ASL Lecce Deliberazione.0001534.30-12-2024

Sede Legale e Direzione Generale
Lecce

DELIBERAZIONE DEL DIRETTORE GENERALE
nella Sede Legale di via Miglietta n. 5 – Lecce

O g g e t t o:	"Privacy e Cybersicurezza" - Iniziativa di Formazione Obbligatoria per i Dipendenti Aziendali

STRUTTURA	CENTRO DI COSTO
Ufficio Formazione	

IL DIRETTORE GENERALE

- Visto il D. Lgs. 30/12/1992 n. 502 e successive modificazioni ed integrazioni;
- Vista la Legge Regionale 28/12/1994, n. 36;
- Vista la Legge Regionale 30/12/1994, n. 38;
- Vista la Legge Regionale 03/08/2006, n. 25;
- Vista la Legge Regionale 28/12/2006, n. 39;
- Vista la Legge Regionale 17/04/2018, n. 15;
- Vista la Deliberazione di Giunta Regionale n. 78 del 06.02.2023;
- Coadiuvato dal Direttore Amministrativo e dal Direttore Sanitario

Azienda Sanitaria Locale di Lecce - Via Miglietta, 5 - 73100 - Lecce
P.I. e C.F. 04008300750 - PEC: protocollo@pec.asl.lecce.it

Il Dirigente del Dipartimento/Area/U.O. **Ufficio Formazione** relaziona e propone in merito.

Relazione Istruttoria

Premesso che

- Il Regolamento Generale sulla Protezione dei Dati (GDPR) - Regolamento UE 2016/679 stabilisce l'obbligo per le aziende sanitarie di proteggere i dati personali dei pazienti e del personale mediante l'adozione di misure tecniche e organizzative adeguate
- Il D.Lgs. 196/2003, Codice in materia di protezione dei dati personali, modificato dal D.Lgs. 101/2018 che recepisce il GDPR a livello nazionale, specifica ulteriori misure di adeguamento e introduce sanzioni per il mancato rispetto degli obblighi privacy
- Le Linee guida dell'Autorità Garante per la protezione dei dati personali forniscono raccomandazioni pratiche per l'implementazione delle misure di sicurezza, includendo aspetti come la gestione delle violazioni dei dati (data breach) e le procedure di valutazione del rischio
- Le norme internazionali ISO/IEC 27001 e 27701 stabiliscono rispettivamente *i requisiti tecnici e operativi per la gestione della sicurezza delle informazioni* e *l'estensione delle misure di sicurezza alla protezione dei dati personali*
- La Legge 90/2024 – *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* – promuove la collaborazione pubblico–privato e programmi di formazione specialistica con l'obiettivo di rafforzare l'autonomia tecnologica e industriale dell'Italia nel settore della cybersicurezza
- La Direttiva NIS1 -*Network and Information Security* - (Direttiva UE 2016/1148) recepita in Italia con il D.Lgs. 65/2018 mira ad innalzare la cooperazione fra gli stati membri e a creare un primo livello di armonizzazione in materia di sicurezza cibernetica
- La successiva Direttiva NIS2 -*Network and Information Security* - (Direttiva UE 2022/2555) recepita in Italia con il D.Lgs. 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 e 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 90/2024 all'art. 8 stabilisce l'obbligo per tutti i soggetti di cui all'art. 1 comma 1, tra cui rientrano le Aziende Sanitarie Locali, di individuare - nella propria organizzazione aziendale - una struttura responsabile della cybersicurezza al cui interno operi e venga individuato il referente per la cybersicurezza
- Con deliberazione del Direttore Generale n. 1434 del 11/12/2024 si è provveduto all'individuazione della **Struttura e del Referente per la Cybersicurezza** e alla designazione del **Punto di Contatto Unico** per l'Azienda Sanitaria Locale di Lecce

Tenuto conto che

- L'art. 32 del Regolamento Generale sulla Protezione dei Dati (GDPR) al paragrafo 4 prevede

Azienda Sanitaria Locale di Lecce - Via Miglietta, 5 - 73100 - Lecce
P.I. e C.F. 04008300750 - PEC: protocollo@pec.asl.lecce.it

che “*Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*”

- La direttiva NIS2 fra le misure tecniche, operative ed organizzative da adottare in materia di cybersicurezza, prevede, tra le altre, l’implementazione di pratiche di igiene informatica di base e attività di formazione in materia di sicurezza informatica

Considerato che

- La direttiva NIS2 rappresenta lo standard di riferimento applicabile dalle Organizzazioni che devono o vogliono raggiungere un elevato livello in termini di cybersicurezza per proteggere i propri asset digitali e garantire la sicurezza dei dati in conformità all’art 32 del Regolamento UE 2016/679 (GDPR)
- Fra le amministrazioni locali soggette agli obblighi di sicurezza informatica elencate nell'Allegato III del D.Lgs. n.138/2024 sono presenti anche le Aziende Sanitarie Locali
- La direttiva NIS2 prevede un obbligo di notifica al CSIRT (Computer Security Incident Response Team) e alle autorità competenti, senza ritardo, di qualsiasi incidente che possa avere un impatto significativo sulla fornitura del servizio
- Un qualsiasi incidente informatico che avviene all’interno dell’organizzazione aziendale ha un potenziale impatto estremamente rilevante sia rispetto alla disponibilità (failure) dei sistemi informativi, sia rispetto alla molteplicità delle “categorie particolari di dati” che possono essere interessate (data breach)
- In base ad un rapporto Clusit 2024, relativamente agli attacchi cyber, la sanità risulta essere il settore più colpito a livello globale con un incremento del 83% rispetto al primo semestre 2023
- Il **Computer Security Incident Response Team (CSIRT)** della Regione Puglia, gestito dalla società in house InnovaPuglia, in collaborazione con l'*Ufficio per la Transizione Digitale* e la *Sezione Crescita Digitale delle Persone, del Territorio e delle Imprese* del Dipartimento Sviluppo Economico della Regione Puglia, ha avviato un’iniziativa di formazione sulla sicurezza informatica già erogata per i dipendenti delle Aziende Sanitarie e delle Agenzie Regionali
- La suddetta iniziativa è stata condotta in collaborazione con l’Azienda Sanitaria Locale di Lecce – Amministrazione Digitale Sicurezza e Privacy – già struttura referente aziendale nel campo della cybersicurezza - utilizzando una piattaforma e contenuti in/formativi resi disponibili dal CSIRT Puglia, al fine di valutare e potenziare le competenze in materia di sicurezza
- Sempre attraverso la stessa piattaforma Amministrazione Digitale Sicurezza e Privacy ha attivato una campagna di **phishing simulato** destinata a tutti i dipendenti aziendali
- Tale campagna ha evidenziato che il livello di conoscenza e consapevolezza rispetto – in particolare – al phishing si è rivelato non totalmente adeguato
- Per migliorare la cultura in cybersicurezza è necessario, di conseguenza, sensibilizzare tutti i dipendenti aziendali con una formazione continua che non può limitarsi ad un evento isolato e sporadico
- E’ obiettivo aziendale rendere fruibili i contenuti in/formativi attraverso l’utilizzo di tutte le

Azienda Sanitaria Locale di Lecce - Via Miglietta, 5 - 73100 - Lecce
P.I. e C.F. 04008300750 - PEC: protocollo@pec.asl.lecce.it

tipologie di dispositivo personale (smartphone, tablet, notebook, pc) al fine di coinvolgere la totalità della platea dei dipendenti indipendentemente dal luogo e dal tempo di fruizione (modalità F.A.D. – Formazione a Distanza)

- Nella consapevolezza che detta attività di formazione è sì strumento efficace ma non necessariamente sufficiente è indispensabile garantire la presenza di un supporto “Privacy e Cybersicurezza” procedendo all’individuazione di n. 2 referenti “Privacy e Cybersicurezza” all’interno delle UOC di appartenenza

Considerato ulteriormente che

Le attività formative in tema di cybersicurezza e privacy sono essenziali per:

