

DELIBERAZIONE DEL DIRETTORE GENERALE

N. DEL

Il Direttore Generale dell'Azienda U.L.S.S. n. 9 SCALIGERA, dott. Patrizia Benini, nominato con D.P.G.R.V. n. 19 del 26/02/2024, coadiuvato dai Direttori:

- dott. Flavia Dal Bosco	Direttore Amministrativo
- dott. Viviana Coffele	Direttore Sanitario f.f.
- dott. Felice Alfonso Nava	Direttore dei Servizi Socio-Sanitari

ha adottato in data odierna la presente deliberazione:

OGGETTO

DEFINIZIONE DEI RUOLI, RESPONSABILITA' E POTERI IN MATERIA DI CYBERSICUREZZA, AI SENSI DELLA DIRETTIVA "NIS2" E DELLA LEGGE N. 90 DEL 28/06/2024

Note per la trasparenza: Con il presente provvedimento si definisce l'organizzazione per la sicurezza informatica dell'Azienda ULSS n. 9 Scaligera e si stabiliscono i ruoli, le responsabilità e i poteri in materia di Cybersicurezza ai sensi della Direttiva NIS2 e della L. n. 90 del 28/06/2024

Il Direttore di UOC Sistemi Informativi

ing. Giorgio Roncolato, riferisce quanto segue.

Richiamati:

- il D.lgs. n. 82 del 7/03/2005 e s.m.i. - "Codice dell'amministrazione digitale" (CAD), all'art. 51 rubricato "Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni", che prescrive ad AgID, al comma 1, il compito di adottare Linee Guida al fine di individuare "le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture";
- La 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;
- il D.lgs. n. 138 del 4/09/2024, recante "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" e, in particolare, l'art. n. 7 e l'art. n. 40, comma 5, lettera b);
- la L. n. 90 del 28/06/2024, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" che prevede adempimenti funzionali al rafforzamento ed alla resilienza delle pubbliche amministrazioni;
- la deliberazione n. 124 del 09/02/2022 "Verifica livelli di sicurezza dei sistemi informatici dell'azienda ULSS n. 9 scaligera e adozione dei primi interventi", con la quale è stata avviata la verifica dei livelli di sicurezza dei sistemi informatici aziendali e sono stati adottati i primi interventi per migliorarne la protezione;
- il Decreto Legge n. 82 del 14 giugno 2021 che ha istituito l'Agenzia per la cybersicurezza nazionale (ACN) quale Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza;
- la DGR n. 1024 del 22/08/2023 che approva il progetto esecutivo del "Computer Emergency Response Team" (CERT) Regionale, in continuità con la DGR n. 1174 del 27/09/2022;
- la deliberazione n. 1086 del 02/11/2023 di "Adesione dell'Azienda ULSS n. 9 Scaligera al progetto "Computer Emergency Response Team" (CERT) regionale" e di approvazione dello schema di convenzione;
- la Determinazione ACN n. 38565 del 26/11/2024 "... informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS ..." in cui vengono definiti ruoli, compiti e impegni dei soggetti essenziali e dei soggetti importanti di cui all'art. 7, comma 6, e all'art. 40, comma 5, lettera b) del D.lgs. n. 138/2024;
- la Determinazione ACN 379907 del 18/12/2025 che stabilisce "le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS" e, in particolare, "le misure di sicurezza di base a carico degli organi di amministrazione e direttivi e in materia di misure di gestione dei rischi per la sicurezza informatica";
- la determinazione ACN n. 379887 del 18/12/2025 che stabilisce "termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimento di designazione dei rappresentanti NIS sul territorio nazionale", prescrive l'obbligo di individuare il "Punto di contatto", il "Sostituto Punto di contatto" ed il "Referente CSIRT e sostituti";

Il Proponente: Il Direttore UOC Sistemi Informativi dott. Giorgio Roncolato



Considerato che:

