**FUNDACIÓN INSTITUTO PROFESIONAL DUOC UC**
**VICERRECTORÍA ACADÉMICA**
**RESOLUCIÓN Nº15/2025**

**APRUEBA DIPLOMADO EN CIBERSEGURIDAD**

**VISTOS:**

1º. El proyecto presentado por la directora de la Escuela de Informática y Telecomunicaciones de Duoc UC.
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", cuyo texto se adjunta a continuación de esta resolución, el cual reemplaza al publicado en Resolución VRA Nº30, de fecha 27 de julio de 2022.

Comuníquese, publíquese y regístrese.

Santiago, abril 21 de 2025.

Alejandra Silva Lafourcade
Firmado digitalmente por Alejandra Silva Lafourcade
Fecha: 2025.04.16 12:21:53 -04'00'

**ALEJANDRA SILVA LAFOURCADE**
DIRECTORA GENERAL DE DESARROLLO ESTUDIANTIL Y EDUCACIÓN CONTÍNUA

Kiyoshi Fukushi
Firmado digitalmente por Kiyoshi Fukushi
Fecha: 2025.04.17 08:13:38 -04'00'

**KIYOSHI FUKUSHI MANDIOLA**
VICERRECTOR ACADÉMICO

KFM/ASL/JMD/jda

**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",** para formar parte de la oferta personas de Educación Continua.

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

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

# DIPLOMADO EN CIBERSEGURIDAD

**RESUMEN:**

Diplomado de oferta abierta desarrollado por la Escuela de Informática y Telecomunicaciones.

La ciberseguridad se ha convertido en un tema relevante en la mayoría de las organizaciones de todos los rubros. El aumento de la dependencia hacia sistemas informáticos tanto en los procesos productivos como funcionales de empresas e instituciones ha conferido un estatus crucial a los datos, un activo que incrementa su valor día a día, aumentando a su vez la demanda de profesionales calificados para el resguardo de éstos. Por este alto valor de los datos, se registra un alarmante aumento de ciberataques que provocan pérdidas, tanto de recursos como de prestigio, en las compañías afectadas. Es por ello que implementar programas de capacitación en seguridad informática para la especialización de expertos con capacidad de liderazgo en el control de la información, es cada vez más necesario.

En consecuencia, se vuelve imprescindible que existan ofertas formativas como ésta, donde los profesionales que se desempeñan en esta área posean una formación permanente centrada en los conocimientos y competencias necesarias para una exitosa trayectoria laboral. Teniendo en consideración este contexto, este programa se orienta en que los profesionales del área de Telecomunicaciones o desarrollo TI profundicen sus conocimientos en Ciberseguridad de la información, entregando herramientas para mejorar su desempeño laboral o buscar nuevas alternativas laborales, con un enfoque práctico y transversal.

El Diplomado tiene una duración de 120 horas cronológicas, en modalidad e-learning asincrónico con componentes sincrónicos.

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

| Nombre Módulos | Horas | % de la nota final de Diplomado |
|---|---|---|
| Ciberseguridad en la Organización | 30 | 25% |
| Gestión en Ciberseguridad | 30 | 25% |
| Ciberseguridad Defensiva | 30 | 25% |
| Ciberseguridad Ofensiva | 30 | 25% |
| **TOTAL DE HORAS** | **120** | **100** |

El diplomado está dirigido a todas aquellos profesionales del área de ciberseguridad y tecnología, personas que hayan estudiado una carrera afín en informática, redes o telecomunicaciones. Personas que posean 3 años de experiencia laboral en el área.

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

# FICHA ÚNICA DE CREACIÓN DE DIPLOMADOS
# PNCT

**1. NOMBRE DEL DIPLOMADO**

DIPLOMADO EN CIBERSEGURIDAD

**2. TOTAL DE HORAS**

120

**3. POBLACIÓN OBJETIVO**

Profesionales del área de ciberseguridad y tecnología. Personas que hayan estudiado una carrera afín en informática, redes o telecomunicaciones. Personas que posean 3 años de experiencia laboral en el área.

**4. REQUISITOS DE INGRESO**

Conocimientos deseables en sistemas operativos y manejo de comandos (Linux y Windows), seguridad de la información y ciberseguridad, e inglés básico a nivel de lectura.

**5. JUSTIFICACIÓN DE CREACIÓN**

La ciberseguridad se ha convertido en un tema relevante en la mayoría de las organizaciones de todos los rubros. El aumento de la dependencia hacia sistemas informáticos tanto en los procesos productivos como funcionales de empresas e instituciones ha conferido un estatus crucial a los datos, un activo que incrementa su valor día a día, aumentando a su vez la demanda de profesionales calificados para el resguardo de éstos. Por este alto valor de los datos, se registra un alarmante aumento de ciberataques que provocan pérdidas, tanto de recursos como de prestigio, en las compañías afectadas. Es por ello que implementar programas de capacitación en seguridad informática para la especialización de expertos con capacidad de liderazgo en el control de la información, es cada vez más necesario.

En consecuencia, se vuelve imprescindible que existan ofertas formativas como ésta, donde los profesionales que se desempeñan en esta área posean una formación permanente centrada en los conocimientos y competencias necesarias para una exitosa trayectoria laboral. Teniendo en consideración este contexto, este programa se orienta en que los profesionales del área de Telecomunicaciones o desarrollo TI profundicen sus conocimientos en Ciberseguridad de la información, entregando herramientas para mejorar su desempeño laboral o buscar nuevas alternativas laborales, con un enfoque práctico y transversal.

## 6. OBJETIVO GENERAL/ IDENTIFICACIÓN PERFIL DE SALIDA

Aplicar procedimientos de control como medio de mejora de las medidas de ciberseguridad en la organización, conforme a las buenas prácticas del sector, protocolos establecidos y normativa vigente.

## 7. UNIDAD ACADÉMICA

Escuela de Informática y Telecomunicaciones

## 8. FECHA

16-12-2024

## 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 |
|---|---|---|
| Ciberseguridad en la organización | 30 | 25% |
| Gestión en ciberseguridad | 30 | 25% |
| Ciberseguridad defensiva | 30 | 25% |
| Ciberseguridad ofensiva | 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 Final |
|---|---|
| 100% | |

## 10. MODALIDAD DE IMPARTICIÓN

| | Modalidad |
|---|---|
| Presencial | |
| Semipresencial | |
| E-learning (asincrónico) | x |

