



Corso di formazione IN MODALITÀ TELEMATICA

Sicurezza Informatica e CyberSecurity

CODICE ATTIVITÀ: 09AN20



4/5/8 giugno 2020

LE RAGIONI E GLI OBIETTIVI

Il Corso si propone di definire i profili di sicurezza dei componenti ICT della Pubblica Amministrazione con particolare riferimento alle amministrazioni universitarie. A valle di una specifica analisi del rischio, si forniranno i principali riferimenti tecnici e normativi che le pubbliche amministrazioni devono affrontare anche rispetto alla prevenzione e al trattamento degli incidenti di sicurezza informatica. Contestualmente si identificheranno gli attuali scenari in funzione dello stato dell'arte ICT, riguardo agli obblighi di sicurezza previsti dal Regolamento UE 2016/679 – GDPR, con l'obiettivo di fornire indicazioni per il contenimento dei rischi e le misure minime ed idonee in riferimento alla normativa nazionale ed europea.

IL PROGRAMMA

4/5/8 giugno 2020

(h. 9.00-12.00)

Sicurezza Informatica e introduzione alla CyberSecurity

La sicurezza dei dati e dei sistemi; le tecniche di autenticazione; pseudo-anonizzazione e cifratura dei dati personali; privacy e web; il cloud pubblico e privato; il back up dei dati; Incident Response: design e best-practices; misure ex-post: analisi forensi; strumenti automatici per l'esercizio dei diritti degli interessati; strategie applicative in specifici contesti di riferimento.

Le misure di sicurezza nel trattamento dei dati personali

Il Regolamento 2016/679/UE; i soggetti; dato personale e trattamento; i diritti dell'interessato; privacy by design e privacy by default; l'accountability; il registro dei trattamenti; il Privacy Officer (DPO); la valutazione di impatto privacy; la violazione di dati personali; le certificazioni; le sanzioni amministrative e la responsabilità civile; la responsabilità penale.

Il nuovo quadro normativo in materia di CyberSecurity

La Direttiva NIS e il D.Lgs. 65/2018 - ambito di applicazione soggettivo e oggettivo - perimetro nazionale di sicurezza cibernetica: gli obblighi che spettano ad aziende e P.A. - gli obblighi in materia di sicurezza: misure tecniche e organizzative per la prevenzione e la gestione dei rischi informatici; monitoraggio; compliance - valutazione dell'impatto degli incidenti e notifiche obbligatorie (rete e sistemi informativi/servizi digitali) - la notifica volontaria - la minaccia cibernetica per la Pubblica Amministrazione e le misure introdotte dalla Circolare AgID 2/2017. Il Data Breach: la segnalazione al Garante; la notifica agli interessati; le tempistiche; il registro delle violazioni.

La figura dell'Amministratore di Sistema

L'amministratore di sistema: funzioni, ruolo e requisiti; gestione di sistemi di autenticazione; profilazione ed autorizzazione; custodia delle credenziali; gestione dei flussi di rete; gestione del back-up e di software complessi; valutazione di requisiti di idoneità e caratteristiche soggettive; designazioni individuali; rapporti con il titolare; elencazione analitica degli ambiti di operatività; individuazione dei privilegi; elenco interno ed aggiornato con estremi identificativi delle persone; conoscibilità dell'identità per i servizi relativi al personale; procedure di accesso ad istanza dei lavoratori. Gestione, registrazione e trattamento dei log degli accessi (modalità e tempi conservazione). Controlli e limiti sull'utilizzo delle informazioni: linee guida del Garante su internet e e-mail.

IL COORDINAMENTO

Dott. Armando CONTI, Università degli Studi di Catania

I RELATORI

Prof. Sebastiano BATTIATO, Università degli Studi di Catania

Ing. Oliver GIUDICE, iCTLab

LA METODOLOGIA DIDATTICA

L'azione formativa sarà condotta tramite webinar in diretta streaming.

La piattaforma utilizzata per l'erogazione del Corso di formazione sarà Microsoft Teams.

LA DURATA

Il Corso di formazione avrà una durata complessiva di **9 ore** di formazione *in modalità telematica*:

- 4 giugno 2020 – prima sessione: h 9.00-12.00
- 5 giugno 2020 – seconda sessione: h 9.00-12.00
- 8 giugno 2020 – terza sessione: h 9.00-12.00