Azienda Sanitaria Locale AL

Sede legale: Via Venezia 6

15121 Alessandria

Partita IVA/Codice Fiscale n. 02190140067

Delibera 345 del 13/05/2025

OGGETTO: LEGGE N. 90 DEL 28.06.2024 "DISPOSIZIONI IN MATERIA DI RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE E DI REATI INFORMATICI" - INDIVIDUAZIONE STRUTTURA AZIENDALE PER LA CYBERSICUREZZA E DESIGNAZIONE REFERENTE.

DIRETTORE GENERALE – Dott. Francesco Marchitelli

Nomina con D.G.R. n. 17-647 del 23.12.2024

ACQUISITI i pareri del

Direttore Sanitario	Dott. Aristide Tortora	Favorevole
Direttore Amministrativo	Dott. Stefano Bergagna	Favorevole

Visto il D.Lgs. n. 502 del 30.12.1992 e successive modificazioni ed integrazioni;

Vista la D.C.R. n. 136-39452 del 22.10.2007 di individuazione delle Aziende Sanitarie Locali e dei relativi ambiti territoriali;

Visto il D.P.G.R. n. 85 del 17.12.2007 di costituzione dell'Azienda Sanitaria Locale AL;

Vista la D.G.R. n. 17-647 del 23.12.2024 di nomina del Direttore Generale dell'ASL AL;

Richiamata la deliberazione del Direttore Generale n. 678 dell'11.10.2017 ad oggetto: "Individuazione degli atti di indirizzo e di governo e degli atti di gestione. Ripartizione delle competenze tra la Direzione Generale e le Strutture dell'A.S.L. AL", come aggiornata con deliberazione n. 11 del 17.01.2025;

Vista la D.G.R. n. 11-8161 del 12.02.2024, ad oggetto: "Atti Aziendali delle AA.SS.RR. – ASL AL di Alessandria – Atto n. 664 del 04.08.2022, modificato con atto n. 655 del 01.08.2023 «Adozione dell'Atto Aziendale dell'ASL AL» recepimento regionale parziale ai sensi della D.C.R. n. 167-14087 del 03.04.2012 all. A, par. 5.1";

Vista la deliberazione del Direttore Generale n. 359 del 18.04.2024 ad oggetto "D.G.R. n. 11-8161 del 12.02.2024. Conclusione procedimento di verifica Atto Aziendale ASL AL – Recepimento prescrizioni regionali";

Premesso che:

- le norme internazionali ISO/IEC 27001 e 27701 definiscono i requisiti tecnici ed operativi per la gestione della sicurezza delle informazioni (ISO/IEC 27001) e per l'estensione delle misure di sicurezza alla protezione dei dati personali (ISO/IEC 27701);
- la Direttiva NIS1 - Network and Information Security - (Direttiva UE 2016/1148), recepita con D.Lgs. n. 65/2018, mira ad innalzare la cooperazione fra gli stati membri e creare un primo livello di armonizzazione in materia di sicurezza cibernetica;
- la successiva Direttiva NIS2 - Network and Information Security - (Direttiva UE 2022/2555), recepita con D.Lgs. n. 138/2024, ha abrogato la Direttiva NIS1 introducendo requisiti più stringenti per la gestione dei rischi e la risposta agli incidenti, aumentando il numero dei soggetti destinatari degli obblighi di cybersicurezza ed obbligando le strutture sanitarie, in quanto rientranti nei "settori ad alta criticità", ad "adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza dei sistemi di rete e di informazione che tali soggetti utilizzano per le loro operazioni o per la fornitura dei loro servizi e per prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi";
- la Legge n. 90 del 28/06/2024, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*", entrata in vigore il 17/07/2024, fornisce indicazioni sia per il miglioramento degli standard di protezione dei sistemi informatici ed informativi sia per l'individuazione di misure tecniche ed organizzative ad uso degli attori coinvolti nei processi di trattamento dei dati di carattere personale;
- l'art. 8 della Legge n. 90/2024 stabilisce l'obbligo per tutti i soggetti di cui all'art. 1 comma 1, tra cui le Aziende Sanitarie Locali, di individuare una struttura della Cybersicurezza al cui interno operi il Referente aziendale per la Cybersicurezza;
- l'art. 8 comma 1 lett. f) della Legge n. 90/2024 prevede che la struttura individuata per la Cybersicurezza provveda alla "pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la Cybersicurezza Nazionale";
- l'Agenzia per la Cybersicurezza Nazionale (ACN), in coerenza con quanto previsto dalla Legge n. 90/2024, ha pubblicato le *"Linee guida per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90*" con lo scopo di indirizzare i soggetti al rafforzamento della propria resilienza tramite l'individuazione di misure di sicurezza e fornendo indicazioni per la loro implementazione nel rispetto di quanto previsto dall'art. 8 comma 1 lett. f);

Preso atto che, ai sensi dell'art. 8 comma 2 della Legge n. 90/2024, il Referente per la Cybersicurezza deve essere individuato "in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza";

Preso atto altresì che l'art. 8 comma 1 della Legge n. 90/2024 dispone "*di individuare, o istituire, una struttura aziendale per la Cybersicurezza che provveda, tra l'altro, allo sviluppo di politiche e di procedure di sicurezza delle informazioni, di definizione ruoli ed organizzazione sistema per la sicurezza delle informazioni, della produzione e dell'aggiornamento del piano programmatico per la sicurezza di dati, sistemi e infrastrutture, del potenziamento delle capacità di gestione degli incidenti, dell'adozione delle misure previste dalle linee guida per la Cybersicurezza emanate dall'ACN, del monitoraggio e valutazione delle minacce e delle vulnerabilità dei sistemi*";