# Ficha Programa No Conducente a Título (PNCT)

| Nombre del curso | Vacantes | Horas totales | Modalidad factible |
|---|---|---|---|
| Ciberseguridad en la Organización | 1 | 30 | Online Asincrónico |

| Identificación |
|---|
| Código SENCE |
| Código curso DuocUC |

| Unidad académica | Subdirector(a) de Escuela | Fecha de elaboración |
|---|---|---|
| Escuela de Informática y Telecomunicaciones | Oscar Araya | Noviembre, 2024 |

| Nombre experto(a) disciplinar | Nombre diseñador(a) curricular | Nombre diseñador(a) instruccional | Analista Instruccional |
|---|---|---|---|
| Helvecia Castro | | Javier Canales | Javier Canales |

| Aporte de valor del programa (no SENCE) |
|---|
| El aumento exponencial del uso de tecnologías de la información en las diversas industrias ha evidenciado brechas importantes en las materias relacionadas a la ciberseguridad, generando riesgos que podrían impactar de forma significativa a las compañías e instituciones. Por esta razón, la mayoría de las organizaciones invierten en capacitación a nivel global, y, en lo particular, en el ámbito informático buscan perfiles que posean conocimientos concretos, específicos y actualizados de ciberseguridad con el fin de resguardar la información y desarrollar buenas prácticas al interior de la organización.<br><br>Es por ello que, en este curso las y los participantes podrán adquirir competencias generales, que permitan la comprensión de los conceptos fundamentales en el contexto de la ciberseguridad, las principales diferencias entre la seguridad de la información y la ciberseguridad, el entendimiento y aplicación de los framework internacionales, normativa nacional, y mejores prácticas para el resguardo de la información al interior de una organización. |

| Caracterización del Participantes |
|---|
| Analistas, arquitectos y administradores de ciberseguridad, auditores, analistas de riesgos y/o profesionales que hayan estudiado una carrera afín en Informática, redes o telecomunicaciones. |

| Requisitos de ingresos participantes |
|---|
| Tecnologías de la información.<br>Gestión de riesgos nivel básico.<br>Conocimientos básicos de estándares de seguridad y controles.<br>Conocimientos básicos en normativa nacional de ciberseguridad.<br>Conocimientos básicos de programación.<br>Conocimientos técnicos de redes, sistemas operativos y comandos (Linux y Windows).<br>Conocimientos generales de herramientas tecnológicas de ciberseguridad (SIEM, DLP, EDR, FW, MFA, IDM, IRM, entre otros). |

| |
|---|
| Requerimientos de Hardware: Procesador Intel de 2.0 GHz (preferible Core dúo) - 1 Gb Memoria RAM (preferible 2 Gb) - Espacio libre en el disco duro de 1 Gb. |
| Requerimientos de Software para participante del curso: Windows 10 o Mac OS X - Office 2007 para Windows u Office 2008 para Mac - Navegador de Internet (Chrome, Firefox y Safari versión para Mac). Internet Explorer no es compatible con la versión actual de Blackboard. - Instalación de programa para visualizar archivos PDF e instalación de herramientas de ofimática. |

| **Competencia a desarrollar / Objetivo General** |
|---|
| Aplicar herramientas de ciberseguridad en el diseño de un plan director en la organización. |

| **Unidades** | **Objetivo Específico** | **Contenidos** | **Horas** | |
|---|---|---|---|---|
| | | | T (40%) | P (60%) |
| **UNIDAD 1**<br><br>Frameworks y estándares de ciberseguridad | Identificar los frameworks de ciberseguridad aplicables de acuerdo con las necesidades de la organización. | • **Framework y estándares aplicables.**<br>• **Leyes y normas nacionales en el contexto de ciberseguridad.**<br>• **Regulación aplicable a la organización según el sector al que pertenece.**<br>• **Metodología de evaluación y gestión de riesgos.** | 6 | 9 |
| **UNIDAD 2**<br><br>Diseño de ciberseguridad en la organización | Aplicar herramientas de ciberseguridad de acuerdo al nivel de madurez de la organización. | • **Modelo PDCA.**<br>• **Análisis y matriz FODA.**<br>• **Diseño de plan de ciberseguridad.**<br>• **Generación de cultura de ciberseguridad.** | 6 | 9 |
| | | Subtotal | 12 | 18 |
| | | Total | 30 | |

| **Estrategias Metodológicas para la Implementación del Curso** |
|---|
| **Metodologías de entrega de contenidos**: Al término de este curso, los participantes podrán aplicar herramientas de ciberseguridad en el diseño de un Plan Director de Ciberseguridad, basado en el análisis y gestión de riesgos cibernéticos, frameworks aplicables y objetivos estratégicos de la organización. La estrategia metodológica se basa en la auto instrucción a través de un programa 100% e-learning asincrónico. El proceso de enseñanza y aprendizaje se desarrollará mediante diversos recursos organizados en el Ambiente Virtual de Aprendizaje de Duoc UC para que los participantes adquieran conocimientos de manera significativa y dinámica. Dichos recursos pueden ser: videos interactivos, guías interactivas, |

infografías, PDF descargable u otros; a través de los cuales se presentarán los contenidos de forma contextualizada y representativa según la realidad laboral de los participantes. El material estará disponible en formatos audiovisuales y descargables. Además, en cada unidad se realizarán actividades formativas mediante análisis de casos, cuestionarios y resolución de problemas.

El curso tiene una duración total de 30 horas distribuidas en 6 semanas, considerando una dedicación semanal de máximo 5 horas. Además, se realizarán encuentros sincrónicos (opcionales) que permitirán a los participantes resolver dudas, profundizar en temas de interés y compartir experiencias con los demás participantes y facilitador.

**Descripción de unidades:**
**Unidad 1:** Durante la primera unidad, los participantes deberán identificar las características de los frameworks y las diversas normativas que aplican a una organización de acuerdo con la actividad que realiza. Además, en esta unidad podrán conocer cómo realizar una evaluación de riesgo que permita identificar el escenario actual de una organización y así proponer mejoras de acuerdo con las brechas identificadas.

**Unidad 2:** Durante el desarrollo de la segunda unidad, los participantes podrán comprender la importancia de la cultura de ciberseguridad, identificar los tipos de presupuestos (CAPEX y OPEX) para diversas iniciativas de ciberseguridad. A su vez, podrán reconocer el ciclo PDCA para la mejora continua y aplicar la matriz FODA en el contexto de la ciberseguridad para contribuir a la toma de decisiones.

Cada unidad cuenta con una evaluación sumativa, las que se centran en una metodología activa/participativa, con foco en el análisis de casos, las cuales se presentan de forma secuenciada y progresiva a lo largo del desarrollo del curso.

En la evaluación final del curso, los participantes deberán elaborar un Plan Director de Ciberseguridad, que contribuya a enfrentar los desafíos de ciberseguridad de una empresa, considerando los elementos desarrollados en las evaluaciones anteriores.

