ANEXO I

Propuesta de dictado

DIPLOMATURA UNIVERSITARIA DE FORMACIÓN CONTINUA EN CIBERSEGURIDAD

-- Cohorte 2024–

1. Datos generales

a. Tipo de curso: Diplomatura

b. Certificado: DIPLOMATURA UNIVERSITARIA DE FORMACIÓN CONTINUA EN CIBERSEGURIDAD

c. Unidades Académicas: FaMAF - FCEFyN

d. Período lectivo: Mayo a diciembre 2024

e. Disponibilidad horaria del alumnado: 234 horas, 156 virtual síncrónicas y un estimativo de 234 horas de trabajo práctico sincrónico/asincrónico e instancias de tutorías. Las 156 horas virtuales sincrónicas comprenden las clases teórico-prácticas de los 5 módulos obligatorios de 24 horas cada uno (120 horas total) y de los 2 módulos obligatorios de 18 horas cada uno (36 horas total).

f. Horario de clases sincrónicas teóricas virtuales: DOS clases semanales de TRES horas reloj los días viernes de 18:30 a 21:30 y sábado de 9:00 a 12:00, según Cronograma incluido más adelante.

g. Lugar en que se desarrollarán las clases: Aula Virtual Famaf

h. Número mínimo y máximo de estudiantes: mínimo 30, máximo 50

i. Perfil de los estudiantes que pueden asistir al curso: El curso se dirige principalmente a Técnicos y/o profesionales que desean incursionar en ciberseguridad o ya están trabajando en el área y necesitan profundizar y/o completar sus conocimientos como analistas de contención de ataques de ciberseguridad.

2. Programa

2.1. Fundamentación

En los últimos años, no pasa un día sin recibir noticias sobre ciberseguridad. Puede ser un ataque de ransomware sobre una red corporativa afectando a miles de clientes con un costo de cientos de millones de pesos, o la inofensiva molestia a ciudadanos mediante correo no deseado que tiene el potencial de ser más riesgoso de lo que aparenta.

La ciberseguridad ha madurado como cuerpo de conocimiento (CYBOK, 2022) y no sólo se refiere a las herramientas y técnicas utilizadas para proteger dispositivos tecnológicos, los datos que contienen y las funciones que realizan. También tiene que ver con aspectos que incluyen la mayoría de las actividades normales de la vida moderna con las que hay que lidiar todos los días, como las contraseñas que protegen un teléfono celular, una computadora y diversas cuentas en línea, así como las prácticas y defensas para mantener todo seguro. Se trata de un campo profesional en crecimiento permanente, para decirlo suavemente. La demanda de ciber profesionales es consistentemente alta, tal como lo describe (CyberSeek, 2022) y las perspectivas para la próxima década son extremadamente prometedoras.

Se ha diseñado este trayecto de formación para reconocer y responder a problemas relacionados con el dominio de la ciberseguridad en el entorno regional. Puede visitar la página "Qué es la ciberseguridad" (¿Ciberseguridad?, 2022) para obtener mayor información a qué nos referimos.

2.2. Objetivo

Incorporar aspectos conceptuales y aptitudes del dominio de la ciberseguridad a la formación de un profesional con nivel técnico vinculado al área de la informática, a fin de que le permita colaborar en la implementación de aspectos básicos de protección de activos de información de una PYME y/o mediana empresa. Desarrollar capacidades para contener y dar una primera respuesta (perfil de analista de primer nivel de un Centro de operación de Ciberseguridad por su sigla en inglés SOC-) a incidentes de ciberseguridad.

2.3. Contenidos

2.3.1. Módulos Obligatorios

Todos los módulos son obligatorios y se dictan de manera virtual sincrónica y comprenden las clases teórico-prácticas. Cinco módulos son de 24 horas de dictado virtual sincrónico cada uno (120 horas total) y dos módulos son 18 horas de dictado virtual sincrónico cada uno (36 horas total).

i. Criptografía aplicada (24 h)

Partiendo de una visión de la teoría de información aplicada al estudio de los sistemas secretos se reflexiona sobre el valor de la información para una correcta toma de decisiones y de las transformaciones a las que se las somete para protegerla.

Propiedades de confidencialidad, integridad, disponibilidad para la información. El uso de la criptografía simétrica, asimétrica y funciones de hash como mecanismo para su implementación. El desarrollo se centrará en algoritmos estándares de uso frecuente en sistemas operativos. Se recorre el estudio de firma digital como servicio compuesto en el contexto de una PKI. Su utilización para autenticación de dominios, firma de código y firma de documentos, entre otros.

Prácticos: Herramientas para la gestión de claves. Uso de algoritmos para intercambio confidencial de información. Controles de integridad. Firma de Código. Ransomware.

ii. Aspectos de seguridad en redes y servidores (24 h)

Protección con firewall basada en zonas. Su aplicación a la protección en el borde de redes empresariales o para delimitación de redes con diferentes niveles de seguridad. La necesidad de IDS/IPS basados en red y host. Su configuración en ambientes virtualizados. Conceptos de Switched Port

Analyzer(SPAN) para despliegue de sensores IDS/IPS. Se deja abierta la necesidad de implementar monitoreo de eventos para completar estos mecanismos de protección.

Prácticos: Implementación de reglas de protección con ZBFW. Uso de Snort, Suricata.

iii. Seguridad en la Nube (24 h)

Introducción a la Seguridad en la Nube. Gestión de Identidades y Accesos. Seguridad de los Datos. Seguridad de la Red. Gobierno, Normas de Seguridad y Mejores Prácticas. Cumplimiento, Supervisión y Auditoría. Respuesta a Incidentes. Herramientas y Servicios de Seguridad.

Prácticos: Creación de cuenta en algún servicio de nube, instalación de recursos de Seguridad para controlar postura y comprender cómo funcionan los permisos en general. Discusión de servicios más complejos.

iv. Autenticación, Autorización y Auditoría (18 h)

Presentación de la necesidad de protección de recursos en terminales utilizando CAD, CAM, RBAC, ABAC, TAC. Su aplicación en sistemas operativos W/L. Reconocer la necesidad de una estrategia de AAA para la gestión de control de acceso. Su aplicación a los dispositivos de una red.

Prácticos: Implementar aspectos de controles de acceso a recursos en W/L. Implementar AAA en una red virtual.

v. Gestión y operación de incidentes de ciberseguridad(24 h)

Estrategias para monitorear eventos de seguridad en una red. Estudio de SIEM/NMS. Security Onion (SECURITYONION, 2022) es una distribución de Linux gratuita y abierta para la búsqueda de amenazas, la supervisión de la seguridad empresarial y la gestión de registros. Incluye una interfaz web nativa con herramientas integradas que los analistas usan para responder a alertas, búsqueda de evidencia de un ataque, catalogar evidencia en casos, monitorear el rendimiento de la red, entre otras funciones. Incluye herramientas de terceros, como Elasticsearch, Logstash, Kibana, Suricata, Zeek (anteriormente conocido como Bro), Wazuh, Stenographer, CyberChef, NetworkMiner y otros.

Prácticos: Instalación y gestión de Security Onion en un ambiente de laboratorio.

vi. Gestión de riesgos de seguridad de la información (24 h)

Necesidad de un SGSI. Políticas de seguridad (Política UNC, 2008) (PAU, 2022). Estándares (ISO 27002, 2022) (ISO27002.ES, 2022). Guías (NSA_a ,2022). ISO 27000 para PYMES como contexto para abordar principios de gestión de riesgos. Minimización de riesgos de ciberseguridad en la protección de los activos de información. Recuperación ante incidentes de ciberseguridad.

Práctico: Elaborar una plan de acción para minimizar riesgos de ciberseguridad en mi organización aplicando políticas de seguridad, estándares y/o guías.

vii. Aspectos de malware y modalidades de ciberataque (18 h)

Modelos de referencia. MITRE ATT&CK (Mitre Attack, 2022). CyberKillChain (CyberKillChain, 2022). Inteligencia de amenazas. Tipos más comunes de malware. Vectores de transmisión y difusión. Estrategías de protección. Phishing. Ransomware. Etc..

Prácticos: Uso de plataformas como VirusTotal. Otras.

3. Estructura de dictado

El dictado de la DIPLOMATURA UNIVERSITARIA DE FORMACIÓN CONTINUA EN CIBERSEGURIDAD 2024 se realizará en formato virtual sincrónico, de la siguiente forma.

Las clases se desarrollarán de manera virtual sincrónica con una metodología expositiva participativa de contenidos teóricos y prácticos, donde el objetivo fundamental es lograr alta interactividad entre los participantes, a través de actividades grupales. Por otro lado, se proponenactividades integradoras en entorno virtual educativo para promover la aplicación de los contenidos a la práctica y el afianzamiento de las competencias de las herramientas. Las clases y actividades integradoras se llevarán a cabo a través de recursos destinados a clases sincrónicasen entorno virtual (zoom, meet). El encuentro sincrónico quedará registrado y disponible para acceder por parte de los estudiantes para facilitar el afianzamiento de los contenidos transmitidos. Además, se evaluará la posibilidad de generar videos explicativos que faciliten la comprensión de los contenidos del programa. El aula virtual funcionará como espacio de encuentro e intercambio, a partir de incorporar diferentes recursos que permitan el trabajo colaborativo. Los recursos que seutilizarán serán software, plataformas colaborativas, plataformas de testeo, videoconferencias, recursos de Moodle y cuestionarios, entre otros.

El Coordinador General será el encargado de mediar el desarrollo administrativo y académico de la diplomatura tanto hacia el interior de las respectivas facultades como con el área central de la Universidad. También son los responsables de la relación de la diplomatura con otras instituciones y con el medio. Coordinarán la relación con los docentes, su contratación y la gestión de su eventual reemplazo en caso de ser necesario.

También coordinarán la recolección y registro de aprobación de los módulos que componen la diplomatura, en un único documento de seguimiento del alumno, el cual también tendrá asociado un seguimiento del pago de las cuotas que correspondan.

4. Evaluación

Los módulos se dictarán en forma consecutiva, y cada uno tendrá una evaluación formativa en un momento intermedio del desarrollo, de tipo diagnóstico; más una evaluación integradora final por módulo. Se evaluarán mediante prueba estructurada escrita y/o presentación de un informe de un pequeño proyecto. La presentación escrita será enviada por el aula virtual y responderá al siguiente formato: portada, introducción, desarrollo, conclusión y bibliografía. Una vez presentado el informe por escrito (según cronograma), se implementará una instancia sincrónicapara su presentación defensa oral de forma presencial o virtual.

La diplomatura tendrá un enfoque práctico-teórico. Los teóricos estarán dirigidos por el abordaje de soluciones a problemas prácticos, fuerte motivación en presentación de problemas y soluciones que se encuentran en la industria de la ciberseguridad. Los teóricos se desarrollan de acuerdo a un modelo de formación profesional con discusión de conceptos cortos y experimentación en entorno virtual. Los prácticos estarán orientados a ejercicios y pequeños proyectos en los que pondrán en práctica los contenidos teóricos y sobre los que centrará la evaluación final. Estos prácticos serán asistidos por tutores de forma virtual no sincrónica.

4.1 Requisitos de aprobación

Aprobar con un mínimo del 70% las evaluaciones parciales, finales y los prácticos. Cumplir con un mínimo de 80% de asistencia a las clases virtuales.

4.2 Bibliografía

1.- CYBOK (2022) https://www.cybok.org/

2.- ¿Ciberseguridad? (2022) https://www.futureoftech.org/cybersecurity/1-what-is-cybersecurity/.

3.- CyberSeek (2022) https://www.cyberseek.org/.

4.- SECURITYONION (2022) https://securityonionsolutions.com/software/.

5.- ISO 27002 (2022). Information security, cybersecurity and privacy protection —Information security controls. Recuperado de https://www.iso.org/standard/75652.html

6.- ISO27702.ES (2022). Recursos relacionados con Sistemas de Gestión de Seguridad de la Información. Recuperado de https://www.iso27000.es/iso27002.html

7.- NSA_a (2022). Network Infrastructure Security Guide. National Security Agency. Cybersecurity Technical Report. Recuperado de https://acortar.link/crJZ18

8.- Política UNC (2008). Política de Seguridad de la Información para la Universidad Nacional de Córdoba. Rec. de https://www.unc.edu.ar/sites/default/files/PoliticadeSeguridad08.pdf

9.- PAU (2022). Políticas de uso aceptable. Uso responsable y no responsable del servicio de red. CeSPI UNLP. Recuperado de https://www.cespi.unlp.edu.ar/cert/politicas-de-uso-aceptable-18905

10.- Mitre Attack (2022). MITRE ATT&CK. Recuperado de https://attack.mitre.org/

11.- Cyber Kill Chain (2022). The Cyber Kill Chain Framework. Recuperado de

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

5. Cronograma Propuesto

Preinscripciones: 1 al 21 de Abril.

Elaboración de orden de mérito: 22 al 25 de Abril.

Publicación de orden de mérito: 26 de Abril.

Inscripción definitiva: del 26 de abril al 10 de Mayo.

Inicio: Viernes 17 de Mayo.

Módulo 1: Criptografía aplicada. Del 17 de Mayo al 8 de Junio. 17, 18, 23, 24 y 31 de Mayo, 1, 7 y 8 de Junio.

Módulo 2: Aspectos de seguridad en redes y servidores. Del 14 de Junio al 13 de Julio. 14, 15, 28, 29 de Junio y 5, 6, 12 y 13 de Julio.

Módulo 3: Gestión y operación de incidentes de ciberseguridad. Del 19 de Julio al 10 de Agosto. 19, 20, 26 y 27 de Julio, 2, 3, 9 y 10 de Agosto.

Módulo 4: Autenticación, Autorización y Auditoría (Control de Acceso). Del 15 al 31 de Agosto. 15, 16, 23, 24, 30 y 31 de Agosto.

Módulo 5: Seguridad en la Nube. Del 6 al 28 de Septiembre. 6, 7, 13, 14, 20, 21, 27 y 28 de Septiembre.

Módulo 6: Gestión de riesgos de seguridad de la información. Del 25 de Octubre al 16 de Noviembre. 25, 26 de Octubre, 1, 2, 8, 9, 15 y 16 de Noviembre.

Módulo 7: Aspectos de malware y modalidades de ciberataque. Del 29 de Noviembre al 14 de Diciembre. 29, 30 de Noviembre y 6,7, 13, 14 de diciembre.

6. Cuerpo Académico Propuesto

El cuerpo académico propuesto es:

6.1 Docentes

Módulo 1: Criptografía aplicada: Ing. Miguel Montes (UNC)

Módulo 2: Aspectos de seguridad en redes y servidores: Prof.Ing.Renzo Mare (UNR) Profesor ayudante: Ing. Federico Damián Quattrin.

M**ódulo 3:** Seguridad en la Nube: Ing. Alfredo Pardo (UCC)

Módulo 4: Autenticación, Autorización y Auditoría (Control de Acceso): Ing. Javier Jorge (INTI - UNC). Profesora ayudante: Lic. Alicia Dominga Mercedes Castro

Módulo 5: Gestión y operación de incidentes de ciberseguridad: Mgter.Ing. Miguel Solinas. Profesores ayudantes: Bachiller Universitaria Gina Commisso (12 h) y Bachiller Universitario Marcos Laureano Olocco (12 h).

Módulo 6: Gestión de riesgos de seguridad de la información: Dr. Fernando Menzaque (UNC)

Módulo 7: Aspectos de malware y modalidades de ciberataque: Lic. Alejandro Houspanossian (Trellix)

6.2. Coordinación general

El Coordinador General tendrá una carga horaria de 20 horas por mes y cobrará en 9 (nueve) cuotas, según lo especificado en el proyecto de presupuesto, para disminuir el impacto de la inflación. El Coordinador será el Dr. Marcos Oliva (FAMAF).

7. Selección de estudiantes

Requisitos de ingreso:

Estudios secundarios completo y para maximizar el aprendizaje, si bien no es necesario poseer un nivel de experto, es recomendable estar familiarizado con cada una de las áreas que a continuación se mencionan:

- Sistemas de numeración hexadecimal, decimal y binario.
- Suite de protocolos TCP/IP (TCP, UDP, IPv4, IPv6, HTTP, DNS, DHCP, ARP, Ethernet).
- Manejo básico de SO Windows y Linux.
- Conocimiento básico de componentes de redes tales como routers, switch, hub y bridge.

- Conceptos de dominios de colisión, dominios de broadcast.
- Entornos de trabajo, lenguajes de scripting y softskills.

Se proveerán materiales de autodiagnóstico y nivelación para que los candidatos sin formación reglada o sin práctica reciente puedan determinar si cumplen con los requisitos de ingreso para la Diplomatura y puedan administrar los contenidos necesarios para complementar su formación de base, si fuera necesario.

En el caso de que el número de inscripciones supere el número de vacantes, el Consejo Académico de la Diplomatura realizará un orden de méritos que publicará oportunamente.

Grilla metodológica

	Horas Teóricas	Horas Prácticas	Horas actividades autonómas	Total	CRE
Módulo 1: Criptografía aplicada	24	--	36	60	2,4
Módulo 2: Aspectos de seguridad en redes y servidores	24	24	12	60	2,4
Módulo 3: Seguridad en la Nube	24	--	36	60	2,4
Módulo 4: Autenticación, Autorización y Auditoría (Control de acceso)	18	18	9	45	1,8
Módulo 5: Gestión y operación de incidentes de ciberseguridad	24	24	12	60	2,4
Módulo 6: Gestión de riesgos de seguridad de la información	24	--	36	60	2,4
Módulo 7: Aspectos de malware y modalidades de ciberataque.	18	--	27	45	1,8
TOTAL	156	66	168	390	15,6