- l'art. 8, comma 1 della L. n. 90/2024 prevede che *"Le pubbliche amministrazioni centrali, [...] e le aziende sanitarie locali"* debbano individuare *"una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provvede:*
 - 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";*
- il medesimo art. 8 al comma 2 prevede inoltre che presso la struttura individuata debba operare un soggetto identificato come *"referente per la cybersicurezza, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza"*; tale soggetto svolge la funzione di Punto di Contatto Unico dell'Amministrazione con l'Agenzia per la Cybersicurezza Nazionale in relazione a quanto previsto dalla stessa Legge 90/2024 e dalle normative settoriali in materia di cybersicurezza a cui è soggetta l'amministrazione;
- l'Allegato 2 della Determinazione ACN n. 379907/2025 *"Misure di sicurezza di base per i soggetti essenziali"* prescrive agli enti pubblici essenziali, quali sono le Aziende Sanitarie, di adottare una *"politica per la gestione del rischio di cybersicurezza"* e di adottare e documentare le *"politiche di sicurezza informatica per almeno i seguenti ambiti:*
 - a) *gestione del rischio;*
 - b) *ruoli e responsabilità;*
 - c) *affidabilità delle risorse umane;*
 - d) *conformità e audit di sicurezza;*
 - e) *gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;*
 - f) *gestione degli asset;*
 - g) *gestione delle vulnerabilità;*
 - h) *continuità operativa, ripristino in caso di disastro e gestione delle crisi;*
 - i) *gestione dell'autenticazione, delle identità digitali e del controllo accessi;*
 - j) *sicurezza fisica;*
 - k) *formazione del personale e consapevolezza;*
 - l) *sicurezza dei dati;*
 - m) *sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;*
 - n) *protezione delle reti e delle comunicazioni;*
 - o) *monitoraggio degli eventi di sicurezza;*
 - p) *risposta agli incidenti e ripristino";*
- la Giunta regionale ha approvato il progetto del CERT (Computer Emergency Response Team) Regionale con DGR n. 1174 del 27/09/2022, avente i seguenti obiettivi:
 - fornire supporto ed assistenza specialistica nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security;
 - agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cibernetici indirizzati a specifici settori, organizzazioni o territori;
 - incentivare l'applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite;
 - facilitare le attività di prevenzione e monitoraggio degli eventi cibernetici sul territorio, agendo come unità capaci di esercitare un controllo più diretto a livello locale;
 - collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva delle organizzazioni in materia di cyber security;
 - accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi a livello locale;
- la medesima DGR n. 1174 del 27/09/2022 attribuisce ai referenti di sicurezza degli enti aderenti al progetto (GRUPPI 1, 2, 3, 4, 5), tra cui l'Azienda ULSS n. 9 Scaligera, la responsabilità dell'implementazione e della manutenzione dei processi e delle procedure definite a livello direttivo.

Preso atto che la Convenzione per l'adesione al CERT (Computer Emergency Response Team) regionale, approvata con la deliberazione n. 1086 del 02/11/2023 e sottoscritta dal Direttore UOC Sistemi Informativi ing. Giorgio Roncolato in data 23/01/2024, prevede la fornitura, tra l'altro, dei seguenti servizi:

- Sensibilizzazione e formazione dei dipendenti dell'Azienda;
- HyperSOC/ Incident management;
- Penetration Testing;
- Threat intelligence.

Preso atto che il punto 1.3.1 dell'Allegato n. 2 della Determinazione ACN n. 379907/2025 prescrive per i "soggetti essenziali", quali l'Azienda ULSS n. 9 Scaligera, di stabilire e comunicare *"i ruoli, le responsabilità e i correlati poteri in materia di cybersicurezza per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo"*.

