FUNDACIÓN INSTITUTO PROFESIONAL DUOC UC
VICERRECTORÍA ACADÉMICA
RESOLUCIÓN N°36/2024

APRUEBA DIPLOMADO EN CIBERSEGURIDAD AVANZADA

VISTOS:

1º. El proyecto presentado por la Directora de la Escuela de Informática y Telecomunicaciones.
2º. Lo previsto en el Instructivo para la Creación y Dictación de Diplomados, aprobado por Resolución de Vicerrectoría Académica N°04/2001, del 26 de abril de 2001.
3º. Las facultades previstas en el artículo 6° del Reglamento General.

RESUELVO:

Aprobar y tener como versión oficial y de aplicación general, el "Diplomado en Ciberseguridad Avanzada", cuyo texto se adjunta a continuación de esta resolución.

Comuníquese, publíquese y regístrese.

Santiago, agosto 23 de 2024.

Alejandra Silva Lafourcade
Firmado digitalmente por Alejandra Silva Lafourcade
Fecha: 2024.08.23 11:21:56 -04'00'

ALEJANDRA SILVA LAFOURCADE
DIRECTORA GENERAL DE DESARROLLO ESTUDIANTIL Y EDUCACIÓN CONTÍNUA

Kiyoshi Fukushi
Firmado digitalmente por Kiyoshi Fukushi
Fecha: 2024.08.23 12:26:34 -04'00'

KIYOSHI FUKUSHI MANDIOLA
VICERRECTOR ACADÉMICO

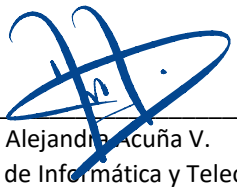
KFM/ASL//JMD/MCS

PRESENTACIÓN DE DIPLOMADO

Señor:
Kiyoshi Fukushi M.
Vicerrector Académico
Duoc UC

Alejandra Acuña V., Directora de la Escuela de Informática y Telecomunicaciones, presenta a la Vicerrectoría Académica, el **"Diplomado en Ciberseguridad Avanzada",** para formar parte de la oferta abierta de Educación Continua.

Agradeceré revisar y emitir la resolución correspondiente para poder ofertar dicho programa.



Alejandra Acuña V.
Directora Escuela de Informática y Telecomunicaciones
Duoc UC

DIPLOMADO EN CIBERSEGURIDAD AVANZADA

RESUMEN:

Diplomado de oferta abierta desarrollado por la Escuela de Informática y Telecomunicaciones. La ciberseguridad se ha convertido en una prioridad crítica para organizaciones de todos los sectores debido al aumento exponencial de la dependencia en sistemas informáticos para procesos productivos y funcionales. Este contexto ha resaltado la importancia de proteger los datos, considerados activos valiosos y vulnerables. Además, el alarmante incremento de ciberataques ha provocado pérdidas significativas de recursos y reputación para las compañías afectadas. Paralelamente, las normativas legales en ciberseguridad y protección de datos personales se han vuelto más estrictas, exigiendo la preparación de profesionales capacitados para cumplir con estos requisitos y proteger la información crítica de las organizaciones.

En respuesta a esta necesidad, el diplomado en Ciberseguridad Avanzada se presenta como una solución integral para formar especialistas capaces de enfrentar los desafíos actuales. En este sentido, este programa ofrece conocimientos profundos en conceptos clave como confidencialidad, integridad, disponibilidad, riesgo, amenaza y vulnerabilidades. Los participantes aprenderán a identificar riesgos y amenazas mediante la aplicación de marcos de referencia en la materia, fortaleciendo la protección de las organizaciones contra ataques y mejorando la seguridad de la información. Esta formación no solo aumenta la empleabilidad de los profesionales, sino que también contribuye a una mayor confianza en el uso de tecnologías digitales, generando un impacto positivo en la seguridad tanto personal como profesional.

El diplomado tiene una duración de 120 horas cronológicas, en modalidad asincrónica.

Para obtener el diplomado, los participantes deberán aprobar los cuatro cursos según la siguiente ponderación:

Nombre Módulos	Horas	% de la nota final de diplomado
Uso de técnicas y estrategias de ciberseguridad en la identificación y análisis de amenazas digitales	30	25%
Estrategias de seguridad defensiva en la protección de información	30	25%
Técnicas forenses y respuestas a incidentes de ciberseguridad	30	25%
Técnicas de evaluación de vulnerabilidades y pruebas de penetración (Ethical hacking)	30	25%
TOTAL DE HORAS	**120**	**100%**

Destinado a profesionales del área de informática, redes y/o telecomunicaciones, tales como: Ingenieros de Sistemas, SRE, DevOps, administradores de plataformas, redes o bases de datos, gerentes o subgerentes de TI, analistas de seguridad, hackers éticos blue o red team, arquitectos de software, jefes de proyectos TI, arquitectos y administradores de ciberseguridad, auditores, analistas de riesgos, desarrolladores de aplicaciones u otros roles relacionados con la ciberseguridad.

Javiera Munizaga D.
Subdirectora de Diseño de Programas Académicos
de Educación Continua

FICHA ÚNICA DE CREACIÓN DE DIPLOMADOS
PNCT

1. NOMBRE DEL DIPLOMADO

Diplomado en Ciberseguridad Avanzada

2. TOTAL DE HORAS

120

3. POBLACIÓN OBJETIVO

Destinado a analistas, arquitectos y administradores de ciberseguridad, auditores, analistas de riesgos, desarrolladores de aplicaciones y/o personas que hayan estudiado una carrera técnica o profesional relacionada, idealmente, con Informática, redes y/o telecomunicaciones. Así también, profesionales como Ingenieros de Sistemas, SRE, DevOps, administradores de plataformas, redes o bases de datos, gerentes o subgerentes de TI, analistas de seguridad, hackers éticos blue o red team, arquitectos de software, jefes de proyectos TI u otros roles relacionados con la entrega de productos o servicios digitales.

4. REQUISITOS DE INGRESO

Poseer conocimientos en uso de Sistemas operativos Linux y Windows, conocimientos básicos de programación en cualquier lenguaje, inglés nivel básico en nivel de lectura, modelo TCP/IP.

5. JUSTIFICACIÓN DE CREACIÓN

La ciberseguridad se ha convertido en una prioridad crítica para organizaciones de todos los sectores debido al aumento exponencial de la dependencia en sistemas informáticos para procesos productivos y funcionales. Este contexto ha resaltado la importancia de proteger los datos, considerados activos valiosos y vulnerables. Además, el alarmante incremento de ciberataques ha provocado pérdidas significativas de recursos y reputación para las compañías afectadas. Paralelamente, las normativas legales en ciberseguridad y protección de datos personales se han vuelto más estrictas, exigiendo la preparación de profesionales capacitados para cumplir con estos requisitos y proteger la información crítica de las organizaciones.

En respuesta a esta necesidad, el diplomado en Ciberseguridad Avanzada se presenta como una solución integral para formar especialistas capaces de enfrentar los desafíos actuales. En este sentido, este programa ofrece conocimientos profundos en conceptos clave como confidencialidad, integridad, disponibilidad, riesgo, amenaza y vulnerabilidades. Los participantes aprenderán a identificar riesgos y amenazas mediante la aplicación de marcos de referencia en la materia, fortaleciendo la protección de las organizaciones contra ataques y mejorando la seguridad de la información. Esta formación no solo aumenta la empleabilidad de los profesionales, sino que también contribuye a una mayor confianza en el uso de tecnologías digitales, generando un impacto positivo en la seguridad tanto personal como profesional.

6. OBJETIVO GENERAL/ IDENTIFICACIÓN PERFIL DE SALIDA

Desarrollar un marco integral de seguridad cibernética que incluya análisis de riesgos, estrategias defensivas, respuestas a incidentes y gestión de vulnerabilidades, utilizando herramientas de ethical hacking y protocolos de análisis forense digital.

7. UNIDAD ACADÉMICA

ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES

8. FECHA

3-7-2024

9. REQUISITOS DE OBTENCIÓN

9.1 - Haber aprobado todos los Cursos del Diplomado

Aprobar los cuatro cursos que componen el Diplomado.

