ARS TOSCANA
agenzia regionale di sanità

DECRETO DEL DIRETTORE

n° 86 del 13/10/2021

Oggetto: Nomina del Chief Information Security Manager - CISO

IL DIRETTORE

Vista la legge regionale 24 febbraio 2005, n. 40 "*Disciplina del servizio sanitario regionale*" e successive modificazioni ed integrazioni;

Visto il Regolamento generale di organizzazione dell'ARS, approvato dalla Giunta regionale con propria deliberazione n. 1320 del 28/10/2019;

Visto il decreto del Presidente della Giunta Regionale n. 90 del 9 aprile 2021, con il quale la sottoscritta è stata nominata Direttore dell'ARS;

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);

Visto il D.lgs 7 marzo 2005, n.82 (Codice dell'amministrazione digitale) e s.m.i.;

Vista la deliberazione della Giunta regionale Toscana n. 585 del 04.06.2018 avente ad oggetto Regolamento (UE) 2016/679 "Regolamento Generale sulla Protezione dei Dati" (GDPR) - Indicazioni alle strutture regionali per la formulazione di linee guida in materia di protezione dati al fine di garantire la compliance dei trattamenti al GDPR;

Considerato che la suddetta deliberazione ha stabilito di individuare nella Direzione Organizzazione e Sistemi informativi la figura del "Security IT Manager" (responsabile della sicurezza delle infrastrutture tecnologiche), nel seguito indicato con Chief Information Security Manager – CISO, con il compito di sovraintendere e controllare che vengano eseguite tutte le misure atte a garantire la sicurezza dei sistemi, delle reti e degli accessi;

Considerata l'esigenza e l'indirizzo contenuto nella suddetta Deliberazione n. 585/2018, in merito alla figura del CISO con l'obiettivo di assicurare all'interno dell'organizzazione le seguenti funzioni:

1. il governo della qualità nella sicurezza IT delle informazioni attraverso funzioni di monitoraggio, controllo delle misure applicate e indicazioni di miglioramento ai soggetti gestori e responsabili della sicurezza IT, verificandone l'applicazione ed i relativi tempi;
2. la gestione del processo di raccolta, gestione e analisi degli incidenti fra cui anche il processo di Data Breach previsto dal GDPR;
3. la gestione della documentazione relativa alle misure di sicurezza adottate nei diversi settori (infrastrutture, sistemi applicazioni), ai controlli effettuati, alle risultanze di tali controlli, ai disciplinari di utilizzo degli strumenti e servizi IT, rendendola immediatamente disponibile in caso di valutazioni, da parte del Garante, del livello di sicurezza adottato;
4. la predisposizione di un piano annuale di interventi finalizzati a svolgere i compiti a lui assegnati;
5. la collaborazione con il Data Protection Officer (DPO) nelle valutazioni dei rischi e degli incidenti;
6. la collaborazione con il responsabile del protocollo e degli archivi al fine dell'individuazione dei rischi e delle soluzioni per ridurli;
7. la collaborazione con il responsabile per la transizione digitale al fine dell'individuazione, programmazione e verifica dei progetti di "trasformazione digitale" in relazione all'obiettivo di innalzare il livello di sicurezza;

Visto il Decreto RT n. 12197 del 13/07/2021 avente ad oggetto "Nomina del Chief Information Security Officer - CISO";

Considerata che Regione Toscana ha manifestato l'esigenza e l'opportunità di condividere la figura del CISO con gli enti dipendenti della Regione di piccole dimensioni che non abbiano personale di idoneo profilo professionale come l'ARS;

Valutato opportuno avvalersi di suddetta possibilità per l'Agenzia;

Dato atto che il presente provvedimento, per sua natura, non è sottoposto al controllo di regolarità contabile;

Tutto ciò premesso e considerato;

DECRETA

1. di avvalersi della facoltà prevista dal Decreto RT n. 12197 del 13/07/2021, sopra citato, di condividere con la Regione Toscana il Chief Information Security Manager – CISO, individuato nella persona dell'Ing. Leonardo Borselli;

2. di incaricare l'Ing. Leonardo Borselli di svolgere almeno i seguenti compiti e funzioni:
   - il governo della qualità nella sicurezza IT delle informazioni attraverso funzioni di monitoraggio, controllo delle misure applicate e indicazioni di miglioramento ai soggetti gestori e responsabili della sicurezza IT, verificandone l'applicazione ed i relativi tempi;
   - la gestione del processo di raccolta, gestione e analisi degli incidenti fra cui anche il processo di Data Breach previsto dal GDPR;
   - la gestione della documentazione relativa alle misure di sicurezza adottate nei diversi settori (infrastrutture, sistemi applicazioni), ai controlli effettuati, alle risultanze di tali controlli, ai disciplinari di utilizzo degli strumenti e servizi IT, rendendola immediatamente disponibile in caso di valutazioni, da parte del Garante, del livello di sicurezza adottato;
   - la predisposizione di un piano annuale di interventi finalizzati a svolgere i compiti a lui assegnati;
   - la collaborazione con il Data Protection Officer (DPO) nelle valutazioni dei rischi e degli incidenti;
   - la collaborazione con il responsabile del protocollo e degli archivi al fine dell'individuazione dei rischi e delle soluzioni per ridurli;
   - la collaborazione con il responsabile per la transizione digitale al fine dell'individuazione, programmazione e verifica dei progetti di "trasformazione digitale" in relazione all'obiettivo di innalzare il livello di sicurezza;

3. di trasmettere il presente atto alla Regione Toscana – Direzione Sistemi informativi, Infrastrutture tecnologiche e Innovazione;

4. di assicurare la pubblicità integrale del presente provvedimento mediante inserimento nella sezione: "Amministrazione trasparente" sul sito web dell'ARS (www.ars.toscana.it).

Il Direttore
TURCO LUCIA
(firmato digitalmente*)

* "Documento informatico sottoscritto con firma digitale ai sensi del D.Lgs n. 82/2005. L'originale informatico è stato predisposto e conservato presso ARS in conformità alle regole tecniche di cui all'art. 71 del D.Lgs n. 82/2005. Nella copia analogica la sottoscrizione con firma autografa è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile secondo le disposizioni di cui all'art. 3 del D.Lgs n. 39/1993."