Considerato che *"lo sviluppo delle politiche e delle procedure di sicurezza delle informazioni"* comporterà un impatto significativo nell'operatività delle diverse strutture dell'Azienda ULSS, imponendo restrizioni e controlli nelle attività informatiche, si ritiene opportuno definire il modello organizzativo della struttura di cybersicurezza come segue:

- nominare quale Punto di Contatto ACN, di cui all'art. 8, comma 2 della L. n. 90/2024, e Referente per la Cybersicurezza l'ing. Giorgio Roncolato, direttore UOC Sistemi Informativi;
- nominare quale Sostituto Punto di Contatto ACN, di cui all'art. 8, comma 2 della L. n. 90/2024, e vice Referente per la Cybersicurezza il sig. Alessandro Fascina, collaboratore tecnico professionale presso l'UOC Sistemi Informativi;
- dare mandato al Punto di Contatto ACN di nominare il Referente CSIRT e i Sostituti CSIRT, come previsto dalla Determinazione ACN n. 379887/2025;
- costituire una struttura di cybersicurezza denominata *"Comitato Esecutivo Cybersicurezza"*, a supporto della Direzione Generale per gli adempimenti previsti dalle normative, composta da:
 - Referente per la Cybersicurezza con funzione di coordinatore;
 - Punto di Contatto ACN o suo sostituto;
 - Segretario NIS con funzione di supporto amministrativo, nominato dal Referente per la Cybersicurezza;
 - Direttore della Funzione Ospedaliera o suo delegato;
 - Direttore della Funzione Territoriale o suo delegato;
 - Direttore del Dipartimento Prevenzione o suo delegato;
 - Direttore UOC Direzione delle Professioni Sanitarie o suo delegato;
 - Direttore UOC Sistemi Informativi o suo delegato;
 - Direttore UOC Servizi Tecnici e Patrimoniali o suo delegato;
 - Responsabile UOS Ingegneria Clinica o suo delegato;
 - Direttore UOC Affari Generali o suo delegato;
 - Responsabile UOS URP Comunicazione e Marketing o suo delegato;
 - Data Protection Officer;
 - Direttore UOC Provveditorato, Economato e Gestione della Logistica o suo delegato;
 - Direttore UOC Gestione Risorse Umane o suo delegato;
 - Ufficio Qualità e Accreditamento o suo delegato;
- di incaricare i componenti del *"Comitato Esecutivo Cybersicurezza"* di nominare i propri delegati entro 15 giorni dall'approvazione della presente delibera e comunicare i nominativi via e-mail all'apposita casella;
- assegnare al *"Comitato Esecutivo Cybersicurezza"*, ferma restando la supervisione della Direzione Generale, i seguenti ruoli e responsabilità:
 - produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'Amministrazione;
 - predisposizione del piano di adeguamento delle "Misure di sicurezza di base per i soggetti essenziali" di cui all'Allegato 2 della Determinazione ACN n. 379907/2025 entro il 31 gennaio 2026;
 - predisposizione delle politiche e delle procedure di cui all'Allegato n. 2 della Determinazione ACN n. 379907/2025 entro 31 ottobre 2026;
 - produzione e aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;
 - produzione e aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;
 - pianificazione e attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici;
 - pianificazione e attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;
 - monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza;
 - relazionare periodicamente, almeno una volta l'anno, la Direzione Generale sulle attività del Comitato e sui futuri adempimenti derivanti da determinate o linee guida di ACN in materia di NIS2;

- costituire il "Comitato di Gestione delle Crisi di Cybersicurezza" composto dalle seguenti figure o, in caso di assenza, dai sostituti individuati con le specifiche deliberazioni:
 - Direttore Generale;
 - Direttore Amministrativo;
 - Direttore Sanitario;
 - Direttore dei Servizi Socio-Sanitari;
 - Referente per la Cybersicurezza;
 - Punto di Contatto ACN;
 - Vice Punto di Contatto ACN;
 - Direttore UOC Sistemi Informativi;
 - Referente CSIRT di II livello;
 - Data Protection Officer;
 - Responsabile UOS URP, Comunicazione e Marketing;
 - Responsabile Ufficio Legale;
 - Direzione della Funzione Ospedaliera;
 - Direttore della Funzione Territoriale;
 - Direttore del Dipartimento di Prevenzione;
 - Direttore UOC Risorse Umane;
 - Direttore UOC Servizi Tecnici e Patrimoniali;
 - Responsabile UOS Ingegneria Clinica;