- Rafforzare la consapevolezza (awareness) e le competenze del personale, in quanto ogni dipendente deve essere in grado di comprendere le implicazioni di un uso improprio dei dati e le potenziali conseguenze di un attacco informatico (le sessioni formative devono includere esempi pratici, simulazioni di attacchi di phishing e protocolli di sicurezza da seguire)
- Assicurare la conformità normativa (compliance), infatti la formazione costante del personale permette di allinearsi alle normative vigenti e di mantenere un approccio aggiornato alle novità legislative. Ciò è particolarmente importante per gestire la complessità delle norme e delle politiche aziendali legate alla sicurezza dei dati.
- Garantire la continuità operativa (Business Continuity), proprio perché un team ben formato è in grado di individuare tempestivamente segnali di minacce informatiche e di adottare contromisure adeguate per evitare interruzioni dei servizi. La continuità operativa dipende dalla capacità di prevenire e mitigare i rischi attraverso una risposta rapida e coordinata
- Proteggere il patrimonio informativo (Security Policy) grazie alla formazione su pratiche di sicurezza avanzate e su protocolli di protezione dei dati che consentono di prevenire accessi non autorizzati e perdite di dati. Ciò contribuisce a salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie

Dato atto che

Le attività formative apportano numerosi benefici a un’azienda sanitaria locale, tra cui:

- Miglioramento della sicurezza complessiva, in quanto la formazione del personale riduce il rischio di errori umani, che spesso sono la causa principale degli incidenti di sicurezza. Il personale consapevole e ben istruito è in grado di identificare situazioni sospette e di adottare misure proattive
- Riduzione dei rischi di sanzioni, grazie alla formazione continua, l'azienda sanitaria può dimostrare agli organi di controllo il proprio impegno nella protezione dei dati personali. La conformità alle normative non solo evita multe e sanzioni, ma migliora la reputazione complessiva della struttura
- Incremento della fiducia da parte di pazienti e stakeholder, infatti la trasparenza nella gestione della sicurezza dei dati, accompagnata da una comunicazione efficace delle misure adottate, contribuisce a rafforzare la fiducia dei pazienti e degli stakeholder nei servizi forniti
- Ottimizzazione dei processi interni, tramite la formazione è possibile standardizzare i processi legati alla sicurezza informatica, rendendo più fluide le operazioni quotidiane. Il

Azienda Sanitaria Locale di Lecce - Via Miglietta, 5 - 73100 - Lecce
P.I. e C.F. 04008300750 - PEC: protocollo@pec.asl.lecce.it

personale acquisisce la capacità di applicare in modo autonomo le misure di protezione, migliorando la qualità del lavoro

- Supporto all'innovazione, grazie alla conoscenza approfondita delle misure di sicurezza e delle tecnologie emergenti è possibile facilitare l'adozione di nuovi strumenti e soluzioni digitali, promuovendo un approccio innovativo e sicuro. La formazione costante garantisce che l'azienda possa affrontare le sfide tecnologiche con competenza e sicurezza

Preso atto

- Di quanto previsto dal D.Lgs. 138/2024 di recepimento della Direttiva NIS2, che impone una serie di obblighi in materia di sicurezza informatica, tra cui la formazione obbligatoria per dipendenti e dirigenti, al fine di garantire una gestione consapevole dei rischi digitali
- Di quanto previsto dall'art. 32 del Regolamento Generale sulla Protezione dei dati (GDPR), secondo cui è necessario prevedere interventi formativi relativamente al trattamento dei dati finalizzati ad illustrare i rischi e i benefici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni
- Della volontà espressa dalla Direzione Strategica Aziendale, interessata in merito da Amministrazione Digitale Sicurezza e Privacy, di avviare, nel rispetto della normativa europea e nazionale e nella consapevolezza dei benefici apportati, uno specifico piano formativo a carattere obbligatorio per tutti i dipendenti aziendali sul tema "Privacy e Cybersicurezza"

PROPOSTA

Per tutto quanto sopra riportato

- **Demandare** alla UOSD Amministrazione Digitale Sicurezza e Privacy e alla UOSD Ufficio Formazione la stesura e la conduzione di un Piano Formativo - **obbligatorio** per tutti i dipendenti aziendali - in materia "Privacy e Cybersicurezza"
- **Indicare** che la somministrazione del Piano Formativo Aziendale avverrà attraverso l'erogazione di corsi distribuiti su 4 differenti livelli di classificazione: livello base, livello intermedio, livello avanzato e formazione in aula
- **Indicare** che i contenuti in/formativi per i livelli base, intermedio e avanzato, saranno erogati, in modalità remota (FAD – Formazione a Distanza), attraverso la Piattaforma CSIRT che rende possibile la fruizione dei moduli da qualsiasi dispositivo personale (smartphone, tablet, notebook, pc)
- **Stabilire** che i moduli in/formativi saranno resi disponibili nell'intervallo temporale 20/01/2025 – 20/04/2025 attraverso l'invio di un messaggio di posta elettronica alla casella PEO nominativa personale aziendale (nome.cognome@asl.lecce.it)
- **Prevedere,** al fine di garantire un livello uniforme di conoscenza, la riproposizione trimestrale dei corsi in/formativi di che trattasi per i dipendenti aziendali (nuovi assunti e/o impossibilitati) che non ne hanno potuto fruire in precedenza
- **Demandare** ai Direttori Responsabili di tutte le Unità Operative Complesse Aziendali l'individuazione di n. 2 Referenti "Privacy e Cybersicurezza"
- **Stabilire** che, per i soli Referenti "Privacy e Cybersicurezza" di UOC sarà obbligatoriamente prevista, oltre al propedeutico superamento dei primi 3 livelli di formazione (base,

Azienda Sanitaria Locale di Lecce - Via Miglietta, 5 - 73100 - Lecce
P.I. e C.F. 04008300750 - PEC: protocollo@pec.asl.lecce.it

intermedio e avanzato), anche la successiva formazione in aula

- **Stabilire** che la partecipazione ai primi due livelli (base ed intermedio) - prevista per tutti i dipendenti aziendali - è **obbligatoria**
- **Stabilire** che la partecipazione alla sessione formativa – livello avanzato - sarà resa disponibile – in forma facoltativa - ai dipendenti che intendono volontariamente approfondire le conoscenze sui temi "Privacy e Cybersicurezza"
- **Stabilire** che il superamento dei due livelli obbligatori (base ed intermedio) e dell'eventuale livello avanzato, qualora la fruizione dei corsi sia avvenuta totalmente fuori dall'orario di servizio, darà diritto al riconoscimento di un credito orario pari alla sommatoria dei "Tempo Riconosciuto" per ogni livello superato, di cui alla tabella seguente
- **Stabilire** che in assenza del superamento di ognuno dei livelli previsti (base, intermedio, avanzato) e/o in presenza della fruizione dei corsi durante l'orario di servizio, non verrà riconosciuto alcun credito orario
- **Indicare** che nella tabella seguente è riportato il tempo riconosciuto per il superamento dello specifico livello se la fruizione del corso è effettuata fuori dal normale orario di servizio

Corso di Formazione – Privacy e Cybersicurezza	
Livello di Classificazione	Tempo Riconosciuto
Base + Intermedio	3 ore
Avanzato	3 ore

- **Indicare** che il superamento dei differenti livelli ed i tempi di fruizione saranno certificati attraverso la Piattaforma CSIRT
- **Stabilire** che il superamento del singolo livello di classificazione sarà determinato dal raggiungimento – certificato dalla piattaforma CSIRT – della soglia del 75% di risposte positive sulla totalità dei quesiti proposti
- **Indicare** che la certificazione dell'avvenuto superamento del livello di classificazione sarà inviata alla casella PEO nominativa personale (nome.cognome@asl.lecce.it) dell'interessato
- **Stabilire** che la formazione in aula, prevista solo per i referenti "Privacy e Cybersicurezza" individuati dai Direttori Responsabili delle UOC, sarà effettuata, a cura del Referente per la Cybersicurezza
- **Indicare** che l'Ufficio Formazione, al termine del periodo stabilito, renderà disponibile all'Area Gestione del Personale i tabulati relativi ai dipendenti che hanno superato i differenti "livelli di classificazione" con il corrispondente "tempo riconosciuto" al fine dell'attribuzione del relativo credito orario
- **Trasmettere** il presente atto all'Area Gestione del Personale per gli adempimenti di competenza
- **Rendere** disponibile attraverso gli strumenti di trasmissione aziendale, il presente atto a tutte le strutture organizzative aziendali