Desde el punto de vista de la evaluación, será un proceso permanente, considerando una evaluación sumativa al final de cada unidad, una sumativa al final del curso, y evaluaciones formativas durante todo el proceso. Cada una de ellas con sus respectivas pautas de evaluación y/o rúbricas.

| **Estrategias Evaluativas del Curso** | | |
|---|---|---|
| CRITERIOS DE EVALUACIÓN<br><br>**Unidad 1**<br><br>- Identifica los frameworks y justifica su aplicabilidad en la organización.<br><br>- Identifica las regulaciones locales aplicables a una organización, según su contexto. | INSTRUMENTOS DE EVALUACIÓN<br><br>Al comenzar el curso, el docente realizará una **evaluación diagnóstica** de conceptos claves de la temática, durante la primera sesión, con el fin de consensuar el nivel de conocimientos previos de los participantes.<br><br>**Unidad 1:**<br>Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, con base en identificación de frameworks y regulaciones de ciberseguridad en contextos de casos hipotéticos.<br>Ponderación: 35%.<br><br>**Unidad 2:** | NORMAS DE APROBACIÓN<br><br>Las calificaciones derivadas de la evaluación sumativa del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. Se corregirá el producto presentado por medio de una rúbrica. |

| | | |
|---|---|---|
| - Identifica estado de riesgos cibernéticos basado en el estándar ISO 27005.<br><br>- Selecciona los controles de los frameworks aplicables para la mitigación de los riesgos cibernéticos identificados.<br><br>- Define y prioriza la ejecución de las acciones requeridas para la mitigación de los riesgos cibernéticos.<br><br>**<u>Unidad 2</u>**<br><br>- Desarrolla un instrumento para medir el nivel de madurez de cibercultura en una organización.<br><br>- Planifica la aplicación del instrumento de medición.<br><br>- Determina las acciones de concientización y formación requeridas en la organización.<br><br>- Estima el tipo de presupuesto que requerirá cada una de las acciones.<br><br>- Diseña el programa de cultura de ciberseguridad.<br><br>**<u>Evaluación Final</u>**<br>- Describe las iniciativas que darán cobertura a la implementación de los controles seleccionados para mitigación de riesgo.<br><br>- Considera programa de cultura de ciberseguridad como parte de las iniciativas. | Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, con base en la aplicación de herramientas de ciberseguridad en contextos de casos hipotéticos.<br>Ponderación: 25%.<br><br>**Unidad 3:**<br>Actividad evaluativa: : Hetero-evaluación con entrega de un Plan Director de Ciberseguridad, evaluado con rúbrica.<br><br>Ponderación: 40% | |

| | | |
|---|---|---|
| - Planifica la implementación de las iniciativas señalando el inicio y término dentro del año calendario.<br><br>- Elabora Roadmap (cronograma anual), considerando la planificación realizada.<br><br>- Asigna la ejecución de las iniciativas a cada uno de los correspondientes equipos que conforman el área de ciberseguridad.<br><br>- Desarrolla Plan Director de Ciberseguridad. | | |

| **Requisito de aprobación** | |
|---|---|
| Modalidad a distancia – Asincrónico | 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)** |
| Plataforma LMS Blackboard. Sistema de videoconferencia online Collaborate integrado a plataforma. | | | **Requerimientos de Hardware:** Procesador Intel de 2.0 GHz (preferible Core dúo) - 1 Gb Memoria RAM (preferible 2 Gb) - Espacio libre en el disco duro de 1 Gb.<br><br>**Requerimientos de Software para participante del curso:** Windows 10 o Mac OS X - Office 2007 para Windows u Office 2008 para Mac - Navegador de Internet | | Material en formato digital<br><br>- NIST<br>- MITRE ATT&CK<br>- CAT-FFIEC<br>- CIS<br>- ISO 27001 - ISO 27002 - ISO 27032 - ISO 31000<br>- GDPR |

| | | | | | |
|---|---|---|---|---|---|
| | | | (Chrome, Firefox y Safari versión para Mac). Internet Explorer no es compatible con la versión actual de Blackboard. - Instalación de programa para visualizar archivos PDF e instalación de herramientas de ofimática.<br><br>Conexión a Internet de banda ancha.<br><br>Parlantes o audífonos para el desarrollo del curso.<br><br>Micrófono. | | Sesiones relacionadas al contenido del curso en formato descargable.<br><br>Evaluaciones y pautas de corrección. |

| **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** | **Ciberseguridad en la Organización** |
| | Gestión en Ciberseguridad |
| | Ciberseguridad Defensiva |
| | Ciberseguridad Ofensiva |

| **RECURSOS DOCENTES: PERFIL DESARROLLADOR** | |
|---|---|
| **PROFESIÓN** | Ingeniero comercial – Magister en riesgos del Negocio- postítulo en transformación digital |
| **AÑOS DE EXPERIENCIA** | 5 años |
| **CONOCIMIENTOS Y HABILIDADES RELEVANTES** | Certificaciones ISO 27032; ISO 27701; ISO 22301 y ISO 27001.<br>Certificaciones internacionales en NIST, CISSP, ITIIL. |
| **OBSERVACIONES** | Experiencia en cargos de CISO y gerente de Ciberseguridad que permiten tener un acercamiento real con la materia y los casos analizados y propuestos |

| RECURSOS DOCENTE: PERFIL RELATOR | |
|---|---|
| **PROFESIÓN** | Ingeniero comercial, Ingeniero Informático o Ingeniero civil |
| **AÑOS DE EXPERIENCIA** | 5 años |
| **CONOCIMIENTOS Y HABILIDADES RELEVANTES** | Certificaciones de Certificaciones ISO 27032; ISO 27701; ISO 22301 y ISO 27001.<br>Certificaciones internacionales en NIST, CISSP, ITIIL.<br>Conocimientos de Basilea,<br>conocimiento en metodología de riesgos. |
| **OBSERVACIONES** | Poseer experiencia laboral y docente demostrable en el área, para que pueda transmitir de mejor manera los análisis de casos y como se abordan los mismos. |

# Ficha Programa No Conducente a Título (PNCT)

| Nombre del curso | Vacantes | Horas totales | Modalidad factible |
|---|---|---|---|
| Gestión en ciberseguridad | 1 | 30 | Online Asincrónico |

| Identificación |
|---|
| Código SENCE |
| Código curso DuocUC |

| Unidad académica | Subdirector(a) de Escuela | Fecha de elaboración |
|---|---|---|
| Escuela de Informática y Telecomunicaciones | Oscar Araya | Noviembre, 2024 |

| Nombre experto(a) disciplinar | Nombre diseñador(a) curricular | Nombre diseñador(a) instruccional | Analista Instruccional |
|---|---|---|---|
| Helvecia Castro/Willy Bascuñán | Natasha Aude | Roxana Acevedo | Javier Canales |

| Aporte de valor del programa (no SENCE) |
|---|
| El intercambio de datos en el ciberespacio ha generado la necesidad de contratar expertos en ciberseguridad, capaces de detectar aquellas brechas de seguridad que son trascendentales para las organizaciones. Desde este punto de vista, resulta fundamental concienciar sobre la importancia de la seguridad de los activos de información, a través del análisis de los factores de riesgo, aplicando los lineamientos definidos por los estándares internacionales y la legislación nacional vigente, asociados a la implementación de un sistema de gestión de seguridad de la información y ciberseguridad.<br><br>Este curso está orientado a que los participantes adquieran herramientas que les permitan mitigar las amenazas digitales con el fin de reducir el riesgo de ciberataques, utilizando las buenas prácticas y controles tecnológicos creados para minimizar la probabilidad y el impacto de ciber amenazas en una organización. |

| Caracterización del Participantes |
|---|
| Analistas, arquitectos y administradores de ciberseguridad, auditores, analistas de riesgos y/o personas que hayan estudiado una carrera afín en Informática, redes o telecomunicaciones. |

| Requisitos de ingresos participantes |
|---|
| Los participantes deben poseer conocimientos previos en:<br>Tecnologías de la información.<br>Redes y telecomunicaciones.<br>Gestión de riesgos.<br>Conocimientos básicos de estándares de seguridad y controles.<br>Inglés nivel básico en nivel de lectura. |
| Requerimientos de Hardware: Procesador Intel de 2.0 GHz (preferible Core dúo) - 1 Gb Memoria RAM (preferible 2 Gb) - Espacio libre en el disco duro de 1 Gb. |

Requerimientos de Software para participante del curso: Windows 7 o Mac OS X - Office 2007 para Windows u Office 2008 para Mac - Navegador de Internet (Chrome, Firefox y Safari versión para Mac). Internet Explorer no es compatible con la versión actual de Blackboard. - Instalación de programa para visualizar archivos PDF e instalación de herramientas de ofimática.

| Competencia a desarrollar / Objetivo General |
|---|
| Aplicar prácticas de ciberseguridad en la gestión de riesgos cibernéticos de una organización. |

| Unidades | Objetivo Específico | Contenidos | Horas | |
|---|---|---|---|---|
| | | | T | P |
| **UNIDAD 1**<br><br>Controles de seguridad de la información | Reconocer controles de seguridad según los riesgos cibernéticos de la organización. | **Estándares de seguridad:**<br>● ISO 27001<br>● ISO 27002<br>● Framework de ciberseguridad NIST<br><br>**Metodología de gestión de riesgos:**<br>● ISO 31000<br><br>**Tipos de controles:**<br>● Preventivos<br>● Detectivos<br>● Correctivos<br><br>**Herramientas tecnológicas de seguridad.** | 4 | 6 |
| **UNIDAD 2**<br><br>Gestión de incidentes de Ciberseguridad y uso de PlayBooks | Aplicar prácticas de ciberseguridad en un plan de respuesta ante una crisis de ciberseguridad. | **Escenarios de ciberataques:**<br>● Ransomware<br>● Phishing<br>● Defacement<br>● DoS<br><br>**Protocolos de actuación ante gestión de crisis de ciberseguridad.**<br><br>**Áreas involucradas ante un escenario de ciberataque.** | 8 | 12 |
| | | Subtotal | 12 | 18 |
| | | Total | 30 | |

| Estrategias Metodológicas para la Implementación del Curso |
|---|
| **Metodologías de entrega de contenidos**: Al término de este curso, los participantes podrán aplicar prácticas de ciberseguridad en la gestión de riesgos cibernéticos de una organización según normativas y estándares vigentes. La estrategia metodológica se basa en la auto instrucción a través de un programa 100% e-learning asincrónico. El proceso de enseñanza y aprendizaje se desarrollará mediante diversos recursos organizados en el Ambiente Virtual de Aprendizaje de Duoc UC para que los participantes adquieran conocimientos de manera significativa y dinámica. Dichos recursos pueden ser: videos interactivos, guías interactivas, infografías, PDF descargable u otros; a través de los cuales se presentarán los contenidos de forma contextualizada y representativa según la realidad laboral de los participantes. El material estará disponible en formatos audiovisuales y descargables. Además, en cada unidad se realizarán actividades formativas mediante análisis de casos, cuestionarios y resolución de problemas.<br><br>El curso tiene una duración total de 30 horas distribuidas en 6 semanas, considerando una dedicación semanal de máximo 5 horas. Además, se realizarán encuentros sincrónicos (opcionales) que permitirán a los participantes resolver dudas, profundizar en temas de interés y compartir experiencias con los demás participantes y facilitador.<br><br>**Descripción de unidades:**<br><br>**Unidad 1:** los participantes reconocerán controles para mitigar los riesgos cibernéticos a los que se encuentra expuesta la organización. En el contexto de un análisis de caso, reconocerán controles existentes y los necesarios de implementar en la organización considerando la revisión de los distintos dominios de las normas ISO 27001/27002 a partir del nivel de madurez de la organización. Esto les permitirá adquirir competencias que podrán utilizar en su contexto laboral.<br><br>**En la segunda unidad**, los participantes tendrán que aplicarán prácticas de ciberseguridad dentro de un plan de respuesta, simulando un posible escenario de algún incidente de ciberseguridad. El plan de respuesta, tendrá como base los protocolos de actuación que se han desarrollado para enfrentar los escenarios de ciberataques, lo cual, les permitirá adquirir competencias que podrán utilizar en su contexto laboral. Asimismo, elaborarán un informe de resultado desde la evaluación del ejercicio del escenario de ciberataque simulado para la realización del plan de respuesta. El informe considera la propuesta de un plan de concientización que contemple las recomendaciones y las soluciones de ciberseguridad aplicables en el contexto de la organización con el objetivo de planificar la gestión y los protocolos a seguir ante un ciberataque. |

| Estrategias Evaluativas del Curso | | |
|---|---|---|
| CRITERIOS DE EVALUACIÓN<br><br>**Unidad 1**<br><br>1. Presenta un Resumen Ejecutivo, acorde al nivel consultivo esperado.<br>2. Categoriza el nivel de madurez por cada uno de los controles que aplican al caso.<br>3. Realiza una Declaración de Aplicabilidad (SoA), consistente con los antecedentes, respecto a la aplicabilidad de los controles ISO 27002:2013. | INSTRUMENTOS DE EVALUACIÓN<br><br>Al comenzar el curso, el docente realizará una **evaluación diagnóstica** de definiciones de conceptos claves durante la primera sesión, con el fin de consensuar el nivel de conocimientos previos de los participantes.<br><br>**Unidad 1:**<br><br>Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, con base en el reconocimiento, dentro de un caso hipotético, de los controles existentes y los necesarios de implementar considerando las normas ISO 27001/27002<br>Ponderación: 30%. | NORMAS DE APROBACIÓN<br><br>Las calificaciones derivadas de la evaluación sumativa del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. Se corregirá el producto presentado por medio de una rúbrica. |