- assegnare al "Comitato di Gestione delle Crisi di Cybersicurezza" i seguenti ruoli e responsabilità:
 - definire la strategia di risposta alla crisi;
 - coordinare tutte le funzioni coinvolte nella gestione;
 - autorizzare interventi urgenti e critici (p.es. approvare azioni come lo spegnimento dei sistemi, l'isolamento di reti o l'attivazione del piano di continuità);
 - identificare e supervisionare, in coordinamento con i team tecnici, le azioni prioritarie di contenimento e mitigazione;
 - validare, di concerto con la Direzione Aziendale, le proposte di comunicazioni ufficiali verso l'esterno predisposte dal Responsabile dell'UOS URP, Comunicazione e Marketing;
 - monitorare l'andamento della crisi valutando costantemente la situazione e decidendo se le misure adottate stanno funzionando;
 - chiudere formalmente la crisi e validare il rapporto post-crisi.

Propone l'adozione del provvedimento sotto riportato.

IL DIRETTORE GENERALE

Vista l'attestazione del Responsabile dell'avvenuta regolare istruttoria della pratica in relazione sia alla sua compatibilità con la vigente legislazione nazionale e regionale, sia alla sua conformità alle direttive e regolamentazione aziendali.

Acquisito agli atti il parere favorevole del Direttore Sanitario, del Direttore Amministrativo e del Direttore dei Servizi Socio-Sanitari per quanto di rispettiva competenza.

DELIBERA

Per le motivazioni esplicitate nelle premesse del presente atto, che qui si intendono integralmente riportate:

1. di approvare le premesse quale parte integrante e sostanziale del presente provvedimento;
2. di nominare quale Punto di Contatto ACN, di cui all'art. 8, comma 2 della L. n. 90/2024, e Referente per la Cybersicurezza l'ing. Giorgio Roncolato, direttore UOC Sistemi Informativi;
3. di nominare quale Sostituto Punto di Contatto ACN, di cui all'art. 8, comma 2 della L. n. 90/2024, e vice Referente per la Cybersicurezza il sig. Alessandro Fascina, collaboratore tecnico professionale presso l'UOC Sistemi Informativi;
4. di dare mandato al Punto di Contatto ACN di nominare il Referente CSIRT e i Sostituti CSIRT, come previsto dalla Determinazione ACN n. 379.887/2025;
5. di costituire una struttura di cybersicurezza denominata "Comitato Esecutivo Cybersicurezza", a supporto della Direzione Generale per gli adempimenti previsti dalle normative, composta dalle seguenti figure:
 - Referente per la Cybersicurezza con funzione di coordinatore;
 - Punto di Contatto ACN o suo sostituto;
 - Segretario NIS con funzione di supporto amministrativo, nominato dal Referente per la Cybersicurezza;
 - Direttore della Funzione Ospedaliera o suo delegato;
 - Direttore della Funzione Territoriale o suo delegato;
 - Direttore del Dipartimento Prevenzione o suo delegato;
 - Direttore UOC Direzione delle Professioni Sanitarie o suo delegato;
 - Direttore UOC Sistemi Informativi o suo delegato;