Preso atto inoltre che:
- nel rispetto dell'art. 8 comma 1 della Legge n. 90/2024, la struttura individuata per la Cybersicurezza dovrà provvedere:

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 dei rischi informatici;
c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'Azienda;
d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'Azienda;
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 ed alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza;

Dato atto che:
- il nominativo del Referente per la Cybersicurezza dovrà essere comunicato all'Agenzia per la Cybersicurezza Nazionale;
- la struttura per la Cybersicurezza, ed il relativo Referente, dovranno collocarsi all'interno di una organizzazione di Cybersicurezza ben definita in cui siano specificati ruoli e responsabilità del personale coinvolto e di eventuali terze parti;

Considerato che:
- le strutture sanitarie, nel rispetto dell'Allegato III del D.Lgs. n. 138/2024, rientrano tra le amministrazioni locali soggette agli obblighi di sicurezza informatica, in quanto settori ad alta criticità;
- il contesto tecnico-organizzativo di un'azienda sanitaria locale è particolarmente complesso e delicato tanto da rendere necessaria l'individuazione, in ottemperanza alla Legge n. 90/2024, di apposita struttura aziendale per la Cybersicurezza;

Ravvisata l'importanza strategica delle attività prescritte, nonché le criticità legate agli adempimenti normativi ed al relativo regime sanzionatorio;

Ritenuto, pertanto:
- di individuare la SSA ICT, in staff alla Direzione Generale, quale struttura di riferimento per la Cybersicurezza ai sensi dell'art. 8 comma 1 della Legge n. 90/2024;
- di individuare e di designare l'Ing. Roberto Pozzi, Dirigente Analista Responsabile SSA ICT, quale Punto di Contatto Unico nel rispetto di quanto previsto dall'art. 7 comma 1 lett. c) della decreto NIS2;

- di delegare il Referente designato ad effettuare la registrazione, di cui all'art. 3 della Determinazione del Direttore Generale ACN n. 38565/2024, sulla piattaforma nazionale dell'Agenzia per la Cybersicurezza Nazionale (ACN);
- di dare mandato al Referente, in collaborazione con la SSA Comunicazione URP Formazione, di organizzare e di avviare percorsi formativi specializzati sulle tematiche legate alla cybersicurezza, ed alla normativa di riferimento, per i dipendenti coinvolti;
- di valutare tramite il Broker assicurativo la copertura del rischio cyber;

Attesta la regolarità tecnica e la legittimità del provvedimento essendo state osservate le norme e le procedure previste per la specifica materia;

Visto il parere espresso dal Direttore Amministrativo e dal Direttore Sanitario ai sensi dell'art. 3/7 D.Lgs. n. 502 del 30.12.1992 e s.m.i.

DELIBERA

1) di dare atto, giusto quanto illustrato in premessa, della complessità, in ambito Cybersicurezza, del contesto tecnico-organizzativo dell'ASL AL e della necessità di individuare ruoli e responsabilità del personale coinvolto e di eventuali terze parti;

2) di individuare la SSA ICT, in Staff alla Direzione Aziendale, quale struttura di riferimento per la Cybersicurezza ai sensi dell'art. 8 comma 1 della Legge n. 90/2024;

3) di individuare e di designare l'Ing. Roberto Pozzi, Dirigente Analista Responsabile SSA ICT, quale Punto di Contatto Unico nel rispetto di quanto previsto dall'art. 7 comma 1 lett. c) del direttiva NIS2;

4) di individuare l'ing. Roberto Pozzi, in possesso di specifiche e comprovate professionalità e competenze in materia di cybersicurezza, quale Referente per la Cybersicurezza ai sensi di quanto disposto dall'art. 8 comma 2 della Legge 90/2024 e dalle "Linee guida per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90";

5) di delegare il Referente designato ad effettuare la registrazione, di cui all'art. 3 della Determinazione del Direttore Generale ACN n. 38565/2024, sulla piattaforma nazionale dell'Agenzia per la Cybersicurezza Nazionale (ACN);

6) di dare mandato al Referente, in collaborazione con la SSA Comunicazione URP Formazione, di organizzare e di avviare percorsi formativi specializzati sulle tematiche legate alla Cybersicurezza, ed alla normativa di riferimento, per i dipendenti coinvolti;

7) di valutare tramite il Broker assicurativo la copertura del rischio cyber;

8) di dichiarare il presente provvedimento immediatamente esecutivo ai sensi dell'art. 28, comma 2, L.R. n. 10/1995, stante l'urgenza di provvedere in merito.

Atto sottoscritto digitalmente ai sensi del D.Lgs. n. 82/2005 e s.m.i.

ATTESTAZIONE DI REGOLARITÀ TECNICA E CONTABILE

S.C. PROPONENTE: S.C. AFFARI GENERALI, RELAZIONI ISTITUZIONALI, TUTELE, ATTIVITA` ISPETTIVA

Proposta 977/25

Responsabile del procedimento: Zavanone Anna

Si attesta la regolarità tecnica e la legittimità del provvedimento essendo state osservate le norme e le procedure previste per la specifica materia.

Il Direttore
Fumarola Angela