| | | |
|---|---|---|
| 4. Categoriza el nivel de madurez por cada uno de los controles identificados.<br>5. Entrega evaluaciones de madurez promedio de los dominios ISO 27002:2013.<br>6. Desarrolla gráfica de visualización del nivel de madurez por dominios ISO27002:2013.<br><br>**<u>Unidad 2</u>**<br><br>1. Define a nivel ejecutivo qué es un ransomware y su impacto organizacional.<br>2. Detalla los métodos típicos de infección, a modo de identificar malas prácticas de los usuarios.<br>3. Explica a nivel gerencial el cómo y por qué construir un playbook ransomware.<br>4. Argumenta si pagar o no por la extorsión de un ransomware.<br>5. Entrega un playbook ransomware.<br>6. Entrega diagrama resumen del playbook Ransomare.<br><br>**<u>Evaluación final</u>**<br><br>1. Describe las actividades que se deben llevar a cabo en un plan de concientización propuesto para la organización.<br>2. Propone actividades de concientización empleando diferentes medios de comunicación o considerando la diversidad de la audiencia.<br>3. Define los responsables y recursos necesarios para el desarrollo de un plan de concientización en una organización.<br>4. Determina los indicadores de logro del plan de concientización propuesto.<br>5. Propone soluciones tecnológicas de | **Unidad 2:**<br>Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, con base en la elaboración de un plan de respuesta ante una crisis de ciberseguridad hipotética, el cual debe contemplar la aplicación de prácticas de ciberseguridad acordes al caso.<br>Ponderación: 30%.<br>**Evaluación final:**<br>Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, con base en la propuesta de implementación de controles desprendidos de la Evaluación de la Unidad 1, y lecciones aprendidas en Evaluación de la Unidad 2, tomando en consideración una práctica ante un incidente de Ransomware.<br>Ponderación: 40% | |

| | | |
|---|---|---|
| ciberseguridad que responde a las necesidades de la organización considerando costo y comparación entre iniciativas.<br>6. Justifica y prioriza soluciones de Ciberseguridad en función de la comparativa de los beneficios que aporta a la organización.<br>7. Identifica controles de seguridad ISO 27002:2013 asociados a los ítemes 1 y 2. | | |

| **Requisito de aprobación** | |
|---|---|
| Modalidad a distancia – Asincrónico | 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)** |
| Plataforma LMS Blackboard. Sistema de videoconferencia online Collaborate integrado a plataforma. | | | **Requerimientos de Hardware:** Procesador Intel de 2.0 GHz (preferible Core dúo) - 1 Gb Memoria RAM (preferible 2 Gb) - Espacio libre en el disco duro de 1 Gb.<br><br>**Requerimientos de Software para participante del curso:** Windows 7 o Mac OS X - Office 2007 para Windows u Office 2008 para Mac - Navegador de Internet (Chrome, Firefox y Safari versión para Mac). Internet Explorer no es compatible con la versión actual de Blackboard. - Instalación de programa para visualizar | | Material en formato digital<br><br>- ISO 27001<br>- ISO 27002<br>- Framework de ciberseguridad NIST<br>- ISO 31000<br><br>Material en formato digital |

| | | | | | |
|---|---|---|---|---|---|
| | | | archivos PDF e instalación de herramientas de ofimática.<br><br>Conexión a Internet de banda ancha.<br><br>Parlantes o audífonos para el desarrollo del curso.<br><br>Micrófono. | | Sesiones relacionadas al contenido del curso en formato descargable.<br><br>Evaluaciones y pautas de corrección. |

| **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** | Ciberseguridad en la Organización |
| | **Gestión en Ciberseguridad** |
| | Ciberseguridad Defensiva |
| | Ciberseguridad Ofensiva |

| **RECURSOS DOCENTES: PERFIL DESARROLLADOR** | |
|---|---|
| **PROFESIÓN** | Ingeniero en Informática |
| **AÑOS DE EXPERIENCIA** | 3 años |
| **CONOCIMIENTOS Y HABILIDADES RELEVANTES** | Conocimientos en ISO 27001, SoC, ciberataque, ciberseguridad. |
| **OBSERVACIONES** | |
| | |

| RECURSOS DOCENTE: PERFIL RELATOR | |
|---|---|
| **PROFESIÓN** | Jefe de seguridad de la información / ciberseguridad. Gerente de TI, CISO, oficial de seguridad. |
| **AÑOS DE EXPERIENCIA** | 3 años |
| **CONOCIMIENTOS Y HABILIDADES RELEVANTES** | Conocimientos en ISO 27001, SoC, ciberataque, ciberseguridad. |
| **OBSERVACIONES** | Capacidad de vincular lo teórico con lo práctico, capacidad de desarrollo de casos / Habilidades para transferir experiencias / procurar que la conceptualización de los conceptos técnicos esté contextualizados /Habilidades relativas a la comunicación asertiva. |

# Ficha Programa No Conducente a Título (PNCT)

| Nombre del curso | Vacantes | Horas totales | Modalidad factible |
|---|---|---|---|
| Ciberseguridad Defensiva | 1 | 30 | Online Asincrónico |

| Identificación |
|---|
| Código SENCE |
| Código curso DuocUC |

| Unidad académica | | Subdirector(a) de Escuela | Fecha de elaboración |
|---|---|---|---|
| Escuela de Informática y Telecomunicaciones | | Oscar Araya | Noviembre, 2024 |

| Nombre experto(a) disciplinar | Nombre diseñador(a) curricular | Nombre diseñador(a) instruccional | Analista Instruccional |
|---|---|---|---|
| Juan Roa | Natasha Aude | Roxana Acevedo | |

| Aporte de valor del programa (no SENCE) |
|---|
| La acelerada expansión de las tecnologías de la información ha evidenciado un importante aumento de la superficie vulnerable en las infraestructuras informáticas de las organizaciones, lo que supone riesgos de ciberseguridad en diversas industrias. Esto ha provocado que las organizaciones inviertan en mecanismos y protocolos de seguridad defensiva, con el fin de garantizar la protección de los activos de información en el ciberespacio, precisando una actualización permanente de quienes se encuentran a cargo de la defensa en ciberseguridad.<br><br>Este curso está orientado a que los participantes adquieran competencias referidas a la protección de los activos de información de las organizaciones, por medio de técnicas y herramientas que permitan estructurar un modelo de defensa a recomendar, implementando los controles de seguridad y monitoreo pertinentes, conforme a la identificación y respuesta a los incidentes de ciberseguridad que se produzcan. |

| Caracterización del Participantes |
|---|
| Personas que posean 3 años de experiencia laboral en el área.<br>Analistas, arquitectos y administradores de ciberseguridad, y/o personas que hayan estudiado una carrera afín en Informática, redes o telecomunicaciones. |

| Requisitos de ingresos participantes |
|---|
| Los participantes deben poseer conocimientos previos en:<br>Redes (networking).<br>Sistemas operativos (Linux y Windows).<br>Conocimientos básicos de seguridad (controles de seguridad).<br>Inglés nivel básico en nivel de lectura. |
| Requerimientos de Hardware: Procesador Intel de 2.0 GHz (preferible Core dúo) - 1 Gb Memoria RAM (preferible 2 Gb) - Espacio libre en el disco duro de 1 Gb. |

Requerimientos de Software para participante del curso: Windows 7 o Mac OS X - Office 2007 para Windows u Office 2008 para Mac - Navegador de Internet (Chrome, Firefox y Safari versión para Mac). Internet Explorer no es compatible con la versión actual de Blackboard. - Instalación de programa para visualizar archivos PDF e instalación de herramientas de ofimática.

| Competencia a desarrollar / Objetivo General |
|---|
| Aplicar medidas de ciberseguridad de activos de información de acuerdo a ciberespacio de la organización. |

| Unidades | Objetivo Específico | Contenidos | T | P (60%) |
|---|---|---|---|---|
| **UNIDAD 1**<br><br>Entendiendo los modelos de defensa | Reconocer modelos de defensa de ciberseguridad con base en distintos escenarios operativos. | **Modelos de Defensa:**<br>● Defensa en profundidad<br>● Seguridad por capas<br><br>**Frameworks y guías de buenas prácticas disponibles**<br><br>● **CIS CONTROLS**<br>● **NIST**<br>● **ISO 27001 / 27032** | 4 | 6 |
| **UNIDAD 2**<br><br>Aplicando un modelo de ciberseguridad defensiva | Aplicar medidas de ciberseguridad defensiva como medio de continuidad operacional de la organización. | **Seguridad por capas: Características de las capas del modelo**<br><br>● Medidas de prevención<br>● Medidas de detección<br>● Medidas de contención<br>● Medidas de reacción<br>● Medidas de Recopilación evidencia/monitoreo de incidentes | 6 | 14 |
| | | Subtotal | 10 | 20 |
| | | Total | 30 | |

| Estrategias Metodológicas para la Implementación del Curso |
|---|
| **Metodologías de entrega de contenidos**: Al término de este curso, los participantes podrán aplicar medidas de ciberseguridad a los activos de información en el ciberespacio, incorporando buenas prácticas y normativa vigente. La estrategia metodológica se basa en la auto instrucción a través de un programa 100% e-learning asincrónico. El proceso de enseñanza y aprendizaje se desarrollará mediante diversos recursos organizados en el Ambiente Virtual de Aprendizaje de Duoc UC para que los participantes adquieran conocimientos de manera significativa y dinámica. Dichos recursos pueden ser: videos interactivos, guías interactivas, infografías, PDF descargable u otros; a través de los cuales se presentarán los contenidos de forma contextualizada y representativa según la realidad laboral de los participantes. El material estará disponible en formatos audiovisuales y descargables. Además, en cada unidad se realizarán actividades formativas mediante análisis de casos, cuestionarios y resolución de problemas. |

El curso tiene una duración total de 30 horas distribuidas en 6 semanas, considerando una dedicación semanal de máximo 5 horas. Además, se realizarán encuentros sincrónicos (opcionales) que permitirán a los participantes resolver dudas, profundizar en temas de interés y compartir experiencias con los demás participantes y facilitador.

**Descripción de las unidades:**

**Unidad 1:** Los participantes reconocerán diversas propuestas de modelos de defensa de ciberseguridad con el fin de cubrir los distintos escenarios en que las organizaciones operan en el ámbito tecnológico. Se desarrollarán actividades de análisis de brecha GAP, en base a un caso específico, y dependiendo del tipo de organización.

**Unidad 2:** Los participantes implementarán un modelo de ciberseguridad defensiva con el fin de minimizar los riesgos que puedan afectar a los activos de información, permitiendo la continuidad operacional de la organización. Los participantes deberán proponer medidas y planes de acción derivados del análisis de brecha y priorización del modelo de ciberseguridad de una organización. Para finalizar el curso, los participantes deberán implementar el modelo de ciberseguridad defensiva propuesto aplicando estándares de evaluación de madurez de ciberseguridad en una organización y justificando la correcta mantención y ajuste del modelo implementado.

| **Estrategias Evaluativas del Curso** | | |
|---|---|---|
| CRITERIOS DE EVALUACIÓN<br><br>**Unidad 1**<br><br>1. Evalúa patrones de comportamiento relativos a la ciberseguridad de la organización.<br><br>2. Selecciona estándares de buenas prácticas y controles que justifiquen la propuesta de un modelo de defensa en profundidad en la organización.<br><br>**Unidad 2**<br><br>1. Prioriza las brechas de cumplimiento de los estándares en base a los riesgos detectados en los activos de la organización.<br><br>2. Propone un modelo de defensa en profundidad que fundamenta la resolución de | INSTRUMENTOS DE EVALUACIÓN<br><br>Al comenzar el curso, el docente realizará una **evaluación diagnóstica** de conceptos claves durante la primera sesión, con el fin de consensuar el nivel de conocimientos previos de los participantes.<br><br>**Unidad 1:**<br><br>Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, con base en la selección de estándares y buenas prácticas asociadas a diversos escenarios y comportamientos operativos de la organización.<br>Ponderación: 30%.<br><br>**Unidad 2:**<br><br>Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, con base en la aplicación de medidas de un modelo de ciberseguridad defensiva como medio de continuidad operacional de la organización en un caso hipotético.<br>Ponderación: 30%. | NORMAS DE APROBACIÓN<br><br>Las calificaciones derivadas de la evaluación sumativa del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. Se corregirá el producto presentado por medio de una rúbrica. |

| | | |
|---|---|---|
| las brechas de ciberseguridad detectadas en la organización.<br><br>**<u>Evaluación Final</u>**<br><br>1. Justifica los criterios de implementación el modelo de ciberseguridad defensiva en función de los análisis previos.<br><br>2. Aplica herramientas para medir la efectividad del modelo de ciberseguridad defensiva implementado. | **Evaluación final:**<br>Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, de un modelo de ciberseguridad defensiva aplicando estándares de evaluación de madurez de ciberseguridad.<br><br>Ponderación: 40% | |

| **Requisito de aprobación** | |
|---|---|
| Modalidad a distancia – Asincrónico | 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)** |
| Plataforma LMS Blackboard. Sistema de videoconferencia online Collaborate integrado a plataforma. | | | **Requerimientos de Hardware:** Procesador Intel de 2.0 GHz (preferible Core dúo) - 1 Gb Memoria RAM (preferible 2 Gb) - Espacio libre en el disco duro de 1 Gb.<br><br>**Requerimientos de Software para participante del curso:** Windows 7 o Mac OS X - Office 2007 para Windows u Office 2008 para Mac - Navegador de Internet (Chrome, Firefox y Safari versión para Mac). Internet Explorer no es compatible con | | Material en formato digital<br><br>Sesiones relacionadas al contenido del curso en formato descargable.<br><br>Evaluaciones y pautas de corrección. |