- Direttore UOC Servizi Tecnici e Patrimoniali o suo delegato;
 - Responsabile UOS Ingegneria Clinica o suo delegato;
 - Direttore UOC Affari Generali o suo delegato;
 - Responsabile UOS URP Comunicazione e Marketing o suo delegato;
 - Data Protection Officer;
 - Direttore UOC Provveditorato, Economato e Gestione della Logistica o suo delegato;
 - Direttore UOC Gestione Risorse Umane o suo delegato;
 - Ufficio Qualità e Accreditamento o suo delegato;
6. di incaricare i componenti del "Comitato Esecutivo Cybersicurezza" di nominare i propri delegati entro 15 giorni dall'approvazione della presente delibera e comunicare i nominativi via e-mail all'apposita casella;
7. di assegnare al "Comitato Esecutivo Cybersicurezza", ferma restando la supervisione della Direzione Generale, i seguenti ruoli e responsabilità:
- produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'Amministrazione;
 - predisposizione del piano di adeguamento delle "Misure di sicurezza di base per i soggetti essenziali" di cui all'Allegato 2 della Determinazione ACN n. 379907/2025 entro il 31 gennaio 2026;
 - predisposizione delle politiche e delle procedure di cui all'Allegato n. 2 della Determinazione ACN n. 379907/2025 entro 31 ottobre 2026;
 - produzione e aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;
 - produzione e aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;
 - pianificazione e attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici;
 - pianificazione e attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN);
 - monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza;
 - relazionare periodicamente, almeno una volta l'anno, alla Direzione Generale sulle attività del Comitato e sui futuri adempimenti derivanti da determinate o linee guida di ACN in materia di NIS2;
8. di costituire il "Comitato di Gestione delle Crisi di Cybersicurezza" composto dalle seguenti figure o, in caso di assenza, dai sostituti individuati con le specifiche deliberazioni:
- Direttore Generale;
 - Direttore Amministrativo;
 - Direttore Sanitario;
 - Direttore dei Servizi Socio-Sanitari;
 - Referente per la Cybersicurezza;
 - Punto di Contatto ACN;
 - Vice Punto di Contatto ACN;
 - Direttore UOC Sistemi Informativi;
 - Referente CSIRT di II livello;
 - Data Protection Officer;
 - Responsabile UOS URP, Comunicazione e Marketing;
 - Responsabile Ufficio Legale;
 - Direzione della Funzione Ospedaliera;
 - Direttore della Funzione Territoriale;
 - Direttore del Dipartimento di Prevenzione;
 - Direttore UOC Risorse Umane;
 - Direttore UOC Servizi Tecnici e Patrimoniali;
 - Responsabile UOS Ingegneria Clinica;
9. di assegnare al "Comitato di Gestione delle Crisi di Cybersicurezza" i seguenti ruoli e responsabilità:
- definire la strategia di risposta alla crisi;
 - coordinare tutte le funzioni coinvolte nella gestione;
 - autorizzare interventi urgenti e critici (p.es. approvare azioni come lo spegnimento dei sistemi, l'isolamento di reti o l'attivazione del piano di continuità);
 - identificare e supervisionare, in coordinamento con i team tecnici, le azioni prioritarie di contenimento e mitigazione;
 - validare, di concerto con la Direzione Aziendale, le proposte di comunicazioni ufficiali verso l'esterno predisposte dal Responsabile dell'UOS URP, Comunicazione e Marketing;
 - monitorare l'andamento della crisi valutando costantemente la situazione e decidendo se le misure adottate sono adeguate;
 - chiudere formalmente la crisi e validare il rapporto post-crisi;



10. di dare atto che il presente provvedimento non comporta spesa a carico del Bilancio dell'Azienda ULSS n. 9 Scaligera;
11. di pubblicare il presente provvedimento nell'Albo Pretorio on-line presente nel sito istituzionale di questa amministrazione e nella sezione "Amministrazione trasparente".

Il Direttore Sanitario f.f.
dott. Viviana Coffele

Il Direttore Amministrativo
dott. Flavia Dal Bosco

Il Direttore dei Servizi Socio-Sanitari
dott. Felice Alfonso Nava

IL DIRETTORE GENERALE
dott. Patrizia Benini



DELIBERAZIONE DEL DIRETTORE GENERALE N. DEL

ATTESTAZIONE DI PUBBLICAZIONE E DI ESECUTIVITÀ

La presente deliberazione è divenuta esecutiva dalla data di adozione.

In data odierna copia della presente deliberazione viene:

- Pubblicata per 15 giorni consecutivi nell'Albo on line, ai sensi e per gli effetti dell'art. 32 – comma 1 – della L. 18.06.2009, n. 69 e s.m.i..
- Trasmessa al Collegio Sindacale, ai sensi dell'art. 10 – comma 5 – della L.R. 14.09.1994, n. 56.

Verona, lì

Il Direttore
UOC Affari Generali

TRASMESSA PER L'ESECUZIONE A:

UOC Sistemi Informativi

TRASMESSA PER CONOSCENZA A: