Ministero dell'Interno

DIPARTIMENTO DEI VIGILI DEL FUOCO E DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVILE
DIREZIONE CENTRALE PER LE RISORSE LOGISTICHE E STRUMENTALI
Ufficio per le Tecnologie dell'Informazione e della Comunicazione

Alle	Direzioni Centrali
Alle	Direzioni regionali e Interregionali
Ai	Comandi dei Vigili del Fuoco
Agli	Uffici di Diretta Collaborazione
All'	Ufficio Centrale Ispettivo
All'	Opera Nazionale di Assistenza

(Invio tramite posta elettronica certificata)

OGGETTO: Piano di formazione "Cybersicurezza 2022" per il personale informatico delle strutture centrali e territoriali del CNVVF.

Nel quadro delle azioni poste in essere per il miglioramento della sicurezza dei sistemi e delle reti e per l'innalzamento della capacità di contrasto alle minacce informatiche, l'Ufficio per le Tecnologie dell'Informazione e della Comunicazione della scrivente Direzione Centrale ha organizzato un piano di formazione in materia di cybersicurezza, che prevede l'erogazione di 7 corsi nel periodo dal 26 settembre al 23 dicembre 2022, della durata di due settimane ciascuno, destinati al personale informatico del CNVVF.

Tale esigenza formativa è fortemente relazionata all'attuale contesto storico, che vede la sicurezza informatica quale elemento indispensabile per assicurare la continuità operativa dei servizi erogati dalle pubbliche amministrazioni ed è in linea con quanto previsto nel documento di "Strategia nazionale per la cybersicurezza 2022-2026" predisposto dall'Agenzia Nazionale per la Cybersicurezza.

Il Piano di formazione "Cybersicurezza 2022" costituisce il primo pacchetto inserito in un più ampio quadro di interventi formativi finalizzati ad aumentare, con progressivo livello di approfondimento, le conoscenze e le capacità operative del personale informatico del CNVVF in tema di cybersicurezza. Si riportano di seguito le informazioni inerenti al Piano di Formazione in questione:

Modalità di erogazione:	F.A.D. sincrona;
Numero Edizioni:	7;
Numero totale discenti:	280 (40 discenti per ciascuna edizione);
Durata di ciascuna edizione:	72h (2 settimane da 36h, su base 5 gg a settimana);
Orario lezioni:	dal lunedì al giovedì dalle ore 8:30 alle ore 13:30, dalle ore 14:30 alle ore 17:30; venerdì dalle ore 8.30 alle ore 12:30;
Staff didattico e direzione corsi:	Personale dell'Ufficio ICT
Commissioni di esame:	Personale dell'Ufficio ICT;

Ministero dell'Interno

DIPARTIMENTO DEI VIGILI DEL FUOCO E DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVILE
DIREZIONE CENTRALE PER LE RISORSE LOGISTICHE E STRUMENTALI
Ufficio per le Tecnologie dell'Informazione e della Comunicazione

Attività di docenza: Personale specialista contrattualizzato dall'Ufficio ICT;

Attività di tutoraggio: Personale addetto contrattualizzato dall'Ufficio ICT (gestione tecnica delle sessioni in videoconferenza, gestione aula, ecc).

Il calendario delle 7 edizioni dei corsi sarà il seguente:

EDIZIONE	PERIODO	UNITÀ DISCENTI
1	26 settembre – 7 ottobre	40
2	10 - 21 ottobre *(da confermare)*	40
3	24 ottobre – 4 novembre *(da confermare)*	40
4	7 novembre – 18 novembre *(da confermare)*	40
5	21 novembre – 2 dicembre *(da confermare)*	40
6	5 dicembre – 19 dicembre *(da confermare)*	40
7	12 dicembre – 23 dicembre *(da confermare)*	40

I referenti per l'organizzazione e l'esecuzione dei corsi sono il D. ing. Marco DI LEONARDO e l'IIE Monica SABATINI. Per ogni informazione o chiarimento sarà possibile contattare l'Ufficio ICT all'indirizzo di posta *formazioneict@vigilfuoco.it*.

Si allega il programma relativo a ciascuna edizione di corso.

