breach, ecc.);

Viste:

- l'attestazione di regolarità dell'istruttoria e legittimità del presente provvedimento espressa dal Responsabile della UOC proponente;
- l'attestazione di regolarità contabile e della relativa copertura economica da parte del Responsabile della UOC Bilancio, Programmazione finanziaria e Contabilità;

Visti i pareri del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio Sanitario, resi per quanto di competenza, ai sensi dell'art. 3 del D. Lgs. n. 502/1992 e ss.mm.ii;

DELIBERA

per i motivi di cui in premessa che qui si intendono integralmente richiamati:

1. di istituire, presso l'ASST Gaetano Pini-CTO, il Comitato Cybersecurity, con funzioni di:
 - coordinamento nella gestione degli incidenti e delle crisi cyber;
 - monitoraggio dell'attuazione degli obblighi derivanti dalla Direttiva NIS2, dal decreto legislativo di recepimento e dalla Legge n. 90/2024;
 - supporto alla Direzione Strategica nelle decisioni relative alla sicurezza cibernetica;
2. di disporre che il Comitato sia composto dalle seguenti figure aziendali:
 - Struttura Cybersecurity ai sensi dell'art.8 della Legge 90/2024:
 - o Direttore UOC Sistemi Informativi Aziendali
 - o Referente Cybersecurity / Punto di Contatto ACN e suo sostituto
 - o Referente CSIRT e suoi sostituti
 - Responsabile UOS Ingegneria Clinica
 - Referente Privacy
 - Data Protection Officer (DPO)
 - Direttore UOC Affari Generali e Legali
 - Direttore UOC Gestione Acquisti



DELIBERAZIONE DEL DIRETTORE GENERALE n. 704 del 23 DIC. 2025

- Direttore Ufficio Relazioni con il Pubblico
- Responsabile ufficio Comunicazione e relazioni esterne
- Direttore Gestione e sviluppo Risorse Umane
- Direttore Servizio Tecnico Patrimoniale
- Direzioni Mediche di Presidio
- Risk Manager
- Direttore DAPSS
- Capi Dipartimento

3. di stabilire che:

- il Comitato si riunisce periodicamente in forma ristretta, con cadenza almeno trimestrale, per il monitoraggio degli adempimenti e la revisione delle misure di sicurezza;
- il Comitato si riunisce in forma allargata in caso di crisi, incidenti gravi o eventi che possano impattare sulla continuità operativa dei servizi sanitari;
- il punto di contatto ed il referente CSIRT assicurano il collegamento con il CSIRT Italia e con gli organismi competenti previsti dalla normativa;
- il Comitato riferisce periodicamente alla Direzione Strategica, fornendo report, raccomandazioni operative e proposte di miglioramento;

4. di dare atto che è stato approvato il Piano di gestione degli incidenti di sicurezza Informatica, conservato agli atti e pubblicato sul Sistema di Gestione Qualità aziendale, il quale:

- definisce i livelli di gravità e classificazione degli incidenti;
- disciplina il flusso interno di rilevazione, analisi, contenimento, ripristino e reporting;
- individua le responsabilità operative e decisionali;
- stabilisce le modalità di notifica ai soggetti esterni previsti dalla normativa (CSIRT Italia, autorità competenti, Garante Privacy in caso di data breach, ecc.);

5. di stabilire che il suddetto Piano entra in vigore dalla data della presente deliberazione:

6. di stabilire che tutte le strutture aziendali sono tenute a:

- applicare quanto previsto dalla procedura;
- collaborare con il Comitato Cybersecurity;
- segnalare tempestivamente ogni potenziale incidente di sicurezza;

7. di dare atto che dal presente provvedimento non derivano oneri diretti a carico del bilancio aziendale;

8. di dare atto che il presente provvedimento è immediatamente esecutivo ai sensi dell'art 17, comma 6, della L.R. n. 33/2009, così come costituito dall'art.1, comma 1, lett w) della L.R. n. 23/2015



DELIBERAZIONE DEL DIRETTORE GENERALE n. 704 del 23 DIC. 2025

9. di disporre la pubblicazione del presente provvedimento all'Albo Pretorio on line aziendale, ai sensi dell'articolo 17, comma 6, della L.R. n. 33/2009, così come sostituito dall'art. 1, comma 1, lett. w) della L.R. n. 23/2015.

IL DIRETTORE SANITARIO
(Dott.ssa Giuliana SABATINO)

IL DIRETTORE SOCIO SANITARIO
(Dott.ssa Rossana GIOVE)

IL DIRETTORE AMMINISTRATIVO
(Dott. Marco PATERNOSTER)

IL DIRETTORE GENERALE
(Dott.ssa Paola LATTUADA)

UOC Sistemi Informativi Aziendali

Si attesta la regolarità amministrativa e tecnica del presente provvedimento
Responsabile del Procedimento ai sensi della L. 241/90: Ing. Ponziano A. Ricciardelli
Pratica trattata da: Ing. Ponziano A. Ricciardelli



DELIBERAZIONE DEL DIRETTORE GENERALE n. 704 del 23 DIC. 2025

RELATA DI PUBBLICAZIONE

Si certifica che la presente deliberazione è pubblicata all'albo pretorio informatico di quest'Azienda sul sito internet istituzionale, così come previsto dall'art. 32, comma 1, L. 69/2009, e dall'art. 8 del D. Lgs. 33/2013, dal 23 DIC. 2025 e vi rimarrà per quindici giorni consecutivi.

La deliberazione si compone di n. 7 pagine e n. 0 pagine di allegati.

UOC Affari Generali e Legali
Il Funzionario addetto

[Handwritten signature]

Per copia conforme all'originale per uso amministrativo
Milano, li _____

UOC Affari Generali e Legali
il Funzionario addetto