Università degli Studi di Palermo

Direzione Generale
Formazione del personale dirigente e t.a.

A tutto il personale TAB

Oggetto: Percorso formativo in materia di "Cybersecurity" - erogato in modalità telematica.

In relazione alla significativa richiesta emersa dall'Analisi dei bisogni formativi 2022, in raccordo con il Dirigente dell'Area Sistemi Informativi e Portale di Ateneo, nel Piano annuale delle attività formative 2022 è stato programmato il corso di formazione indicato in oggetto, che avrà una durata complessiva di 27 ore erogate nelle seguenti modalità.

a) Cybersecurity: nr. 6 moduli da 3 ore ciascuno (a cura di ORSA CONSULTING di Palermo);
b) Cybersecurity in Ateneo: nr. 3 moduli da 3 ore ciascuno (a cura di personale qualificato del SIA).

In allegato si riporta il programma dettagliato dell'intero percorso formativo

Per procedere all'iscrizione, **il cui termine è fissato al 22 aprile p.v.,** occorre:

1. collegarsi al seguente link con le stesse credenziali utilizzate per l'accesso all'indirizzo e-mail UniPa: https://gsa.unipa.it/formazione/IscrizioneCorsi.dll;
2. compilare il modulo online e "confermare l'iscrizione".

Il nulla osta, previsto dall'art 7, comma 11, del Regolamento per l'attività formativa del personale, potrà essere rilasciato dal proprio responsabile di struttura **entro il 29 aprile 2022**, attraverso l'apposita piattaforma informatica ***resoweb***.

Confermando la propria partecipazione al corso, i convocati sono tenuti a partecipare all'evento formativo; la mancata effettiva presenza **senza idonea giustificazione** comporta l'esclusione per sei mesi da altri eventi formativi (art. 6, comma 4, Regolamento per l'attività formativa del personale).
In virtù della Convenzione AMU, sottoscritta tra l'Ateneo e l'AOUP "Paolo Giaccone" di Palermo il 21 dicembre 2021, la presente nota viene inviata all'Unità di Staff Formazione dell'AUOP per il seguito di competenza.

Ai sensi dell'art. 3, comma 9 del Regolamento per l'attività formativa del Personale tecnico amministrativo dell'Università degli Studi di Palermo, la presente convocazione sarà pubblicata sulla intranet del Portale di Ateneo www.unipa.it.

Il Direttore Generale
Dott. Antonio Romeo
Firmato digitalmente da: Riccardo Uccello
Motivo: Per delega del Direttore Generale
Data: 04/04/2022 13:00:03

Hotel de France – Salita Intendenza, 1 - 90133 Palermo
formazionepersonale@unipa.it - http://www.unipa.it
Tel. 091/23893844

Programma percorso formativo in materia di Cybersecurity

MODULO 1
INTRODUZIONE ALLA CYBERSECURITY ED AGLI ASPETTI DI AWARENESS:
LA SICUREZZA DEI DATI INFORMATICI - Docente: ing. Finizio

- Introduzione ed obiettivi del corso
- Il concetto di safety e di security
- Il concetto di dati e informazioni
- Il concetto di sicurezza delle informazioni
- Il concetto di cybersecurity
- Il concetto di sistema di gestione per la sicurezza delle informazioni secondo lo standard ISO/IEC27001
- Il concetto di rischio e livello di rischio
- Il processo di valutazione del rischio

MODULO 2
L'IDENTIFICAZIONE DELLA MINACCIA - Docente: ing. Sacerdoti

- Gli agenti di minaccia
- Le tecniche di minaccia strumentali
- Le tecniche di minaccia con impatto sulle informazioni (ambito logico)

MODULO 3
PROTEZIONE DAGLI ATTACCHI INFORMATICI E PROCEDURE GESTIONALI
Docente: ing. Marino

- Il Rapporto Clusit 2021 sulla sicurezza ICT in Italia: presentazione dei dati salienti
- Il paper di Enisa security smart airports: elementi di interesse
- Condotte di cyber attacco e cyber warfare: differenze e conseguenze
- Le Principali misure di protezione ex Allegato b, DPCM 81/2021
- Politiche di backup delle informazioni.

MODULO 4
LE MISURE DI PROTEZIONE E LA CYBERSECURITY PARTECIPATA - Docente: ing. Marino

- Addestramento ed awareness dei processi di sicurezza dei dati e dei sistemi informativi
- Tecnologie per la protezione di sistemi informativi ed asset
- Le principali misure di rilevamento ex Allegato b, DPCM 81/2021

MODULO 5
L'IDENTIFICAZIONE DELLA MINACCIA - Docente: ing. Sacerdoti

- Attacco e protezione
- I 15 controlli essenziali di cybersecurity derivanti dal framework nazionale di cybersecurity
- Pronto Intervento
- Tecniche di difesa
- Prevenzione

MODULO 6
LE RESPONSABILITÀ LEGALI DEGLI UTILIZZATORI E GESTORI DEI DATI INFORMATICI.
I CYBERCRIMINI - Docente: avv. Alfisi

- Responsabilità civile
- Responsabilità amministrativa
- Responsabilità penale
- Il cybercrimine
- Crimini che hanno come obiettivo reti o dispositivi
- Crimini in cui vengono utilizzati dispositivi informatici per partecipare ad attività criminali
- Come combattere il cybercrimine

- I crimini informatici
- Frode informatica
- Accesso abusivo a un sistema informatico
- Detenzione e diffusione abusiva di codici di accesso a sistemi
- Diffusione di hardware e software diretti a danneggiare sistemi
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- La tutela dell'utente
- Le misure minime di sicurezza dell'utente.

CYBERSECURITY IN ATENEO

Intervento introduttivo del Dirigente Area Sistemi Informativi e Portale di Ateneo, ***Dott. Riccardo Uccello****.*

MODULO 1 - Gaetano Pisano:

- Prevenzione e protezione delle minacce rivolte ai dispositivi fissi e mobili;
- ingegneria sociale e impersonation: le tecniche di attacco rivolte all'Utente;
- vademecum per il lavoro da remoto e non;
- guida all'installazione e alle caratteristiche di sicurezza, della vpn GlobalProtect;
- guida all'uso consapevole dei servizi di rete di Unipa.

MODULO 2 - Benedetto Vassallo:

- Uso consapevole dei servizi di comunicazione Asincrona;
- Tecniche di attacco relativi a phishing e email intruder;
- Protezioni dei sistemi e servizi di cloud.

MODULO 3 - Carmelo Belfiore:

- Il documento in Ateneo: conformità e protezione del sistema documentale.