9.2 - La distribución de la nota final de aprobación del diplomado se desglosa de la siguiente manera:

Nombre Curso	Horas	% de la nota final de Diplomado
Uso de técnicas y estrategias de ciberseguridad en la identificación y análisis de amenazas	30	25%
Estrategias de seguridad defensiva en la protección de información	30	25%
Técnicas forenses y respuestas a incidentes de ciberseguridad	30	25%

Técnicas de evaluación de vulnerabilidades y pruebas de penetración (Ethical hacking)	30	25%
	120	**100%**

Nota final (en caso que el Diplomado contemple una actividad evaluativa final)

El porcentaje asignado al curso y actividad evaluativa final debe ser establecido por la Unidad Académica

Porcentaje Asignado al curso	Porcentaje Asignado a la Actividad Evaluativa
100%	

10. MODALIDAD DE IMPARTICIÓN

	Modalidad
Presencial	
Semipresencial	
E-learning (asincrónico)	x

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso:	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
Uso de técnicas y estrategias de ciberseguridad en la identificación y análisis de amenazas digitales	50		30	Asincrónico

Identificación
Código SENCE
Código curso DuocUC

Unidad académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Escuela de Informática y Telecomunicaciones	Oscar Araya	Mayo, 2024

Especialista disciplinar	Diseñador(a) curricular	Diseñador(a) instruccional	Analista instruccional
Guillermo Farias	Noelia Escalona	Adleny Nieves	Javier Canales

Aporte de valor del programa (no SENCE)

La ciberseguridad se ha posicionado como un tema de gran relevancia en prácticamente todas las organizaciones, independientemente de su sector. El crecimiento de la dependencia de los sistemas informáticos en los procesos tanto productivos como funcionales de empresas e instituciones ha conferido un estatus crítico a los datos. Estos activos, cuyo valor aumenta constantemente, han generado una creciente demanda de profesionales altamente capacitados para su protección. Este incremento en el valor de los datos ha sido acompañado por un alarmante aumento en los ciberataques, los cuales provocan pérdidas significativas tanto de recursos como de reputación para las compañías afectadas.

Además de lo mencionado anteriormente, se agregan normativas legales cada vez más rigurosas en el ámbito de la ciberseguridad y la protección de datos personales a nivel nacional. Estas normativas requieren la preparación de profesionales capacitados para cumplirlas adecuadamente.

En consecuencia, los aprendizajes de este curso permitirán reconocer conceptos de confidencialidad, integridad, disponibilidad, riesgo, amenaza y vulnerabilidades, potenciando las habilidades y conocimientos de ciberseguridad, identificar riesgos y amenazas aplicando marcos de referencia en la materia, pudiendo robustecer la protección de organizaciones ante amenazas, la identificación de vulnerabilidades y de esta forma apoyar la protección de la información crítica y sistemas de información , generado una mejora sustancial en la seguridad personal y profesional y mayor confianza en el uso de las tecnologías digitales.

Caracterización del participante

El curso de Ciberseguridad está dirigido a profesionales, que cumplen roles Ingenieros de Sistemas, SRE, DevOps, Administradores de plataformas, redes o bases de datos, Gerentes o Subgerentes de TI, Analistas de seguridad, Hackers éticos blue o red team, Arquitectos de software, jefes de proyectos TI u otros roles relacionados con la entrega de productos o servicios digitales.

Requisitos de ingreso del participante

Poseer conocimientos en:

- Uso de Sistemas operativos Linux y Windows.
- Conocimientos básicos de programación en cualquier lenguaje.
- Inglés nivel básico en nivel de lectura.

- Modelo TCP/IP.

Requisitos técnicos del participante
Sistema Operativo Windows 10 o superior; iOS 11 o posterior Memoria RAM: 16 GB o más Procesador: velocidad de 2 GHz o superior Tarjeta de sonido Resolución de monitor: 1024 x 768 o superior. Navegadores Recomendados: Google Crome (última versión), Mozilla Firefox (última versión), Microsoft Edge Cámara, micrófono, parlantes y/o audífonos Lector de PDF, como Adobe Acrobat Reader (adobe.com) o Foxit Reader (foxit.com) Conexión a Internet de mínimo 10 horas a la semana y de 12mbps o más para una adecuada experiencia de videoconferencia y visualización de recursos de aprendizaje (para medir la velocidad de su enlace a internet, puede visitar la página http://www.speedtest.net/).

Objetivo general
Desarrollar un análisis de riesgos de acuerdo con las amenazas y vulnerabilidades de una organización.

Unidades	Objetivo específico	Contenidos	Horas	
			T	P
Unidad 1: Conceptos y Normativas de seguridad informática	Identificar conceptos, normas y estándares de seguridad informática, de acuerdo con las necesidades de una organización.	Fundamentos de la seguridad informática: • Triada de la seguridad. • Amenazas, vulnerabilidades y riesgos. • Matriz de riesgos. • Modelo de Zero Trust. Normas y estándares de cibersegurdad: • Estándar ISO/IEC 27000. • Ley de delitos Informáticos. • Ley Marco de Ciberseguridad. • Ley de protección de datos personales.	4	6
Unidad 2: Vulnerabilidades y amenazas	Aplicar herramientas de análisis de vulnerabilidades y amenazas de ciberseguridad en la infraestructura TI de una organización.	Análisis y Gestión de Vulnerabilidades: • Clasificación y Scoring de Vulnerabilidades (CVSS). • Herramientas y técnicas de análisis de vulnerabilidades. Detección de amenazas e intrusiones: • Modelo de amenaza STRIDE. • OWASP TOP TEN WEB. • Framework MITRE Att&ck.	8	12
		Subtotal	12	18
		Horas totales	30	

Estrategias metodológicas
La estrategia metodológica de este curso corresponde a la auto instrucción, considerando el diseño del curso en una modalidad 100% online a través del Ambiente Virtual de Aprendizaje (AVA) establecido por Duoc UC. El proceso de enseñanza/aprendizaje se desarrollará a través de diversos recursos que estarán dispuestos de forma ordenada en el AVA, permitiendo maximizar la accesibilidad y la efectividad del aprendizaje, al proporcionar una estructura clara y coherente que permite a los participantes navegar fácilmente por el contenido del curso. Con la finalidad de que los participantes adquieran el conocimiento de manera significativa, dinámica y contextualizada, se diseñarán recursos de enseñanza/aprendizaje considerando una secuencia que permita activar los conocimientos previos y poder vincularlos con nuevas ideas, demostrar o contextualizar los contenidos en escenarios lo más reales posibles, aplicar lo aprendido a través de evaluaciones formativa o sumativas a través de metodología como análisis de casos y problemas representativos de la realidad laboral de los participantes, y, finalmente, promover la integración de los aprendizajes, facilitando que los conocimientos adquiridos se consoliden y se puedan aplicar de manera efectiva en situaciones reales, reforzando así la capacidad de los participantes para enfrentar desafíos profesionales en sus puestos de trabajo. El curso tiene 2 unidades de contenidos, distribuidas en 6 semanas, que permiten realizar un recorrido desde lo general a lo particular. La unidad 1 tiene como objetivo identificar conceptos, normas y estándares de seguridad informática, de acuerdo con las necesidades de una organización. Se abordará la identificación de conceptos básicos de ciberseguridad y normativas vigentes, permitiendo que los y las participantes puedan comprender de manera correcta elementos clave de la ciberseguridad en contextos organizacionales. Para ello se utilizará una metodología basada en preguntas a través de cuestionarios establecidos en el AVA con retroalimentación automática. La unidad 2 tiene por objetivo aplicar herramientas de análisis de vulnerabilidades y amenazas de ciberseguridad en componentes de la infraestructura TI de una organización, por lo tanto, se profundizará sobre la aplicación de herramientas de análisis de vulnerabilidades y amenazas, logrando que los participantes no sólo aprendan a identificar y medir riesgos asociados a través de CVSS, sino que también puedan analizar amenazas identificando tácticas y estrategias a través de la aplicación de diversas herramientas. Para ello, se utilizará una metodología basada en casos, donde los participantes deberán resolver una serie de encargados relacionados con la disciplina, utilizando herramientas de ciberseguridad, por ejemplo, frameworks y marcos de trabajo que permitan resolver las solicitudes de manera correcta.

Estrategias evaluativas		
Criterios de evaluación:	**Instrumentos de evaluación:**	**Normas de aprobación:**
Evaluación diagnóstica		
• Identifica el concepto de disponibilidad. • Identifica el concepto de integridad. • Identifica el concepto de confidencialidad. • Diferencia entre riesgo, amenaza y vulnerabilidad. • Reconoce marcos de trabajo o herramientas.	Al comenzar el curso, se realizará una evaluación diagnóstica por medio de definiciones de conceptos claves durante la primera sesión, con el fin de consensuar el nivel de conocimientos previos de los participantes. Evaluado mediante una prueba de alternativas disponible en sistema.	Esta evaluación no tiene ponderación.
Unidad 1		

• Identifica conceptos y normativas de ciberseguridad. • Diferencia los conceptos de amenaza, vulnerabilidad y riesgo. • Identifica riesgos de ciberseguridad. • Identifica aspectos de normativas en caso.	La evaluación se desarrollará a través de un detallado caso de estudio que presentará una serie de preguntas de opción múltiple, todas ellas relacionadas con el caso expuesto. Este enfoque permitirá a los participantes no solo demostrar la comprensión de los conceptos teóricos, sino también aplicarlos de manera práctica en un contexto realista.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 30%.**
Unidad 2		
• Reconoce vulnerabilidades en un escenario aplicado. • Reconoce amenazas en un escenario. • Aplica herramientas de análisis de amenazas de ciberseguridad en componentes de la infraestructura TI de una organización. • Reconoce tácticas y técnicas asociadas a amenazas. • Aplica modelo CVSS para determinar el nivel de riesgo de una vulnerabilidad. • Analiza vulnerabilidades en componentes de la infraestructura TI de una organización usando herramientas de análisis vulnerabilidades.	En esta evaluación el participante deberá aplicar calculadora CVSS en la identificación de vulnerabilidades y amenazas, de tal forma que pueda establecer el nivel de riesgo de vulnerabilidad, a partir de un caso práctico. Esta prueba será evaluada por medio de una **rúbrica.**	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 30%.**
Evaluación Final		
• Aplica CVSS para establecer el nivel de riesgo de una vulnerabilidad. • Diferencia entre Riesgos, amenaza y vulnerabilidad, según marco OWASP TOP TEN • Describe tácticas Mitre Att&ck asociadas a amenazas y/o vulnerabilidades. • Aplica técnicas Mitre Att&ck para identificar amenazas y/o vulnerabilidades.	La evaluación final consiste en el desarrollo de un análisis de riesgos de acuerdo con las amenazas y vulnerabilidades de un caso práctico. Este análisis será evidenciado a través de un informe. Esta prueba será evaluada por medio de una **rúbrica**. El caso usado en esta evaluación necesita que el participante aplique los conocimientos con mayor profundidad relacionándolo a marcos específicos y además necesita relacionar elementos del caso para completar eficientemente la identificación de Amenazas, Vulnerabilidades y riesgos, debiendo además estructura el resultado	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 40%.**

• Utiliza categorías de STRIDE para identificar amenazas	para una comunicación eficiente en un informe.	
	INSTRUMENTO PARA SENCE: Evaluación diagnostica mediante cuestionario de selección múltiple medido con pauta de evaluación. Evaluaciones parciales: - Unidad 1: Mediante caso con cuestionario medido con pauta de evaluación. - Unidad 2: Mediante caso medido con rubrica. Evaluación Final: mediante informe y caso medido con rubrica.	

Requisito de aprobación	
Modalidad presencial	Asistencia Mínima de 75% de las horas totales del curso y nota mínima de aprobación 4.0
Modalidad sincrónica - asincrónica	Conectividad sobre un 75% y nota mínima de aprobación 4.0

Recursos para la implementación del curso					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
Características de la infraestructura requerida para la ejecución del curso. Definir y dejar establecidos los insumos, herramientas, materiales o equipos que se necesitan para llevar a cabo de forma exitosa el curso.	**Dónde se impartirá el curso** ***Anexo ficha de costos**	**Indicar cantidad**	**Tipo de equipo y/o herramienta para la implementación del curso** ***Indicar duración de licencias o equipamientos.**	**Indicar cantidad**	**Indicar el material que se requiere para la implementación del curso**
Plataforma LMS Blackboard. Sistema de videoconferencia online Collaborate integrado a plataforma.	Curso de modalidad remota asincrónica	1 1 1 1 1	Escritorio Computador Cámara Micrófono Silla ergonómica	1 1	Material en formato digital - OWASP - MITRE ATT&CK - CVSS - Normativa, Ley 21.459, Ley 21.663

Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Escuela)
Máximo dos años

Articulación *Sección a completar por Subdirector(a)		**Código/Sigla/Nombre Certificado**
Programa Regular o EDC	**Escuela**	

Diplomado: En caso de que el curso pertenezca a un diplomado, se deberá indicar el nombre del diplomado, y el nombre de todos los cursos de diplomado, en el orden que corresponda.	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
Diplomado en Ciberseguridad avanzada	**Estrategias de seguridad defensiva en la protección de información**
Diplomado en Ciberseguridad avanzada	**Técnicas Forenses y Respuesta a Incidentes de ciberseguridad**
Diplomado en Ciberseguridad avanzada	**Evaluación de Vulnerabilidades y Pruebas de Penetración (Ethical hacking)**

Otros cursos relacionados con la temática Incluir cursos que tengamos diseñados y que se relacionen con la temática, por ejemplo, si la PNCT corresponde a un curso de Excel avanzado, en este apartado se puede incluir el curso de: Power BI avanzando

Recursos docentes: Perfil desarrollador	
Profesión	Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines.
Años de experiencia	4 años
Conocimientos y habilidades relevantes	Experiencia en proyectos de seguridad en TI, experiencia en educación superior, habilidades de relatoría, Certificaciones deseables en ISO27001, CEH o equivalentes.
Observaciones Describir el perfil del profesional que puede diseñar/actualizar este curso, no de la persona que lo está diseñando en este momento.	

Recursos docentes: Perfil relator	
Profesión	Profesional dedicado a la ciberseguridad, idealmente, Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines, entre otros especialistas.
Años de experiencia	2-3 años
Conocimientos y habilidades relevantes	Experiencia en proyectos de seguridad en TI como analista de seguridad, habilidades de relatoría, Certificaciones deseables CEH, eJPT o equivalentes.
Observaciones Describir el perfil teniendo presente que será el profesional responsable de desarrollar la relatoría del curso.	

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso:	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
Estrategias de seguridad defensiva en la protección de información	50		30	Asincrónico

Identificación
Código SENCE
Código curso DuocUC

Unidad académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Escuela de Informática y Telecomunicaciones	Oscar Araya	Mayo, 2024

Especialista disciplinar	Diseñador(a) curricular	Diseñador(a) instruccional	Analista instruccional
Nicolás Contador	Noelia Escalona	Adleny Nieves	Javier Canales

Aporte de valor del programa (no SENCE)

La creciente interdependencia entre la tecnología y los negocios ha transformado drásticamente el panorama empresarial, generando una demanda sin precedentes de profesionales altamente capacitados en ciberseguridad defensiva. Este cambio se debe en gran parte al aumento exponencial del intercambio de datos en el entorno digital y a la proliferación de amenazas cibernéticas sofisticadas que buscan explotar cualquier vulnerabilidad en los sistemas informáticos.

En este contexto, la detección y mitigación efectiva de las brechas de seguridad se ha convertido en una prioridad crítica para las organizaciones de todos los sectores. La pérdida o compromiso de datos sensibles puede tener consecuencias devastadoras, tanto en términos financieros como de reputación. Por lo tanto, la capacidad de proteger los activos de información se ha vuelto esencial para garantizar la continuidad operativa y la confianza del cliente.

Para hacer frente a este desafío, se presenta este curso especializado en ciberseguridad defensiva. Diseñado con un enfoque práctico y orientado a resultados, el programa proporcionará a los participantes herramientas y habilidades para enfrentar los complejos desafíos de seguridad cibernética de las organizaciones actualmente.

Caracterización del participante

Analistas de ciberseguridad, técnicos e ingenieros de ciberseguridad, auditores, analistas de riesgos y/o personas que hayan estudiado una carrera afín en Informática, redes o telecomunicaciones.

Requisitos de ingreso del participante

Poseer conocimientos en:

- Uso de Sistemas operativos Linux y Windows.
- Conocimientos básicos de programación en cualquier lenguaje.
- Inglés nivel básico en nivel de lectura.
- Modelo TCP/IP.

Requisitos técnicos del participante

Sistema Operativo Windows 10 o superior; iOS 11 o posterior
Memoria RAM: 16 GB o más

Procesador: velocidad de 2 GHz o superior Tarjeta de sonido Resolución de monitor: 1024 x 768 o superior. Navegadores Recomendados: Google Crome (última versión), Mozilla Firefox (última versión), Microsoft Edge Cámara, micrófono, parlantes y/o audífonos Lector de PDF, como Adobe Acrobat Reader (adobe.com) o Foxit Reader (foxit.com) Conexión a Internet de mínimo 10 horas a la semana y de 12mbps o más para una adecuada experiencia de videoconferencia y visualización de recursos de aprendizaje (para medir la velocidad de su enlace a internet, puede visitar la página http://www.speedtest.net/).

Objetivo general
Desarrollar una estrategia de seguridad defensiva de acuerdo con la detección temprana de ciberamenzas.

Unidades	**Objetivo específico**	**Contenidos**	**Horas**	
			T	**P**
Unidad 1: Fundamentos de Seguridad defensiva	Identificar los tipos de ataques cibernéticos de acuerdo con sus características distintivas.	Introducción a la Seguridad Defensiva: • Definición de seguridad defensiva. • Importancia de la seguridad defensiva en un entorno cibernético. Security Operations Center (SOC): • Funciones y roles dentro de un SOC. • Procesos y procedimientos operativos en un SOC. • Herramientas utilizadas en un SOC. Cyber Kill Chain: • Concepto y fases de la Cyber Kill Chain. • Utilidad de la Cyber Kill Chain en la detección y respuesta a amenazas. Detección de Ataques: • Técnicas y herramientas para la detección de ataques cibernéticos. • Análisis de indicadores de compromiso (IOC) y firmas de ataques. • Implementación de controles para la detección temprana de ataques.	4	6
Unidad 2: Tecnologías de un Centro de Cyber Operaciones	Aplicar tecnológicas de detección de ciberataques de acuerdo con el estándar de funcionamiento de un centro de operaciones de seguridad (SoC).	Implementación y uso de un SIEM: • Instalación una solución SIEM. • Configuración y despliegue un SIEM. • Agrega y registra agentes. Implementación de NIDS:	5	15

		• Implementación y configuración de un sistema de detección de intrusiones basado en red. • Integración de NIDS al SIEM. Análisis de malware. Cyber Threat Intelligence: • Recopilar, analizar y utilizar herramientas y plataformas de inteligencia de amenazas. • Identificar fuentes de inteligencia. • Evaluar la credibilidad de la información.		
		Subtotal	12	18
		Horas totales	30	

Estrategias metodológicas
La estrategia metodológica de este curso se basa en la auto instrucción, diseñado para ser completamente online a través del Ambiente Virtual de Aprendizaje (AVA) de Duoc UC. El proceso de enseñanza/aprendizaje se desarrollará mediante diversos recursos organizados de forma ordenada en el AVA, maximizando la accesibilidad y la efectividad del aprendizaje. La estructura clara y coherente del curso permite a los participantes navegar fácilmente por el contenido. Con el objetivo de que los participantes adquieran conocimientos de manera significativa, dinámica y contextualizada, se diseñarán recursos de enseñanza/aprendizaje con una secuencia que active conocimientos previos y los vincule con nuevas ideas. Los contenidos se demostrarán o contextualizarán en escenarios lo más reales posibles, permitiendo aplicar lo aprendido mediante evaluaciones formativas y sumativas a través de metodologías como el análisis de casos y problemas representativos de la realidad laboral de los participantes. Finalmente, se promoverá la integración de los aprendizajes, facilitando que los conocimientos adquiridos se consoliden y puedan aplicarse de manera efectiva en situaciones reales, reforzando así la capacidad de los participantes para enfrentar desafíos profesionales en sus puestos de trabajo. El curso consta de dos unidades: En la primera unidad, se abordarán los conceptos clave de un centro de operaciones de ciberseguridad (SoC) a través de recursos de auto instrucción, como videos y guías. Se estudiarán el modelo de ataque Cyber Kill Chain, la matriz de tácticas y técnicas de MITRE ATT&CK Framework, y las técnicas de análisis de phishing y detección de ataques cibernéticos. Estos conocimientos se pondrán en práctica mediante una metodología basada en preguntas, utilizando cuestionarios con retroalimentación automática en el AVA. La segunda unidad busca que los participantes apliquen herramientas y plataformas de análisis para la implementación de un Sistema de Gestión de Eventos e Información de Seguridad (SIEM) para la detección y respuesta a incidentes. Se utilizará una metodología basada en problemas y análisis de casos basados en contextos reales de la disciplina, favoreciendo el proceso de aprendizaje y el posterior uso de los conocimientos adquiridos en el puesto de trabajo.

El curso considera el uso de simulaciones y ejercicios prácticos, donde los participantes podrán practicar técnicas de análisis y detección. Esto puede incluir ejercicios de laboratorio virtual donde los estudiantes interactúen con entornos simulados de red y sistemas comprometidos, como Atomic Red Team y testmynids.

Estrategias evaluativas		
Criterios de evaluación:	**Instrumentos de evaluación:**	**Normas de aprobación:**
Evaluación diagnóstica		
• Identifica estrategias elementales de seguridad defensiva. • Identifica las características de la detección temprana de ciberamenazas. • Diferencia la implementación y uso de un SIEM de la implementación de un NIDS. • Reconoce los pasos para una instalación de una solución SIEM.	La evaluación diagnóstica se realizará al inicio del curso. Se enfocará en reconocer los conocimientos previos de los participantes en torno a los conceptos y contenidos elementales de estrategias de seguridad defensiva, basadas en la detección temprana de ciberamenazas. Se presentará en un formato cuestionario, con 10 reactivos de selección múltiple simple, 4 distractores, respuesta y retroalimentación automatizada.	Esta evaluación no tiene ponderación.
Unidad 1		
• Reconoce la importancia de la seguridad defensiva en un entorno cibernético. • Identifica amenazas cibernéticas como ataques a activos de conformación, tácticas, técnicas y procedimientos. • Identifica los procesos y procedimientos en un Soc y las herramientas que se utilizan. • Comprende el concepto y fases de la Cyber Kill Chain, además de su utilidad. • Identifica técnicas y herramientas para la detección de ataques cibernéticos. • Comprende la importancia de la implementación de controles para la detección temprana de ataques.	En esta evaluación los estudiantes realizarán una evaluación de selección simple que considera un caso de estudio basado en cuatro áreas clave: Seguridad defensiva, Introducción a la Seguridad Defensiva, Security Operations Center (SOC), Cyber Kill Chain, Detección de Ataques. La prueba considera 20 preguntas de selección múltiple simple, cada pregunta contendrá 4 distractores y ofrecerá respuestas y retroalimentación automatizadas.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 30%.**
Unidad 2		

• Identifica fuentes de amenazas. • Analiza herramientas y plataformas de inteligencia de amenaza. • Aplica herramientas y plataformas de inteligencia de amenaza. • Aplica las herramientas y tecnologías de gestión de alertas y detección de intrusiones en una red virtual o física. • Utiliza las herramientas y plataformas de inteligencia de amenazas y análisis de malware.	Se aplicará una evaluación grupal, basada en la resolución de problemas, en donde los participantes deberán aplicar las máquinas virtuales y/o tecnologías de detección de amenazas para realizar el levantamiento de un diagnóstico de alertas de seguridad y se deberá entregar el informe de la aplicación del proceso. Se evaluará la instalación, en máquinas virtuales, de un SIEM, un IDS y su integración a la plataforma, y agentes del SIEM, además del análisis dinámico de una muestra de malware y del análisis de alertas y generación de indicadores de compromiso, en plataformas de inteligencia de ciberamenazas. Esta prueba será evaluada por medio de una **rúbrica.**	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 30%.**
Evaluación Final		
• Utilizar herramientas y plataformas para la obtención del diagnóstico de gestión de alertas. • Utiliza la plataforma SIEM para la detección de amenazas y gestión de eventos e información de seguridad. • Analiza el resultado de las alertas en plataformas de inteligencia de ciberamenazas, para determinar su veracidad y categorización. • Desarrolla estrategias de seguridad defensiva que permitan el resguardo de la información.	El trabajo final es de carácter individual. A partir del diagnóstico de gestión de alertas, el participante entregará un informe que contemple las evidencias del análisis e investigación de las alertas recibidas en la plataforma SIEM, utilizando herramientas y tecnologías de inteligencia de ciberamanenazas y de detección de intrusiones. Además de las estrategias de seguridad defensivas para la protección de la información, según el caso, para que el cliente evalúe su aplicación o no. Esta prueba será evaluada por medio de una **rúbrica.**	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 40%.**
	INSTRUMENTO PARA SENCE: Evaluación diagnostica mediante cuestionario de selección múltiple medido con pauta de evaluación. Evaluaciones parciales: - Unidad 1: Mediante caso con cuestionario medido con pauta de evaluación. - Unidad 2: Mediante caso medido con rubrica.	

	Evaluación Final: mediante informe y caso medido con rubrica.	
Requisito de aprobación		
Modalidad presencial	Asistencia Mínima de 75% de las horas totales del curso y nota mínima de aprobación 4.0	
Modalidad sincrónica - asincrónica	Conectividad sobre un 75% y nota mínima de aprobación 4.0	

Recursos para la implementación del curso					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
Características de la infraestructura requerida para la ejecución del curso. Definir y dejar establecidos los insumos, herramientas, materiales o equipos que se necesitan para llevar a cabo de forma exitosa el curso.	**Dónde se impartirá el curso** ***Anexo ficha de costos**	**Indicar cantidad**	**Tipo de equipo y/o herramienta para la implementación del curso** ***Indicar duración de licencias o equipamientos.**	**Indicar cantidad**	**Indicar el material que se requiere para la implementación del curso**
Plataforma LMS Blackboard. Sistema de videoconferencia online Collaborate integrado a plataforma.	Curso de modalidad remota asincrónica	1 1 1 1 1	Escritorio Computador Cámara Micrófono Silla ergonómica	1 1	Se utilizará material y portales gratuitos.

Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Escuela)
Máximo dos años

Articulación *Sección a completar por Subdirector(a)		**Código/Sigla/Nombre Certificado**
Programa Regular o EDC	**Escuela**	

Diplomado: En caso de que el curso pertenezca a un diplomado, se deberá indicar el nombre del diplomado, y el nombre de todos los cursos de diplomado, en el orden que corresponda.	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
Diplomado en Ciberseguridad Avanzada	**Uso de técnicas y estrategias de ciberseguridad en la identificación y análisis de amenazas digitales**
Diplomado en Ciberseguridad Avanzada	**Técnicas forenses y respuesta a incidentes**
Diplomado en Ciberseguridad Avanzada	**Evaluación de Vulnerabilidades y Pruebas de Penetración (Ethical hacking)**

Otros cursos relacionados con la temática Incluir cursos que tengamos diseñados y que se relacionen con la temática, por ejemplo, si la PNCT corresponde a un curso de Excel avanzado, en este apartado se puede incluir el curso de: Power BI avanzando

Recursos docentes: Perfil desarrollador	
Profesión	Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines.
Años de experiencia	4 años
Conocimientos y habilidades relevantes	Experiencia en proyectos de seguridad en TI, experiencia en educación superior, habilidades de relatoría, Certificaciones deseables en ISO27001, CEH o equivalentes.
Observaciones Describir el perfil del profesional que puede diseñar/actualizar este curso, no de la persona que lo está diseñando en este momento.	

Recursos docentes: Perfil relator	
Profesión	Profesional dedicado a la ciberseguridad, idealmente, Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines, entre otros especialistas.
Años de experiencia	2-3 años
Conocimientos y habilidades relevantes	Experiencia en proyectos de seguridad en TI como analista de seguridad, habilidades de relatoría, Certificaciones deseables CEH, eJPT o equivalentes.
Observaciones Describir el perfil teniendo presente que será el profesional responsable de desarrollar la relatoría del curso.	

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso:	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
Técnicas Forenses Y Respuesta A Incidentes de Ciberseguridad	50		30	Asincrónico

Identificación
Código SENCE
Código curso DuocUC

Unidad académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Escuela de Informática y Telecomunicaciones	Oscar Araya	Mayo/2024

Especialista disciplinar	Diseñador(a) curricular	Diseñador(a) instruccional	Analista instruccional
Jaime Gómez	Noelia Escalona	Paula Doenitz	Javier Canales

Aporte de valor del programa (no SENCE)

La creciente dependencia de los sistemas informáticos para llevar a cabo operaciones, almacenar datos sensibles, comunicarse con usuarios y colaboradores, así como proteger información confidencial, expone a las entidades a mayores riesgos de amenazas cibernéticas. Hoy en día, las organizaciones enfrentan una amplia gama de riesgos, desde ataques aislados hasta acciones sofisticadas de ciberdelincuencia. Es necesario analizar, peritar y comprender estos incidentes para tomar medidas correctivas, prevenir futuros ataques y mitigar sus impactos, al tiempo que se preserva la confianza y reputación de la entidad.

En este contexto, el curso propuesto permitirá a los participantes adquirir competencias generales para comprender los conceptos fundamentales de las técnicas forenses y la respuesta a incidentes en ciberseguridad. También aprenderán a diferenciar los tipos de ciberataques, a aplicar técnicas de investigación de incidentes y manejo de evidencias según los protocolos establecidos, y a reconocer estrategias para responder a incidentes de seguridad cibernética. La instancia ofrece una oportunidad para mejorar la empleabilidad del participante y enfrentar los desafíos de seguridad cibernética en el mercado laboral actual, junto con contribuir a mejorar la transparencia de la información y fortalecer la confianza de usuarios y colaboradores en las diversas entidades públicas y privadas.

Caracterización del participante

Analistas, arquitectos y administradores de ciberseguridad, auditores, analistas de riesgos, desarrolladores de aplicaciones y/o personas que hayan estudiado una carrera afín en Informática, redes o telecomunicaciones.

Requisitos de ingreso del participante

Poseer conocimientos en:

- Uso de Sistemas operativos Linux y Windows.
- Conocimientos básicos de programación en cualquier lenguaje.
- Inglés nivel básico en nivel de lectura.
- Conocimiento en uso de virtualbox o vmware Workstation.
- Modelo OSI, TCP/IP, direccionamiento IP.

Requisitos técnicos del participante

Sistema Operativo Windows 10 o superior; iOS 11 o posterior Memoria RAM: 16 GB o más Procesador: velocidad de 2 GHz o superior Tarjeta de sonido Resolución de monitor: 1024 x 768 o superior. Navegadores Recomendados: Google Crome (última versión), Mozilla Firefox (última versión), Microsoft Edge Cámara, micrófono, parlantes y/o audífonos Lector de PDF, como Adobe Acrobat Reader (adobe.com) o Foxit Reader (foxit.com) Conexión a Internet de mínimo 10 horas a la semana y de 12mbps o más para una adecuada experiencia de videoconferencia y visualización de recursos de aprendizaje (para medir la velocidad de su enlace a internet, puede visitar la página http://www.speedtest.net/).

Objetivo general
Diseñar acciones de respuesta a incidentes de ciberseguridad basados en protocolos análisis forense digital.

Unidades	**Objetivo específico**	**Contenidos**	**Horas**	
			T	**P**
Unidad 1: Análisis Forense Digital.	Aplicar técnicas de análisis forense digital en incidentes de seguridad informática	Proceso de investigación forense: • Conceptos generales de investigación forense. • Herramientas y técnicas de investigación. • Adquisición de Data. • Presentación de evidencias. Análisis forense digital: • Análisis Forense de Sistemas Operativos. • Análisis Forense de Red. • Análisis de malware. • Hunting.	4	6
Unidad 2: Respuesta a incidentes.	Aplicar técnicas de respuesta a incidentes de seguridad informática.	Proceso de respuesta a incidentes de ciberseguridad. Respuestas a incidentes: • Respuesta a incidentes Web. • Respuesta a incidentes de malware. • Respuesta a incidentes de correo electrónico. • Respuesta a incidentes Cloud. Mitigación de efectos de incidentes de ciberseguridad.	5	15
		Subtotal	10	20
		Horas totales	30	

