NIS 2 Directive Lead Implementer

CODICE	**DT0297**
DURATA	**5 gg**
PREZZO	**1.790,00 €**
EXAM	

DESCRIZIONE

L'importanza di solide misure di cybersecurity non può essere sopravvalutata, poiché le organizzazioni si trovano sempre più spesso ad affrontare tutti i tipi di attacchi informatici.

La direttiva NIS 2 è una normativa concepita per rafforzare la sicurezza informatica dei settori delle infrastrutture critiche, come l'energia, i trasporti, la sanità e i servizi digitali, settori delle infrastrutture critiche, tra cui energia, trasporti, sanità e servizi digitali.

Il corso di formazione NIS 2 Directive Lead Implementer, ha l'obiettivo di acquisire una conoscenza approfondita dei requisiti della direttiva, strategie di implementazione e delle migliori pratiche che proteggono le infrastrutture critiche dalle minacce informatiche.

Attraverso le sessioni interattive ed esercitazioni, i discenti impareranno a valutare i rischi di cybersecurity dell'organizzazione, a sviluppare solidi piani di risposta agli incidenti e a implementare misure di sicurezza efficaci per soddisfare i requisiti della direttiva NIS2.

Inoltre, si acquisiranno approfondimenti sugli standard di settore (ISO/IEC 27001, ISO 22301 ecc.) e sulle best practice che vi permetteranno di rimanere aggiornati sull'evoluzione del panorama delle minacce e di implementare soluzioni di cybersecurity all'avanguardia.

OBIETTIVI RAGGIUNTI

- Spiegare i concetti fondamentali della direttiva NIS 2 e i suoi requisiti;
- Comprendere a fondo i principi, le strategie, le metodologie e gli strumenti necessari per implementare e gestire in modo efficiente un programma di cybersecurity in conformità alla Direttiva NIS 2;
- Imparare a interpretare e implementare i requisiti della Direttiva NIS 2 nel contesto specifico di un'organizzazione;
- Avviare e pianificare l'implementazione dei requisiti della Direttiva NIS 2, utilizzando le best practice;
- Acquisire le conoscenze necessarie per supportare un'organizzazione nella pianificazione,

implementazione, gestione, monitoraggio e mantenimento di un programma di cybersecurity in conformità alla Direttiva NIS 2.

TARGET

- Professionisti della cybersecurity che desiderano comprendere a fondo i requisiti della direttiva NIS2 e apprendere strategie pratiche per l'implementazione di solide misure di cybersecurity;
- Manager e professionisti IT che desiderano acquisire conoscenze sull'implementazione di sistemi sicuri e migliorare la resilienza dei sistemi critici;
- Funzionari governativi e responsabili normativi dell'applicazione della Direttiva NIS 2.

PREREQUISTI

I requisiti principali per partecipare a questo corso di formazione sono la comprensione dei concetti fondamentali della cybersecurity.

CONTENUTI

Giorno 1

Introduzione alla Direttiva NIS 2 e avvio dell'implementazione della Direttiva NIS 2

- Obiettivi e struttura del corso di formazione
- Standard e quadri normativi
- Direttiva NIS

Giorno 2

Analisi del programma di conformità alla direttiva NIS 2, gestione delle risorse e gestione del rischio

- Cybersecurity Governance
- Ruoli e responsabilità nella cybersecurity
- Asset Management
- Risk Management

Giorno 3

Analisi del programma di conformità alla direttiva NIS 2, gestione delle risorse e gestione del rischio

- Controlli di cybersecurity
- Sicurezza della catena di approvvigionamento

- Incident Management
- Crisis management

Giorno 4

Controlli di cybersecurity, gestione degli incidenti e gestione delle crisi

- Business Continuity
- Sensibilizzazione e formazione
- Misurazione, monitoraggio e reporting di prestazioni e metriche

Giorno 5 Mattina

Gestione del miglioramento e della comunicazione ICT

- Miglioramento Continuo
- Comunicazione
- Chiusura del corso di formazione

Giorno 5 Pomeriggio

Esame finale

- Dominio 1 - Concetti e definizioni fondamentali della direttiva NIS 2
- Dominio 2 - Pianificazione dell'attuazione dei requisiti della direttiva NIS 2
- Dominio 3 - Ruoli e responsabilità della sicurezza informatica e gestione del rischio
- Dominio 4 - Controlli di cybersecurity, gestione degli incidenti e gestione delle crisi
- Dominio 5 - Comunicazione e consapevolezza
- Dominio 6 - Test e monitoraggio di un programma di cybersecurity