REGIONE DEL VENETO
ULSS7 PEDEMONTANA
Via dei Lotti, n. 40
36061 Bassano del Grappa (VI)
Codice fiscale e partita IVA 00913430245

N. 1387 DEL 24/08/2026

DELIBERAZIONE
del

DIRETTORE GENERALE

Nominato con D.P.G.R. n. 21 del 28/02/2026

Coadiuvato dai sigg.:

DIRETTORE AMMINISTRATIVO	dott.ssa LAURA ESPOSITO
DIRETTORE SANITARIO	dr. ANTONIO DI CAPRIO
DIRETTORE DEI SERVIZI SOCIO – SANITARI	dott.ssa PAOLA VESCOVI

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

IL DIRETTORE GENERALE
DELL'AZIENDA ULSS 7 PEDEMONTANA
dott. Giovanni Carretta

Documento informatico firmato digitalmente ai sensi del D. Lgs n. 82/2005, del T.U. n. 445/2000 e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa; il documento informatico è conservato digitalmente negli archivi informatici dell'Azienda.

Proponente: UOC SISTEMI INFORMATIVI
Anno Proposta: 2026 Numero Proposta: 1379/26

Il Dirigente, Direttore dell'UOC Sistemi informativi, nonché responsabile del procedimento, attesta che la presente proposta di deliberazione è stata regolarmente istruita nel rispetto della vigente normativa nazionale, regionale e regolamentare: f.to Alan Pettenà.

Il Direttore di UOC Sistemi Informativi 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;
- 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. 1790 del 24/10/2023 dell'Azienda ULSS 7 Pedemontana ad oggetto "Progetto computer emergency response team (CERT) regionale. adesione e approvazione schema di convenzione con Regione del Veneto.";
- 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";

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 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";

- 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:
  - gestione del rischio;
  - ruoli e responsabilità;
  - affidabilità delle risorse umane;
  - conformità e audit di sicurezza;
  - gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
  - gestione degli asset;
  - gestione delle vulnerabilità;
  - continuità operativa, ripristino in caso di disastro e gestione delle crisi;
  - gestione dell'autenticazione, delle identità digitali e del controllo accessi;
  - sicurezza fisica;
  - formazione del personale e consapevolezza;
  - sicurezza dei dati;
  - sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
  - protezione delle reti e delle comunicazioni;
  - monitoraggio degli eventi di sicurezza;
  - 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. 7 Pedemontana, 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. 1790 del 24/10/2023 dell'Azienda ULSS 7 Pedemontana 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", tra i quali l'Azienda ULSS n 7 Pedemontana, 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;

Per quanto sopra il Dirigente propone di:

- nominare quale Punto di Contatto NIS, di cui all'art. 8, comma 2 della L. n. 90/2024, e Referente per la Cybersicurezza, il direttore UOC Sistemi Informativi;
- nominare quale Sostituto Punto di Contatto NIS, di cui all'art. 8, comma 2 della L. n.90/2024, e vice Referente per la Cybersicurezza l'assegnatario della funzione organizzativa di area tecnologica o suo delegato presso l'UOC Sistemi Informativi;
- dare mandato al Punto di Contatto NIS 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 NIS o suo sostituto;
  - Data Protection Officer;
  - Direttore della Funzione Ospedaliera o suo delegato;
  - Direttore della Funzione Territoriale o suo delegato;
  - Direttore del Dipartimento di Prevenzione o suo delegato;
  - Direttore UOC Affari Generali o suo delegato;
  - Direttore UOC Direzione delle Professioni Sanitarie o suo delegato;
  - Direttore UOC Gestione Risorse Umane o suo delegato;
  - Direttore UOC Provveditorato, Economato e Gestione della Logistica o suo delegato;
  - Direttore UOC Servizi Tecnici Patrimoniali o suo delegato;
  - Direttore UOC Sistemi Informativi o suo delegato;

- Direttore UOSD Formazione o suo delegato;
- Responsabile UOS Ingegneria Clinica o suo delegato;
- Responsabile Ufficio Relazioni con il Pubblico e Comunicazione o suo delegato;

- di richiedere ai membri del Comitato Esecutivo Cybersicurezza di nominare per iscritto ed entro 15 giorni dalla data di approvazione della presente delibera un delegato considerando quanto segue:
  - i nominativi dei delegati devono essere comunicati al Punto di Contatto NIS entro il termine perentorio sopra indicato.
  - la designazione non comporta il trasferimento delle responsabilità al soggetto delegato, il quale agisce per conto del soggetto delegante.
- 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;
  - predisposizione delle politiche e documentazione di cui all'Allegato n. 2 della Determinazione ACN n. 379907/2025 entro 14 ottobre 2026;
  - gestione/produzione e aggiornamento sistema di analisi preventiva del rischio cyber e di un piano per la relativa gestione;
  - pianificazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale e di interventi di potenziamento delle capacità per la gestione dei rischi cyber.
  - relazionare periodicamente, almeno una volta l'anno, la Direzione Generale sulle attività del Comitato, adempimenti derivanti da determine/linee guida di ACN in materia di NIS2 e da normativa in ambito Cybersicurezza.
- 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 NIS;
  - Sostituto del Punto di Contatto NIS;
  - Data Protection Officer;
  - Referente CSIRT o sostituti;
  - Direzione della Funzione Ospedaliera;
  - Direttore della Funzione Territoriale;
  - Direttore del Dipartimento di Prevenzione;
  - Direttore della UOC Direzione delle Professioni Sanitarie
  - Direttore UOC Gestione Risorse Umane;
  - Direttore UOC Servizi Tecnici Patrimoniali;
  - Direttore UOC Sistemi Informativi;
  - Responsabile Ufficio Affari Legali;