Estrategias metodológicas
La estrategia metodológica de este curso se basa en la auto instrucción, implementada a través del Ambiente Virtual de Aprendizaje (AVA) de Duoc UC, en una modalidad 100% online. El proceso de enseñanza/aprendizaje se desarrollará mediante diversos recursos organizados en el AVA, optimizando la accesibilidad y la efectividad del aprendizaje al proporcionar una estructura clara y coherente que facilita la navegación por el contenido del curso. Con el objetivo de que los participantes adquieran el conocimiento de manera significativa, dinámica y contextualizada, se diseñarán recursos de enseñanza/aprendizaje con una secuencia que active los conocimientos previos y los vincule con nuevas ideas, demuestre o contextualice los contenidos en escenarios realistas, y permita la aplicación de lo aprendido mediante evaluaciones formativas o sumativas. Se utilizarán metodologías como el análisis de casos y problemas representativos de la realidad laboral de los participantes. Esto promoverá la integración de los aprendizajes, facilitando que los conocimientos adquiridos se consoliden y puedan aplicarse de manera efectiva en situaciones reales, reforzando así la capacidad de los participantes para enfrentar desafíos profesionales en sus puestos de trabajo. El curso se estructurará en dos unidades a lo largo de seis semanas. En la primera unidad, se establecerán las bases para comprender las técnicas, herramientas y procedimientos de Análisis Forense Digital. Para ello, se emplearán herramientas de enseñanza como cuestionarios formativos y casos prácticos. Los participantes responderán a diversos enunciados en el aula virtual (AVA), utilizando máquinas virtuales para identificar las alternativas correctas. Estas actividades permitirán a los participantes aplicar los conceptos teóricos en un entorno simulado, facilitando el aprendizaje práctico de las técnicas de análisis forense digital. En la unidad 2 de Respuesta a Incidentes, se profundizará en el proceso de respuesta a incidentes de ciberseguridad y la mitigación de sus efectos. Se utilizará una metodología basada en problemas, donde los participantes abordarán situaciones hipotéticas contextualizadas en la temática del curso. Los participantes deberán responder a una serie de enunciados en el aula virtual (AVA). Estas actividades permitirán aplicar conocimientos teóricos a situaciones prácticas, utilizando herramientas de simulación y análisis disponibles en el AVA para evaluar y mitigar incidentes de ciberseguridad de manera efectiva. Al finalizar el curso, los participantes deberán ser capaces de evaluar técnicas de análisis forense digital y estrategias de respuesta a incidentes de ciberseguridad en casos aplicados, analizando la pertinencia de los procedimientos, así como la correcta gestión de respuestas a incidentes.

Estrategias evaluativas		
Criterios de evaluación:	**Instrumentos de evaluación:**	**Normas de aprobación:**
Evaluación diagnóstica		
• Identifica el concepto de investigación forense. • Identifica las áreas críticas de infraestructura tecnológica de la información susceptible a ataques de ciberseguridad.	La evaluación diagnóstica se realizará al inicio del curso. Se enfocará en reconocer los conocimientos previos de los participantes en torno a los conceptos y contenidos elementales de ciberseguridad, técnicas de análisis forense y respuesta a incidentes. Se presentará en un formato cuestionario, con 10 reactivos de selección	Esta evaluación no tiene ponderación.

• Reconoce el concepto análisis de Data en el marco de la ciberseguridad. • Reconoce los conceptos asociados al manejo de incidentes de ciberseguridad.	múltiple simple, 4 distractores, respuesta y retroalimentación automatizada.	
Unidad 1		
• Identifica conceptos generales del proceso de investigación forense en un escenario aplicado. • Compara técnicas de análisis forense y presentación de evidencias digitales entre tecnologías de información. • Aplica herramientas de investigación y adquisición de DATA de evidencias digitales. • Aplica acciones detección de amenazas en los sistemas de una organización.	La evaluación se realizará en base a casos de estudio, que presentarán escenarios de problemáticas donde se verán amenazados los sistemas digitales de una o más organizaciones. Para la gestión de los casos se usarán máquinas virtuales, como parte de un entorno controlado donde los participantes resolverán problemas específicos y a través de su gestión obtendrán las respuestas para responder al cuestionario de 20 reactivos de selección múltiple simple y compleja, 4 distractores, respuesta y retroalimentación automatizada. En la evaluación se presentarán antecedentes sobre la identificación de conceptos generales, herramientas de investigación para la recuperación de datos, reconstrucción de eventos y análisis de DATA. Junto con la mención a técnicas de análisis forense de distintas tecnologías de información y presentación de evidencias.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 30%.**
Unidad 2		
• Compara la efectividad de los sistemas de seguridad digital mediante técnicas de análisis forense y presentación de evidencias aplicada a distintas tecnologías de información. • Opera acciones detección de amenazas en los sistemas de una organización, mediante herramientas de investigación y adquisición de DATA de evidencias digitales. • Aplica la matriz de análisis en la identificación y priorización de los riesgos de seguridad de la información en una	La evaluación se centrará en el análisis de casos de estudio que abordan el proceso de respuesta a incidentes de ciberseguridad en una o más organizaciones. Estos casos de estudio explorarán ejemplos de respuestas a incidentes web, malware, correo electrónico y Cloud, ofreciendo un panorama amplio de las amenazas y desafíos que enfrentan las organizaciones en el ámbito de la ciberseguridad. Además de examinar las respuestas a los incidentes, se destacarán estrategias de mitigación para minimizar los efectos adversos de futuros incidentes de seguridad. Los estudiantes, como parte de la evaluación, deberán crear un entregable en forma de matriz de análisis. Esta matriz simulará una situación de trabajo real, donde se identificarán y priorizarán los riesgos de seguridad de la información dentro de una organización. Esta herramienta permitirá a	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. Se mantiene, **Esta evaluación tiene una ponderación de un 30%.**

organización, considerando diferentes escenarios de amenazas. • Registra controles de prevención de incidentes de acuerdo con el contexto de la organización. • Analiza los resultados de la matriz de análisis, destacando los riesgos críticos que requieren una atención inmediata.	los responsables de seguridad y a los tomadores de decisiones comprender mejor las amenazas y los posibles impactos en la seguridad de los activos de información, fomentando así la toma de decisiones informadas y estratégicas en materia de ciberseguridad.	
Evaluación final		
• Aplica CVSS para establecer el nivel de riesgo de una vulnerabilidad. • Diferencia entre Riesgos, amenaza y vulnerabilidad, según marco OWASP TOP TEN. • Describe tácticas Mitre Att&ck asociadas a amenazas y/o vulnerabilidades. • Aplica técnicas Mitre Att&ck para identificar amenazas y/o vulnerabilidades. • Utiliza categorías de STRIDE para identificar amenazas.	La evaluación final consiste en la entrega de un Informe de Análisis de Amenazas, vulnerabilidades y riesgos de un caso, el cual tendrá una ponderación del 40%, y que además será evaluado por medio de una rúbrica. El caso usado en esta evaluación necesita que el participante aplique los conocimientos con mayor profundidad relacionándolo a marcos específicos, relacionando elementos del caso para completar eficientemente la identificación de Amenazas, Vulnerabilidades y riesgos, debiendo además estructurar el resultado para una comunicación eficiente en un informe.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 40%.**
	INSTRUMENTO PARA SENCE: Evaluación diagnostica mediante cuestionario de selección múltiple medido con pauta de evaluación. Evaluaciones parciales: - Unidad 1: Mediante caso con cuestionario medido con pauta de evaluación. - Unidad 2: Mediante caso medido con rubrica. Evaluación Final: mediante informe y caso medido con rubrica.	
Requisito de aprobación		
Modalidad presencial	Asistencia Mínima de 75% de las horas totales del curso y nota mínima de aprobación 4.0	
Modalidad sincrónica - asincrónica	Conectividad sobre un 75% y nota mínima de aprobación 4.0	

Recursos para la implementación del curso					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
Características de la infraestructura requerida para la ejecución del curso.	**Dónde se impartirá el curso** ***Anexo ficha de costos**	**Indicar cantidad**	**Tipo de equipo y/o herramienta para la implementación del curso** ***Indicar duración de licencias o equipamientos.**	**Indicar cantidad**	**Indicar el material que se requiere para la implementación del curso**
Se necesita un módulo o mesón individual. Red wifi o alámbrica, debe ser capaz de mantener una comunicación fluida en la actividad remota y una respuesta rápida para el uso del simulador Electude. Todos estos son ejemplos, se deben ajustar curso a curso.	Curso de modalidad remota sincrónica Todos estos son ejemplos, se deben ajustar curso a curso.	1 1 1 1 1 1 Todos estos son ejemplos, se deben ajustar curso a curso.	Escritorio Computador Cámara Micrófono Silla ergonómica Simulador Electude Todos estos son ejemplos, se deben ajustar curso a curso.	1 1 Todos estos son ejemplos, se deben ajustar curso a curso.	**No se requerirán, pues todos los softwares son de licencia open** Todos estos son ejemplos, se deben ajustar curso a curso.

Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Escuela)
Máximo dos años

Articulación *Sección a completar por Subdirector(a)		**Código/Sigla/Nombre Certificado**
Programa Regular o EDC	**Escuela**	

Diplomado:	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
Diplomado en Ciberseguridad Avanzada	Uso de técnicas y estrategias de ciberseguridad en la identificación y análisis de amenazas digitales
Diplomado en Ciberseguridad Avanzada	Estrategias de seguridad defensiva en la protección y análisis de información
Diplomado en Ciberseguridad Avanzada	Evaluación de Vulnerabilidades y Pruebas de Penetración (Ethical hacking)

Otros cursos relacionados con la temática

Recursos docentes: Perfil desarrollador	
Profesión	Ingeniero en Computación o Informática.
Años de experiencia	Más de 5 años de experiencia en las disciplinas de análisis forense y respuesta a incidentes.
Conocimientos y habilidades relevantes	Certificación de ciberseguridad: CHFI Conocimientos de análisis forense digital. Conocimiento de respuesta a incidentes.
Observaciones Describir el perfil del profesional que puede diseñar/actualizar este curso, no de la persona que lo está diseñando en este momento.	

Recursos docentes: Perfil relator	
Profesión	Profesional dedicado a la ciberseguridad, idealmente, Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines, entre otros especialistas.
Años de experiencia	3 años de experiencia
Conocimientos y habilidades relevantes	Experiencia en trabajo en análisis forense digital, gestión de redes, herramientas de ciberseguridad (kali, metaspoit, volatility, FTK Imager, Autopsy) y sistemas operativos.
Observaciones Describir el perfil teniendo presente que será el profesional responsable de desarrollar la relatoría del curso.	Es muy importante que este docente tenga experiencia en el uso de máquinas virtuales (kali, metaspoit, volatility, FTK Imager, Autopsy, entre otras).

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso:	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
Técnicas de Evaluación de Vulnerabilidades y Pruebas de Penetración (Ethical hacking)	50		30	Asincrónico

Identificación
Código SENCE
Código curso DuocUC

Unidad académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Escuela de Informática y Telecomunicaciones	Oscar Araya	Mayo, 2024

Especialista disciplinar	Diseñador(a) curricular	Diseñador(a) instruccional	Analista instruccional
Giovanni Morchio Peña	Noelia Escalona	Paula Doenitz	Javier Canales

Aporte de valor del programa (no SENCE)

En el contexto actual, la creciente sofisticación y costos asociados a los ciberataques plantean una demanda imperativa de profesionales altamente capacitados en seguridad cibernética. Las organizaciones requieren personal experto en evaluar vulnerabilidades, llevar a cabo pruebas éticas de penetración y fortalecer las medidas de seguridad.

Para abordar esta necesidad, se presenta este curso, enfocado en proporcionar conocimientos y habilidades prácticas para realizar evaluaciones exhaustivas de seguridad. Los participantes aprenderán a detectar y manejar vulnerabilidades de forma controlada, así como a formular recomendaciones efectivas para mejorar la postura de seguridad de las empresas. Además, se abordarán aspectos éticos y legales cruciales, preparando a los estudiantes para ejercer su profesión de manera responsable, cumpliendo con las regulaciones vigentes.

Caracterización del participante

Analistas, arquitectos y administradores de ciberseguridad, auditores, analistas de riesgos, desarrolladores de aplicaciones y/o personas que hayan estudiado una carrera afín en Informática, redes o telecomunicaciones.

Requisitos de ingreso del participante

Poseer conocimientos en:

- Uso de Sistemas operativos Linux y Windows.
- Conocimientos básicos de programación en cualquier lenguaje.
- Inglés nivel básico en nivel de lectura.
- Modelo TCP/IP.

Requisitos técnicos del participante

Sistema Operativo Windows 10 o superior; iOS 11 o posterior
Memoria RAM: 16 GB o más
Procesador: velocidad de 2 GHz o superior
Tarjeta de sonido
Resolución de monitor: 1024 x 768 o superior.
Navegadores Recomendados: Google Crome (última versión), Mozilla Firefox (última versión), Microsoft Edge

Cámara, micrófono, parlantes y/o audífonos
Lector de PDF, como Adobe Acrobat Reader (adobe.com) o Foxit Reader (foxit.com)
Conexión a Internet de mínimo 10 horas a la semana y de 12mbps o más para una adecuada experiencia de videoconferencia y visualización de recursos de aprendizaje (para medir la velocidad de su enlace a internet, puede visitar la página http://www.speedtest.net/).

Objetivo general
Diseñar un marco de gestión de vulnerabilidades de la infraestructura digital de una organización a través de herramientas de ethical hacking y acciones de mitigación de riesgos.

Unidades	Objetivo específico	Contenidos	Horas	
			T	P
Unidad 1: Análisis de vulnerabilidades aplicado a Ethical Hacking	Analizar herramientas y etapas de detección y evaluación de vulnerabilidades, y ethical hacking de acuerdo con la infraestructura digital organizacional.	- Contexto de evaluación de vulnerabilidades y ethical hacking. - Clasificación y tipo de vulnerabilidades: • Matriz de cruza. - Etapas de un pentesting en la evaluación de vulnerabilidades y herramientas para detectar la superficie de ataque. - Revisión de las herramientas de detección y evaluación de vulnerabilidades tipo opensource y de pago.	4	6
Unidad 2: Pruebas de Penetración (Ethical Hacking)	Aplicar técnicas de hacking ético mediante pruebas de penetración controlada por etapas y generación de recomendaciones en la mitigación de riesgos.	- Conceptos de hacking ético y aspectos legales. - Ejecución de las etapas de pentesting. - Estrategias efectivas de mitigación de riesgos a ciberataques: Viabilidad.Efectividad y adaptabilidad a escenarios de amenazas emergentes. - Creación de documentación y uso de herramientas para la gestión de vulnerabilidades.	5	15
		Subtotal	9	21
		Horas totales	30	

Estrategias metodológicas
La estrategia metodológica de este curso corresponde a la auto instrucción, considerando el diseño del curso en una modalidad 100% online a través del Ambiente Virtual de Aprendizaje (AVA) establecido por Duoc UC. El proceso de enseñanza/aprendizaje se desarrollará a través de diversos recursos que estarán dispuestos de forma ordenada en el AVA, permitiendo maximizar la accesibilidad y la efectividad del aprendizaje, al proporcionar una estructura clara y coherente que permite a los participantes navegar fácilmente por el contenido del curso.

Con la finalidad de que los participantes adquieran el conocimiento de manera significativa, dinámica y contextualizada, se diseñarán recursos de enseñanza/aprendizaje considerando una secuencia que permita activar los conocimientos previos y poder vincularlos con nuevas ideas, demostrar o contextualizar los contenidos en escenarios lo más reales posibles, aplicar lo aprendido a través de evaluaciones formativa o sumativas a través de metodología como análisis de casos y problemas representativos de la realidad laboral de los participantes, y, finalmente, promover la integración de los aprendizajes, facilitando que los conocimientos adquiridos se consoliden y se puedan aplicar de manera efectiva en situaciones reales, reforzando así la capacidad de los participantes para enfrentar desafíos profesionales en sus puestos de trabajo.

El curso consta de dos unidades:

La primera unidad, tiene como objetivo Analizar herramientas y etapas de detección y evaluación de vulnerabilidades, y ethical hacking de acuerdo con la infraestructura digital organizacional. Para ello, se establecerán diversos recursos que, además de permitir que identifiquen los conceptos clave, puedan aplicar la información a través de actividades formativas que prepararán a los participantes y así puedan alcanzar el objetivo de la unidad a través del desarrollo de una evaluación parcial.

La segunda unidad, tiene como objetivo aplicar técnicas de hacking ético mediante pruebas de penetración controlada por etapas y generación de recomendaciones en la mitigación de riesgos. Para ello, se realizarán diversos tipos de actividades formativas, de tal forma que todos los participantes puedan llegar de la mejor forma al desarrollo de la evaluación parcial de la unidad.

