

SUPSI

NIST Cybersecurity framework e COBIT

Modulo breve

Presentazione

L'ambiente informatico aziendale, in generale, è sempre più connesso, complesso e fonte di rischi (email malevoli, siti fasulli, software difettosi, fornitori collegati/integrati con i sistemi aziendali, infrastruttura cloud, persone interne o esterne malintenzionate ecc.). I rischi, se dovessero concretarsi, potrebbero generare danni seri alla reputazione e alla sostenibilità dell'azienda interessata, come accaduto a varie organizzazioni, anche svizzere, nonché avere ripercussioni più ampie. Pertanto le aziende sono chiamate a proteggere il proprio patrimonio "informativo" e i "propri" dati indipendentemente da chi si occupa della loro gestione. Partendo dai principali rischi informatici questo corso propone delle misure di controllo preventive sulla base del NIST Cybersecurity framework e di COBIT.

Obiettivi

Questo corso presenta il NIST Cybersecurity framework (CSF) e il modello COBIT per la gestione dei rischi di Cybersecurity. I partecipanti potranno mettere in pratica quanto appreso mediante le esercitazioni previste. In particolare, il corso consentirà ai partecipanti di:

- Descrivere i concetti chiave di COBIT per il governo e il controllo dell'informatica
- Identificare le finalità del NIST Cybersecurity framework (CSF)
- Approfondire le sette fasi previste dal NIST Cybersecurity framework (CSF)
- Applicare e valutare le misure da adottare in azienda con l'aiuto di COBIT
- Apprezzare le raccomandazioni svizzere in materia

Destinatari

I possibili partecipanti includono dirigenti IT, gestori della sicurezza delle informazioni (CISO - Chief Information Security Officer), gestori dei rischi aziendali (CRO - Chief Risk Officer), consulenti IT, revisori interni ed esterni (auditor).

Requisiti

Conoscenze generali di sicurezza informatica e di COBIT sono auspicabili.

Certificato

2 crediti di studio ECTS.

Crediti di studio ECTS

2 ECTS

Programma

- Introduzione
- I principali rischi informatici
- Concetti fondamentali di COBIT
- Panoramica del NIST Cybersecurity framework (CSF)
- Le sette fasi del processo del CSF:
 1. Definire le priorità e il perimetro
 2. Orientare l'azione
 3. Definire lo stato attuale (Create current profile)
 4. Eseguire una valutazione dei rischi (Risk assessment)
 5. Definire il traguardo da raggiungere (Create target profile)
 6. Determinare, analizzare e priorizzare gli scostamenti
 7. Allestire il piano d'azione
- Standard minimo emesso dalla Confederazione per migliorare la resilienza delle TIC
- Prevenire la cyber criminalità - Guida per i Comuni
- Conclusione

Durata

24 ore-lezione

Responsabile/i

Roberto Mastropietro, professore SUPSI

Relatore/i

Eugenio Corti, Consulente informatico

Date

19, 26 aprile, 3, 10, 17, 24 maggio 2023

Orari

17.30-21.00

Luogo

SUPSI, Dipartimento tecnologie innovative, Polo universitario Lugano, Campus Est, Via La Santa 1, CH-6962 Lugano-Viganello.

Le lezioni avranno luogo in modalità blended learning.

Costo

CH 900.00

È previsto uno sconto del 10% per i soci individuali di AFTI, AITI, ATEC e itSMF.

Contatti

roberto.mastropietro@supsi.ch

Informazioni

SUPSI, Dipartimento tecnologie innovative
Polo universitario Lugano - Campus Est
Via La Santa 1
CH-6962 Lugano-Viganello
T +41(0)58 666 66 84
dti.fc@supsi.ch

Termine d'iscrizione

Entro il 24 marzo 2023

Link per le iscrizioni

<https://fc-catalogo.app.supsi.ch/Course/Details/36573>