Azienda Sanitaria Locale di Lecce - Via Miglietta, 5 - 73100 - Lecce
P.I. e C.F. 04008300750 - PEC: protocollo@pec.asl.lecce.it

- **Dare atto** che tutti coloro che sono stati interessati dall'istruttoria del procedimento e del compimento di ogni atto endoprocedimentale, nonché i firmatari del presente atto hanno attestato e qui attestano di non versare in alcuna situazione di conflitto di interesse, anche solo potenziale, ex art. 6-bis, l. n. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. n. 62/2013, artt. 6, c. 3, e 7 del Codice di comportamento aziendale (adottato con DDG n. 1778/2014), art. 1, c. 9, lett. e), L. n. 190/2012, e Par. 4.16, Sez. 4 "Rischi corruttivi e trasparenza", del PIAO aziendale 2024-2026 (adottato con DDG n. 87 del 31/01/2024), tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, comma 2, D.Lgs. n. 165/2001 per le fattispecie in cui detta norma trovi applicazione

Il DIRETTORE GENERALE

Vista la relazione istruttoria e la proposta;

Viste le sottoscrizioni apposte in calce al presente provvedimento da parte del Responsabile dell'istruttoria **VARVARA ANNA**, del Responsabile del Procedimento **CAPPELLUTI TASTI ANTONIO** e del Responsabile della proposta **MOSCARA PAOLO,** attestanti il rispetto della vigente normativa regionale, nazionale e comunitaria;

Acquisito il parere favorevole del Direttore Amministrativo e del Direttore Sanitario;

D E L I B E R A

Per tutto quanto sopra riportato

- **Demandare** alla UOSD Amministrazione Digitale Sicurezza e Privacy e alla UOSD Ufficio Formazione la stesura e la conduzione di un Piano Formativo - **obbligatorio** per tutti i dipendenti aziendali - in materia "Privacy e Cybersicurezza"
- **Indicare** che la somministrazione del Piano Formativo Aziendale avverrà attraverso l'erogazione di corsi distribuiti su 4 differenti livelli di classificazione: livello base, livello intermedio, livello avanzato e formazione in aula
- **Indicare** che i contenuti in/formativi per i livelli base, intermedio e avanzato, saranno erogati, in modalità remota (FAD – Formazione a Distanza), attraverso la Piattaforma CSIRT che rende possibile la fruizione dei moduli da qualsiasi dispositivo personale (smartphone, tablet, notebook, pc)
- **Stabilire** che i moduli in/formativi saranno resi disponibili nell'intervallo temporale 20/01/2025 – 20/04/2025 attraverso l'invio di un messaggio di posta elettronica alla casella PEO nominativa personale aziendale (nome.cognome@asl.lecce.it)
- **Prevedere,** al fine di garantire un livello uniforme di conoscenza, la riproposizione trimestrale dei corsi in/formativi di che trattasi per i dipendenti aziendali (nuovi assunti e/o impossibilitati) che non ne hanno potuto fruire in precedenza
- **Demandare** ai Direttori Responsabili di tutte le Unità Operative Complesse Aziendali l'individuazione di n. 2 Referenti "Privacy e Cybersicurezza"
- **Stabilire** che, per i soli Referenti "Privacy e Cybersicurezza" di UOC sarà obbligatoriamente

Azienda Sanitaria Locale di Lecce - Via Miglietta, 5 - 73100 - Lecce
P.I. e C.F. 04008300750 - PEC: protocollo@pec.asl.lecce.it

prevista, oltre al propedeutico superamento dei primi 3 livelli di formazione (base, intermedio e avanzato), anche la successiva formazione in aula