Se destaca el enfoque práctico que tendrá el curso a través del uso de ejercicios para que los estudiantes puedan aplicar los conceptos aprendidos, a través de la exploración del contexto que rodea la evaluación de vulnerabilidades y el ethical hacking, la utilización de herramientas para detectar y evaluar posibles debilidades en la seguridad y la implementación de estrategias eficaces para mitigar riesgos y de las técnicas éticas de hacking mediante pruebas controladas a través del uso de las herramientas correspondientes, ofreciendo recomendaciones para mejorar la seguridad de los sistemas informáticos. Se cubrirán conceptos básicos de hacking ético, aspectos legales, técnicas de evaluación de sistemas, ejemplos de pruebas controladas y éticas, así como la documentación de vulnerabilidades críticas y la elaboración de informes técnicos que incluyan recomendaciones para abordar vulnerabilidades críticas.

Estrategias evaluativas		
Criterios de evaluación:	**Instrumentos de evaluación:**	**Normas de aprobación:**
Evaluación diagnóstica		
• Identifica las áreas críticas de infraestructura informática que son vulnerables al hacking. • Diferencia las características entre el hacking y hacking ético. • Identifica la importancia estratégica para la infraestructura informática de la evaluación de vulnerabilidades y pruebas de penetración.	La evaluación diagnóstica se realizará al inicio del curso. Se enfocará en reconocer los conocimientos previos de los participantes en torno a los conceptos y contenidos elementales de Evaluación de vulnerabilidades y ethical hacking. Se presentará en un formato cuestionario, con 10 reactivos de selección múltiple simple, 4 distractores, respuesta y retroalimentación automatizada.	Esta evaluación no tiene ponderación.

• Reconoce la importancia ética legal en la realización de pruebas de penetración.		
Unidad 1		
• Identifica los conceptos asociados a ethical hacking y evaluación de vulnerabilidades informáticas. • Analiza el contexto de ciberseguridad que rodea la evaluación de vulnerabilidades y el ethical hacking. • Aplica la matriz de cruzada en la categorización y clasificación de tipos de vulnerabilidades en casos de estudio específicos. • Analiza las etapas del pentesting y las herramientas de detección de superficies de ataque.	Los estudiantes analizarán casos de estudio basados en cuatro áreas clave: el contexto de evaluación de vulnerabilidades y ethical hacking, la clasificación y tipos de vulnerabilidades mediante el uso de una matriz de cruza, las etapas de un pentesting para la evaluación de vulnerabilidades, y las herramientas para detectar y evaluar vulnerabilidades. Esta evaluación se realizará a través de un cuestionario con 20 enunciados de selección múltiple simple, cada pregunta contendrá 4 distractores y ofrecerá respuestas y retroalimentación automatizadas.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 30%.**
Unidad 2		
• Analiza el contexto de evaluación de vulnerabilidades y ethical hacking en un entorno empresarial en búsqueda de mejoras prácticas y enfoques adaptados a cada situación. • Aplica técnicas de hacking ético en la evaluación de sistemas informáticos en casos aplicados basado en los principios éticos y límites legales. • Aplica etapas de pentesting en el reconocimiento de amenazas de seguridad en sistemas y redes. • Utiliza estrategias de mitigación de riesgo para las amenazas emergentes considerando su viabilidad, efectividad y adaptabilidad a escenarios de amenazas emergentes.	La evaluación consistirá en la aplicación de técnicas de hacking ético y aspectos legales en situaciones prácticas. A partir de ellas, se solicitará a los participantes ejecutar las etapas de pentesting, incluyendo la identificación de vulnerabilidades y la evaluación de la seguridad de sistemas y redes informáticas. Se evaluará también la capacidad de los participantes para aplicar las estrategias aprendidas de mitigación de riesgos para minimizar la superficie de ataque. El resultado del trabajo se integrará en un informe y será evaluado a través de una rúbrica.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 30%.**
Evaluación Final		

• Aplica los pasos de pentesting mediante la búsqueda activa de vulnerabilidades y puntos de entrada de posibles ataques cibernéticos. • Diagnóstica los riesgos identificados durante la evaluación de vulnerabilidades, priorizando aquellos que representen una amenaza significativa para la seguridad de la organización. • Aplica los aspectos legales y éticos en la gestión de diagnóstico, pruebas de penetración, y diseño de informe de vulnerabilidades considerando la conformidad con las regulaciones vigentes, la protección de la privacidad y la responsabilidad legal. • Elabora un informe detallado que documente los riesgos identificados. • Diseña estrategias de mitigación efectivas.	La evaluación final se presentará en formato de caso aplicado de una organización ficticia que entrega un requerimiento de evaluación de vulnerabilidades y pruebas de penetración de sistemas informáticos. Los casos se presentarán mediante máquinas virtuales. El participante asumirá el rol de consultor, deberá evaluar un ambiente simulado, documentarla, aplicar los pasos pentesting, y finalmente generar un informe de riesgos y diseño de estrategias de mitigación para la organización.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. **Esta evaluación tiene una ponderación de un 40%.**
	INSTRUMENTO PARA SENCE: Evaluación diagnostica mediante cuestionario de selección múltiple medido con pauta de evaluación. Evaluaciones parciales: - Unidad 1: Mediante caso con cuestionario medido con pauta de evaluación. - Unidad 2: Mediante caso medido con rubrica. Evaluación Final: mediante informe y caso medido con rubrica.	
Requisito de aprobación		
Modalidad presencial	Asistencia Mínima de 75% de las horas totales del curso y nota mínima de aprobación 4.0	
Modalidad sincrónica - asincrónica	Conectividad sobre un 75% y nota mínima de aprobación 4.0	

Recursos para la implementación del curso					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
Características de la infraestructura requerida para la ejecución del curso. Definir y dejar establecidos los insumos, herramientas, materiales o equipos que se necesitan para llevar a cabo de forma exitosa el curso.	**Dónde se impartirá el curso** ***Anexo ficha de costos**	**Indicar cantidad**	**Tipo de equipo y/o herramienta para la implementación del curso** ***Indicar duración de licencias o equipamientos.**	**Indicar cantidad**	**Indicar el material que se requiere para la implementación del curso**
Plataforma LMS Blackboard. Sistema de videoconferencia online Collaborate integrado a plataforma.	Curso de modalidad remota asincrónica	1 1 1 1 1	Escritorio Computador Cámara Micrófono Silla ergonómica	1 1	Máquinas virtuales gratuitas.

Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Escuela)
Máximo dos años

Articulación *Sección a completar por Subdirector(a)		Código/Sigla/Nombre Certificado
Programa Regular o EDC	**Escuela**	

Diplomado: En caso de que el curso pertenezca a un diplomado, se deberá indicar el nombre del diplomado, y el nombre de todos los cursos de diplomado, en el orden que corresponda.	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
Diplomado en Ciberseguridad Avanzada	**Uso de técnicas y estrategias de ciberseguridad en la identificación y análisis de amenazas digitales**
Diplomado en Ciberseguridad Avanzada	**Estrategias de seguridad defensiva en la protección de información**
Diplomado en Ciberseguridad Avanzada	**Técnicas forenses y respuesta a incidentes de ciberseguridad**

Otros cursos relacionados con la temática Incluir cursos que tengamos diseñados y que se relacionen con la temática, por ejemplo, si la PNCT corresponde a un curso de Excel avanzado, en este apartado se puede incluir el curso de: Power BI avanzando

Recursos docentes: Perfil desarrollador	
Profesión	Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines.
Años de experiencia	4 años
Conocimientos y habilidades relevantes	Experiencia en proyectos de seguridad en TI, experiencia en educación superior, habilidades de relatoría, Certificaciones deseables en ISO27001, CEH o equivalentes.
Observaciones Describir el perfil del profesional que puede diseñar/actualizar este curso, no de la persona que lo está diseñando en este momento.	

Recursos docentes: Perfil relator	
Profesión	Profesional dedicado a la ciberseguridad, idealmente, Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines, entre otros especialistas.
Años de experiencia	2-3 años
Conocimientos y habilidades relevantes	Experiencia en proyectos de seguridad en TI como analista de seguridad, habilidades de relatoría, Certificaciones deseables CEH, eJPT o equivalentes.
Observaciones Describir el perfil teniendo presente que será el profesional responsable de desarrollar la relatoría del curso.	