| | | | | | |
|---|---|---|---|---|---|
| | | | la versión actual de Blackboard. - Instalación de programa para visualizar archivos PDF e instalación de herramientas de ofimática.<br><br>Conexión a Internet de banda ancha.<br><br>Parlantes o audífonos para el desarrollo del curso.<br><br>Micrófono. | | |

| **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** | Ciberseguridad en la Organización |
| | Gestión en Ciberseguridad |
| | **Seguridad Defensiva** |
| | Seguridad Ofensiva |

| **RECURSOS DOCENTES: PERFIL DESARROLLADOR** | |
|---|---|
| **PROFESIÓN** | Ingeniero en Informática |
| **AÑOS DE EXPERIENCIA** | 20 años |
| **CONOCIMIENTOS Y HABILIDADES RELEVANTES** | Conocimientos en ciberseguridad, estrategia, planificación, gestión de riesgo. |
| **OBSERVACIONES** | |
| | |

| RECURSOS DOCENTE: PERFIL RELATOR | |
|---|---|
| **PROFESIÓN** | Ingeniero en telecomunicaciones, Ingeniero en Informática, Ingeniero civil. |
| **AÑOS DE EXPERIENCIA** | al menos 5 años |
| **CONOCIMIENTOS Y HABILIDADES RELEVANTES** | Conocimientos en ciberseguridad, estrategia, planificación, gestión de riesgo. |
| **OBSERVACIONES** | |

# Ficha Programa No Conducente a Título (PNCT)

| Nombre del curso | Vacantes | Horas totales | Modalidad factible |
|---|---|---|---|
| Ciberseguridad Ofensiva | 1 | 30 | Online asincrónico |

| Identificación |
|---|
| Código SENCE |
| Código curso DuocUC |

| Unidad académica | Subdirector(a) de Escuela | Fecha de elaboración |
|---|---|---|
| Escuela de Informática y Telecomunicaciones | Oscar Araya | Noviembre, 2024 |

| Nombre experto(a) disciplinar | Nombre diseñador(a) curricular | Nombre diseñador(a) instruccional | Analista Instruccional |
|---|---|---|---|
| Jaime Gómez | Natasha Aude | Roxana Acevedo | Javier Canales |

| Aporte de valor del programa (no SENCE) |
|---|
| Las organizaciones han tenido un gran aumento en el uso de las tecnologías de información en el último tiempo, lo que trae consigo un incremento de los ciberataques, por ello, es primordial contar con mecanismos y protocolos para proteger sus activos de información. Para esto, es importante que existan especialistas que analicen constantemente la seguridad de una organización desde el punto de vista de los atacantes, los cuales, sean capaces de construir herramientas de ataque personalizado con el fin de evidenciar fallas y vulnerabilidades, que contribuyan a aumentar la capacidad de detección a través de la explotación con el fin de obtener evidencias y corregirlas oportunamente.<br><br>Este curso está orientado a que los participantes adquieran competencias que les permitan proponer un plan de mitigación, por medio de la evaluación de la capacidad que tiene una organización para proteger sus activos críticos en tiempo real, medir sus capacidades de detección y respuesta, considerando el plano tecnológico, de procesos y el factor humano. |

| Caracterización del Participantes |
|---|
| Personas que posean 3 años de experiencia laboral en el área.<br>Analistas, arquitectos de ciberseguridad, administradores de ciberseguridad, Pentester y/o personas que hayan estudiado una carrera afín en Informática, redes o telecomunicaciones. |

| Requisitos de ingresos participantes |
|---|
| Los participantes deben poseer conocimientos previos en:<br>Redes (networking).<br>Sistemas operativos (Linux y Windows).<br>Conocimientos básicos de seguridad (controles de seguridad).<br>Inglés nivel básico en nivel de lectura. |
| Sistema Operativo Windows 10 o superior; iOS 11 o posterior<br>Memoria RAM: 16 GB o más<br>Procesador: velocidad de 2 GHz o superior<br>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/).

| Competencia a desarrollar / Objetivo General |
|---|
| Aplicar medidas de un plan de mitigación de brechas de ciberseguridad de acuerdo a las necesidades de la organización. |

| Unidades | Objetivo Específico | Contenidos | T | P (60%) |
|---|---|---|---|---|
| **UNIDAD 1**<br><br>Descubrimiento de activos de información | Reconocer vulnerabilidades de las versiones de aplicaciones y sistemas operativos instaladas en la red de una empresa. | ● Búsqueda de información en fuentes abiertas<br>● Reconocimiento activo<br>● Enumeración<br>● Análisis de vulnerabilidades | 4 | 8 |
| **UNIDAD 2**<br><br>Explotación de vulnerabilidades | Aplicar medidas de un plan de mitigación de brechas de ciberseguridad con base en las vulnerabilidades encontradas.<br>. | ● Explotación sobre sistemas operativos (Windows, Linux)<br>● Explotación sobre aplicaciones web<br>● Inyección SQL<br>● Ingeniería Social<br>● Hacking de red<br>● Reporte de Plan de Mitigación | 6 | 12 |
| | | Subtotal | 10 | 20 |
| | | Total | 30 | |

| Estrategias Metodológicas para la Implementación del Curso |
|---|
| **Metodologías de entrega de contenidos**: Al término de este curso, los participantes podrán aplicar medidas de un plan de mitigación de brechas de ciberseguridad de acuerdo a las necesidades de la organización. La estrategia metodológica se basa en la auto instrucción a través de un programa 100% e-learning asincrónico. El proceso de enseñanza y aprendizaje se desarrollará mediante diversos recursos organizados en el Ambiente Virtual de Aprendizaje de Duoc UC para que los participantes adquieran conocimientos de manera significativa y dinámica. Dichos recursos pueden ser: videos interactivos, guías interactivas, infografías, PDF descargable u otros; a través de los cuales se presentarán los contenidos de forma contextualizada y representativa según la realidad laboral de los participantes. El material estará disponible en formatos audiovisuales y descargables. Además, en cada unidad se realizarán actividades formativas mediante análisis de casos, cuestionarios y resolución de problemas. |

El curso tiene una duración total de 30 horas distribuidas en 6 semanas, considerando una dedicación semanal de máximo 5 horas. Además, se realizarán encuentros sincrónicos (opcionales) que permitirán a los participantes resolver dudas, profundizar en temas de interés y compartir experiencias con los demás participantes y facilitador.