- **Stabilire** che la partecipazione ai primi due livelli (base ed intermedio) - prevista per tutti i dipendenti aziendali - è **obbligatoria**
- **Stabilire** che la partecipazione alla sessione formativa – livello avanzato - sarà resa disponibile – in forma facoltativa - ai dipendenti che intendono volontariamente approfondire le conoscenze sui temi "Privacy e Cybersicurezza"
- **Stabilire** che il superamento dei due livelli obbligatori (base ed intermedio) e dell'eventuale livello avanzato, qualora la fruizione dei corsi sia avvenuta totalmente fuori dall'orario di servizio, darà diritto al riconoscimento di un credito orario pari alla sommatoria dei "Tempo Riconosciuto" per ogni livello superato, di cui alla tabella seguente
- **Stabilire** che in assenza del superamento di ognuno dei livelli previsti (base, intermedio, avanzato) e/o in presenza della fruizione dei corsi durante l'orario di servizio, non verrà riconosciuto alcun credito orario
- **Indicare** che nella tabella seguente è riportato il tempo riconosciuto per il superamento dello specifico livello se la fruizione del corso è effettuata fuori dal normale orario di servizio

Corso di Formazione – Privacy e Cybersicurezza	
Livello di Classificazione	Tempo Riconosciuto
Base + Intermedio	3 ore
Avanzato	3 ore

- **Indicare** che il superamento dei differenti livelli ed i tempi di fruizione saranno certificati attraverso la Piattaforma CSIRT
- **Stabilire** che il superamento del singolo livello di classificazione sarà determinato dal raggiungimento – certificato dalla piattaforma CSIRT – della soglia del 75% di risposte positive sulla totalità dei quesiti proposti
- **Indicare** che la certificazione dell'avvenuto superamento del livello di classificazione sarà inviata alla casella PEO nominativa personale (nome.cognome@asl.lecce.it) dell'interessato
- **Stabilire** che la formazione in aula, prevista solo per i referenti "Privacy e Cybersicurezza" individuati dai Direttori Responsabili delle UOC, sarà effettuata, a cura del Referente per la Cybersicurezza
- **Indicare** che l'Ufficio Formazione, al termine del periodo stabilito, renderà disponibile all'Area Gestione del Personale i tabulati relativi ai dipendenti che hanno superato i differenti "livelli di classificazione" con il corrispondente "tempo riconosciuto" al fine dell'attribuzione del relativo credito orario
- **Trasmettere** il presente atto all'Area Gestione del Personale per gli adempimenti di competenza
- **Rendere** disponibile attraverso gli strumenti di trasmissione aziendale, il presente atto a

Azienda Sanitaria Locale di Lecce - Via Miglietta, 5 - 73100 - Lecce
P.I. e C.F. 04008300750 - PEC: protocollo@pec.asl.lecce.it

tutte le strutture organizzative aziendali

- **Dare atto** che tutti coloro che sono stati interessati dall'istruttoria del procedimento e del compimento di ogni atto endoprocedimentale, nonché i firmatari del presente atto hanno attestato e qui attestano di non versare in alcuna situazione di conflitto di interesse, anche solo potenziale, ex art. 6-bis, l. n. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. n. 62/2013, artt. 6, c. 3, e 7 del Codice di comportamento aziendale (adottato con DDG n. 1778/2014), art. 1, c. 9, lett. e), L. n. 190/2012, e Par. 4.16, Sez. 4 "Rischi corruttivi e trasparenza", del PIAO aziendale 2024-2026 (adottato con DDG n. 87 del 31/01/2024), tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, comma 2, D.Lgs. n. 165/2001 per le fattispecie in cui detta norma trovi applicazione

Il Responsabile dell'istruttoria
VARVARA ANNA

Il Responsabile del procedimento
CAPPELLUTI TASTI ANTONIO

Il Dirigente del Dipartimento/Area/U.O.
MOSCARA PAOLO

PARERI

Direttore Sanitario	**Direttore Amministrativo**
Positivo	**Positivo**
Data	Data
30/12/2024	**30/12/2024**
Il Direttore Sanitario **NACCI MARIA**	Il Direttore Amministrativo **TEDESCHI YANKO**

Il Direttore Generale
ROSSI STEFANO
Documento firmato digitalmente ai sensi del
D.Lgs 82/2005 s.m.i. e norme collegate

Azienda Sanitaria Locale di Lecce - Via Miglietta, 5 - 73100 - Lecce
P.I. e C.F. 04008300750 - PEC: protocollo@pec.asl.lecce.it