Sicurezza informatica: NIS 2, L.90/2024 e D.Lgs.138/2024 per pubblica amministrazione, partecipate e imprese

Codice corso
RSI021

Durata e data
1 giorno, in data da stabilire con il committente.

Orario
9-13 (in alternativa 14-18, a seguito di accordi con il committente).

Quota di partecipazione
--,00 € + IVA

Docente
Ing. Saverio Rubini
Docente in master universitari e corsi di formazione professionale, esperto di sicurezza informatica e di tecnologie di comunicazione digitale, consulente aziendale di organizzazione informatica e di Intelligenza Artificiale, sistemista di rete, progettista e creatore di siti Internet, autore di libri e articoli di informatica (Apogeo, Il sole 24 ore, McGraw-Hill).

Obiettivi
Conoscere le finalità della **Legge** cyber italiana **90/2024** e le attività imposte dal **D.Lgs. 138/2024** (entrambe già **in vigore a ottobre 2024**) per il rafforzamento della cybersicurezza nazionale in **recepimento** della direttiva **NIS 2** e sulle responsabilità penali per reati informatici dal punto di vista operativo.
Sapere come **registrare** la propria **organizzazione** e gli altri dati richiesti dal D.Lgs.138/2024 **nel sito dell'ACN** (Agenzia per la Cybersicurezza Nazionale) nelle specifiche scadenze annuali, per **evitare** onerose **sanzioni** e sospensioni dell'attività lavorativa **a carico dei dirigenti** responsabili.
Essere in grado di mettere in atto gli adempimenti che obbligano alla **rilevazione** dei dati relativi ai **sistemi informatici** e alle infrastrutture di **rete** dell'organizzazione da inserire nel sito dell'ACN.
Riuscire a **organizzare** la **documentazione** da produrre e le attività di **formazione** obbligatorie per il personale.
Rispettare gli obblighi di legge relativi alla **notifica** degli **incidenti informatici** nei tempi e nei modi richiesti dalle disposizioni.

Sede

Le lezioni sono tenute in presenza nella sede messa a disposizione dall'organizzazione che invia l'ordine.

Destinatari

Dirigenti Responsabili della Transizione al Digitale (impianti informatici, servizi di comunicazione digitali, reti) di amministrazioni pubbliche centrali e locali, partecipate, aziende erogatrici di servizi energetici, di telefonia, acquedotti, di altri servizi essenziali per i cittadini.
Amministratori e responsabili della transizione digitale di grandi imprese private, di studi di consulenza e aziende di qualsiasi dimensione che forniscono apparecchiature, consulenza e servizi informatici a soggetti importanti o essenziali.

Prerequisiti

Ricoprire una posizione lavorativa nella gestione di servizi e di infrastrutture informatiche in:

- organizzazioni pubbliche e partecipate
- imprese di settori critici o ad alta criticità
- soggetti importanti o essenziali
- fornitori di apparecchiature, consulenza e/o servizi informatici a uno dei soggetti precedenti

Supporto e materiali didattici

I moduli didattici possono comprendere prove pratiche per acquisire competenze materiali svolte con apparecchiature informatiche fornite in aula dal committente.
Durante le lezioni vengono forniti assistenza e supporto individuale.
Dispense e materiali didattici di ogni lezione sono forniti in formato digitale.

Rilascio attestato di frequenza e profitto

Al termine del corso, a ogni partecipante viene rilasciato un attestato con le caratteristiche del percorso formativo e quanto è stato frequentato (come risulta dai fogli di presenza).

Programma

- **Finalità della L.90/2024 e del D.Lgs.138/2024 (già in vigore a ottobre 2024)**
  - Maggiore contrasto agli attacchi informatici e rilevanza penale dei reati
- **Destinatari delle leggi**
  - Soggetti pubblici e privati coinvolti, attività critiche, soggetti importanti ed essenziali, quali imprese e quali aziende di consulenza, tipi di fornitori
- **Adempimenti obbligatori**
  - Struttura e referente della sicurezza informatica, documentazione da produrre, segnalazioni incidenti, professionisti esterni, formazione, conformità normative
- **Contratti di approvvigionamento nella pubblica amministrazione**
  - Criteri per l'aggiudicazione, premialità
- **Adempimenti iniziali e periodici**
  - Dati da fornire nel sito dell'ACN (**Agenzia per la Cybersicurezza Nazionale**), calendario date di scadenza tassative, aggiornamenti obbligatori
- **Documentazione da produrre**
  - Quali protocolli registrare e quali dispositivi, software e dati delle infrastrutture di rete rilevare
- **Misure tecniche minime da adottare**
  - Misure organizzative, tecnologiche e relative al personale
- **Notifiche**
  - Quando, quali e in che tempi segnalare notifiche di incidenti informatici
- **Responsabilità e sanzioni**
  - Figure aziendali responsabili, percentuale del fatturato per sanzioni economiche e importi massimi, maggiorazioni, sospensione attività lavorativa per i responsabili
- **Collaborazione tecnica, obblighi e imposizioni dell'ACN**
  - Tipologie di prodotti, servizi e processi da adottare obbligatoriamente, interventi del CSIRT (Computer Security Incident Response Team)