- Responsabile UOS Ingegneria Clinica;
- Responsabile dell'Ufficio Relazioni con il Pubblico e Comunicazione;

- 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 le proposte di comunicazioni ufficiali verso l'esterno predisposte dal Responsabile dell'Ufficio Relazioni con il Pubblico e Comunicazione;
  - 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.

IL DIRETTORE GENERALE

Vista la relazione e la proposta del Responsabile del procedimento;

Dato atto che il responsabile del servizio competente ha attestato l'avvenuta regolare istruttoria della pratica, in ordine alla compatibilità con la vigente legislazione statale, regionale e regolamentare;

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

1. di approvare le premesse quale parte integrante e sostanziale del presente provvedimento;

2. di nominare quale Punto di Contatto NIS, di cui all'art. 8, comma 2 della L. n. 90/2024, e Referente per la Cybersicurezza, il direttore UOC Sistemi Informativi;

3. di nominare quale Sostituto Punto di Contatto NIS, di cui all'art. 8, comma 2 della L. n. 90/2024, e vice Referente per la Cybersicurezza l'assegnatario della funzione organizzativa di area tecnologica presso l'UOC Sistemi Informativi;

4. di dare mandato al Punto di Contatto NIS di nominare il Referente CSIRT e i Sostituti CSIRT, come previsto dalla Determinazione ACN n. 379887/2025;

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 NIS o suo sostituto;
   - Data Protection Officer;
   - Direttore della Funzione Ospedaliera o suo delegato;
   - Direttore della Funzione Territoriale o suo delegato;
   - Direttore del Dipartimento di Prevenzione o suo delegato;
   - Direttore UOC Affari Generali o suo delegato;

- Direttore UOC Direzione delle Professioni Sanitarie o suo delegato;
- Direttore UOC Gestione Risorse Umane o suo delegato;
- Direttore UOC Provveditorato, Economato e Gestione della Logistica o suo delegato;
- Direttore UOC Servizi Tecnici Patrimoniali o suo delegato;
- Direttore UOC Sistemi Informativi o suo delegato;
- Direttore UOSD Formazione o suo delegato;
- Responsabile UOS Ingegneria Clinica o suo delegato;
- Responsabile Ufficio Relazioni con il Pubblico e Comunicazione o suo delegato;

6. 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;
   - predisposizione delle politiche e documentazione di cui all'Allegato n. 2 della Determinazione ACN n. 379907/2025 entro 14 ottobre 2026;
   - gestione/produzione e aggiornamento sistema di analisi preventiva del rischio cyber e di un piano per la relativa gestione;
   - pianificazione dell’adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall’Agenzia per la cybersicurezza nazionale e di interventi di potenziamento delle capacità per la gestione dei rischi cyber.
   - relazionare periodicamente, almeno una volta l'anno, la Direzione Generale sulle attività del Comitato, adempimenti derivanti da determine/linee guida di ACN in materia di NIS2 e da normativa in ambito Cybersicurezza.
7. di richiedere ai membri del Comitato Esecutivo Cybersicurezza di nominare per iscritto ed entro 15 giorni dalla data di approvazione della presente delibera un delegato considerando quanto segue:
   - i nominativi dei delegati devono essere comunicati al Punto di Contatto NIS entro il termine perentorio sopra indicato.
   - la designazione non comporta il trasferimento delle responsabilità al soggetto delegato, il quale agisce per conto del soggetto delegante.
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 NIS;
   - Sostituto del Punto di Contatto NIS;
   - Data Protection Officer;
   - Referente CSIRT o sostituti;
   - Direttore della Funzione Ospedaliera;
   - Direttore della Funzione Territoriale;

- Direttore del Dipartimento di Prevenzione;
- Direttore della UOC Direzione delle Professioni Sanitarie
- Direttore UOC Gestione Risorse Umane;
- Direttore UOC Servizi Tecnici Patrimoniali;
- Direttore UOC Sistemi Informativi;
- Responsabile Ufficio Affari Legali;
- Responsabile UOS Ingegneria Clinica;
- Responsabile Ufficio Relazioni con il Pubblico e Comunicazione;

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'Ufficio Relazioni con il Pubblico e Comunicazione;
   - 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. 7 Pedemontana;

11. di dare atto che la presente deliberazione viene pubblicata all'albo del sito istituzionale dell'Azienda per 10 gg. continuativi, inviata contestualmente al Collegio Sindacale e diventa esecutiva il giorno stesso della sua pubblicazione, come da norma regolamentare approvata con deliberazione n. 1386 del 22/7/2022.