Al fine di consentire l'organizzazione dei corsi, preliminarmente all'avvio del Piano di Formazione sarà erogato a tutto il personale informatico del CNVVF un questionario on line. La compilazione del questionario avrà valore di adesione al corso e sarà attivo **dal 12 al 14 settembre 2022**. Il questionario avrà durata di 30 minuti e sarà costituito da 30 domande a risposta multipla (1 punto a risposta esatta; -0,1 punti a risposta errata; 0 punti a risposta nulla). Qualora il numero delle adesioni fosse auspicabilmente superiore al massimale previsto (nr. 280 discenti), l'Ufficio ICT provvederà ad organizzare edizioni aggiuntive nell'anno 2023.

Seguirà, con successiva nota, il link alla piattaforma su cui verrà reso disponibile il questionario e la conferma del calendario.

IL DIRETTORE CENTRALE
(NANNI)
(documento firmato digitalmente ai sensi di legge)

NANNI GIOVANNI
MINISTERO
DELL'INTERNO/80219290584
01.09.2022 13:47:56
GMT+01:00

LISTA DI DISTRIBUZIONE
POZZI
DI LEONARDO
SABATINI

POZZI DAVIDE
MINISTERO
DELL'INTERNO/80219290584
01.09.2022 11:00:19
GMT+01:00

Ministero dell'Interno

DIPARTIMENTO DEI VIGILI DEL FUOCO E DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVILE
DIREZIONE CENTRALE PER LE RISORSE LOGISTICHE E STRUMENTALI
Ufficio per le Tecnologie dell'Informazione e della Comunicazione

ALLEGATO – PROGRAMMA DEL CORSO

Threats, Attacks, Vulnerabilities	**1.** Overview sulle tematiche generali di Cybersecurity: concetti ed elementi chiave (es. minacce, rischi e contromisure. Tipologie di attaccanti e metodologie di attacco. Best practice per utenti ed amministratori. (4h)
Governance, Risk and Compliance	**2.** Overview generale sulle normative in ambito Cybersecurity e Data Protection (include GDPR, NIS, PSNC, Misure minime AgiD, ecc.) e risvolti operativi per le aziende e per la gestione delle risorse del sistema informativo. (4h) **3.** Fondamenti di Cyber Risk Management, overview sulle metodologie e strumenti per l'analisi del rischio. (8h)
Architecture and Design Implementation	**4.** Approccio Security by design, overview sulle attività di sicurezza durante il ciclo di vita degli asset informatici, infrastrutture e applicazioni, overview delle principali soluzioni di sicurezza, configurazione sicura dei sistemi. **Lab** Code review guidata. (8h) **5.** Fondamenti di Cloud e Cloud Security, principali strumenti e tecnologie a supporto. (4h) **6.** Network & Infrastructure Security: principi di networking, principali strumenti di networking e sicurezza delle reti (Firewall, IDS, IPS, NGFW, Anti-Dos), segregazione delle reti, meccanismi di autenticazione. (8h) **7.** Endpoint Security: Endpoint threat, file e disk encription, AV, NextGen AV e EPP, Infrastructure device for endpoint protection, endpoint hardening, email security, endpoint controls (CIS). (8h) **8.** Identity & Access e PKI: fondamenti di gestione utenze, profili, accessi e privilegi, modalità di autenticazione e gestione certificati, fondamenti di crittografia, CA e PKI. (8h)
Operations e Incident Response	**9.** Vulnerability Management & Ethical Hacking: processi di Ethical Hacking (concetti di VA/PT, Red Team, ecc.). **Lab** Visione guidata dell'hacking di una macchina. (8h) **10.** Strutture di Cyber Detection & Response e tecnologie a supporto: overview sulle principali strutture di Cyber Monitoring & Response (SOC, CERT, SIEM, SOAR), ruoli, task e principali differenze tra di essi, processi di Incident response, tecnologie di XDR, MDR, ecc. (8h) **11.** Threat & Security Intelligence: introduzione alla security intelligence & OSINT, frodi, ecc. Lab Esercitazione pratica in ambito OSINT. (4h)

Via Cavour n. 5 – 00184 Roma – Tel. 06 46529913
ril.ufficioict@vigilfuoco.it - ril.ufficioict@cert.vigilfuoco.it