**Descripción de unidades:**

**Unidad 1:** El participante utilizará herramientas que permiten reconocer las versiones de las aplicaciones y sistemas operativos que están instaladas en la red de una empresa y sus vulnerabilidades. Se desarrollará por medio de actividades que permitan descubrir, mediante una red simulada, los activos de información que posee la empresa, los cuales permiten detectar las brechas de seguridad por medio de la aplicación de herramientas, evidenciándose mediante la entrega de un reporte de inventario de activos de información con el detalle de las brechas de seguridad de un caso práctico.

**Unidad 2:** El participante determinará un plan de mitigación de brechas de ciberseguridad, tomando como base el objetivo el nivel de riesgo de las vulnerabilidades encontradas y de evidencias obtenidas a través del proceso de explotación. Durante el desarrollo de esta unidad, se desarrollan ejercicios de explotación en ambiente simulado en sistemas operativos, aplicaciones web, base de datos, entre otras, con el fin de que los participantes puedan elaborar un plan de mitigación a partir de casos prácticos. Para finalizar el curso, se evaluará por medio de la entrega del Plan de mitigación por parte de cada uno de los estudiantes.

| **Estrategias Evaluativas del Curso** | | |
|---|---|---|
| CRITERIOS DE EVALUACIÓN<br><br>**Unidad 1**<br><br>1. Utiliza fuentes de información: páginas web de proveedores donde se publiquen errores y defectos de los sistemas o aplicaciones.<br>2. Detecta vulnerabilidades por medio de simulaciones de ciberataques.<br>3. Utiliza técnicas de enumeración para imitar los ciberataques.<br>4. Utiliza las mismas técnicas y procedimientos que emplean los atacantes.<br>5. Clasifica las vulnerabilidades según indicadores de riesgo TI. | INSTRUMENTOS DE EVALUACIÓN<br><br>Al comenzar el curso, el docente realizará una **evaluación diagnóstica** de conceptos claves durante la primera sesión, con el fin de consensuar el nivel de conocimientos previos de los participantes.<br><br>**Unidad 1:**<br><br>Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, con base en el reconocimiento de las vulnerabilidades de las aplicaciones y sistemas operativos de la red de una empresa de un caso hipotético.<br>Ponderación: 30%.<br><br>**Unidad 2:**<br>Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, con base en la selección de medidas de mitigación a las distintas brechas de ciberseguridad encontradas.<br>Ponderación: 30%.<br><br>**Evaluación final:** | NORMAS DE APROBACIÓN<br><br>Las calificaciones derivadas de la evaluación sumativa del curso estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación del curso. Se corregirá el producto presentado por medio de una rúbrica. |

| | | |
|---|---|---|
| 6. Aporta información de priorización al plan de mitigación y clasificación de riesgo TI.<br><br>**<u>Unidad 2</u>**<br><br>1. Emplea una lista de chequeo de requerimientos de seguridad de la organización.<br><br>2. Detecta brechas para mitigar el riesgo de ciberataques a través de la explotación.<br><br>3. Identifica las rutas que un ciberatacante tomará.<br><br>4. Accede a los controladores de dominio, bases de datos, aplicaciones web y computadores de alto perfil.<br><br>5. Comprueba o refuta el impacto potencial de las vulnerabilidades detectadas.<br><br>6. Desarrolla herramientas y scripts para determinadas vulnerabilidades que faciliten el ataque.<br><br>7. Documenta los hallazgos y los momentos (día y hora) en que fue realizada cada intrusión.<br><br>8. Identifica los activos más y menos afectados ante un ciberataque.<br><br>**<u>Evaluación final</u>** | Actividad evaluativa: Hetero-evaluación con entrega de encargo, evaluado con rúbrica, de un plan de mitigación integral de brechas.<br>Ponderación: 40% | |

| | | |
|---|---|---|
| 1. Categoriza el alcance e impactos de los datos obtenidos.<br>2. Determina rankings de vulnerabilidades provistos por las herramientas de evaluación.<br>3. Realiza un resumen que está dirigido a cargos de alto nivel de la organización.<br>4. Incluye estadísticas y un diagnóstico preciso del estado de la seguridad del objetivo de la evaluación.<br>5. Realiza un mapeo de riesgos a través de una matriz que cuantifique todos los descubrimientos y vulnerabilidades detectadas.<br>6. Explica las consecuencias que puede implicar una vulnerabilidad detectada y documentada de todos los elementos afectados.<br>7. Indica recomendaciones cuya implementación permita solucionar los problemas identificados. | | |

| **Requisito de aprobación** | |
|---|---|
| Modalidad a distancia – Asincrónico | 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)** |

| | | | | | |
|---|---|---|---|---|---|
| Plataforma LMS Blackboard. Sistema de videoconferencia online Collaborate integrado a plataforma. | | | **Requerimientos de Hardware:** Procesador Intel de 2.0 GHz (preferible Core dúo) - 1 Gb Memoria RAM (preferible 2 Gb) - Espacio libre en el disco duro de 1 Gb.<br><br>**Requerimientos de Software para participante del curso:** Windows 7 o Mac OS X - Office 2007 para Windows u Office 2008 para Mac - Navegador de Internet (Chrome, Firefox y Safari versión para Mac). Internet Explorer no es compatible con la versión actual de Blackboard. - Instalación de programa para visualizar archivos PDF e instalación de herramientas de ofimática.<br><br>Conexión a Internet de banda ancha.<br><br>Parlantes o audífonos para el desarrollo del curso.<br><br>Micrófono. | | Material en formato digital<br><br>Sesiones relacionadas al contenido del curso en formato descargable.<br><br>Evaluaciones y pautas de corrección.<br><br>Metasploitable<br><br>Win 10<br><br>Kali |

| **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** | Ciberseguridad en la Organización |
| | Gestión en Ciberseguridad |
| | Seguridad Defensiva |
| | **Seguridad Ofensiva** |

| RECURSOS DOCENTES: PERFIL DESARROLLADOR | |
|---|---|
| **PROFESIÓN** | Ingeniero civil electrónico |
| **AÑOS DE EXPERIENCIA** | 25 años y 10 años de experiencia en seguridad ofensiva |
| **CONOCIMIENTOS Y HABILIDADES RELEVANTES** | Certificación CEH Máster, conocimientos en redes, seguridad, sistemas operativos, networking. |
| **OBSERVACIONES** | Experiencia en servicio de Hacking ético en diversas organizaciones e industrias. |
| | |

| RECURSOS DOCENTE: PERFIL RELATOR | |
|---|---|
| **PROFESIÓN** | Ingeniero en informática, Ingeniero en redes o carrera afín |
| **AÑOS DE EXPERIENCIA** | 5 años |
| **CONOCIMIENTOS Y HABILIDADES RELEVANTES** | Conocimientos en computación nivel medio, Pentesting, sistemas operativos (Windows Linux), redes de computadores. |
| **OBSERVACIONES** | Poseer certificaciones en Hacking ético (CEH, OSCP) |