**FUNDACIÓN INSTITUTO PROFESIONAL DUOC UC**

**VICERRECTORÍA ACADÉMICA**

**RESOLUCIÓN Nº18/2025**

**APRUEBA DIPLOMADO EN CIBERSEGURIDAD Y PROTECCIÓN DE DATOS**

**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 y Protección de Datos"**, cuyo texto se adjunta a continuación de esta resolución, el cual reemplaza al publicado en Resolución VRA Nº03, de fecha 04 de enero de 2022.

Comuníquese, publíquese y regístrese.

Santiago, mayo 14 de 2025.

Alejandra Silva Lafourcade
Firmado digitalmente por Alejandra Silva Lafourcade
Fecha: 2025.05.14 15:44:49 -04'00'

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

Kiyoshi Fukushi
Firmado digitalmente por Kiyoshi Fukushi
Fecha: 2025.05.15 09:52:07 -04'00'

**KIYOSHI FUKUSHI MANDIOLA**
VICERRECTOR ACADÉMICO

KFM/ASL/JMD/jda

**PRESENTACIÓN DE DIPLOMADO**

Señor:
Kiyoshi Fukushi M.
Vicerrector Académico
Duoc UC

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

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

Alejandra Acuña
Directora Escuela de Informática y Telecomunicaciones
Duoc UC

# DIPLOMADO EN CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

**Resumen:**

Diplomado de oferta empresa desarrollado por la Escuela de Informática y Telecomunicaciones para la empresa SONDA.

La ciberseguridad se ha convertido en un pilar fundamental para la protección de la información en organizaciones de todos los sectores. Con el crecimiento de las amenazas digitales, es imprescindible contar con profesionales capacitados en seguridad informática, gestión de riesgos, auditoría y cumplimiento legal.

Este diplomado abarca desde la aplicación de técnicas básicas de seguridad hasta el uso de herramientas avanzadas de ciberseguridad, permitiendo a los participantes fortalecer la protección de sistemas y datos frente a posibles ataques. Además, incluye la gestión de auditorías informáticas y el conocimiento del marco legal vigente, garantizando el cumplimiento de normativas como la Ley de Protección de Datos Personales.

El Diplomado tiene una duración de 120 horas cronológicas, en modalidad sincrónica.

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

| Nombre Módulos | Horas | % de la nota final de Diplomado |
|---|---|---|
| Aplicación de técnicas básicas de seguridad informática | 20 | 20% |
| Aplicación de técnicas de gestión de la seguridad informática | 30 | 25% |
| Aplicación de herramientas de ciberseguridad | 30 | 25% |
| Técnicas de Gestión de Auditoría Informática | 25 | 20% |
| Aplicación Del Marco Legal y Ley De Protección De Datos Personales | 15 | 10% |
| **TOTAL DE HORAS** | **120** | **100** |

El Diplomado está dirigido a administrativos, agentes técnicos de soporte, administradores de redes, sistemas y BBDD, administrativos y técnicos de Data Center.

**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 y Protección de Datos

**2. TOTAL DE HORAS**

120

**3. POBLACIÓN OBJETIVO**

El Diplomado está dirigido a administrativos, agentes técnicos de soporte, administradores de redes, sistemas y BBDD, administrativos y técnicos de Data Center.

**4. REQUISITOS DE INGRESO**

Experiencia comprobable en áreas relacionadas con tecnología, informática, sistemas o afines.

## 5. JUSTIFICACIÓN DE CREACIÓN

La ciberseguridad se ha convertido en un pilar fundamental para la protección de la información en organizaciones de todos los sectores. Con el crecimiento de las amenazas digitales, es imprescindible contar con profesionales capacitados en seguridad informática, gestión de riesgos, auditoría y cumplimiento legal. Este diplomado abarca desde la aplicación de técnicas básicas de seguridad hasta el uso de herramientas avanzadas de ciberseguridad, permitiendo a los participantes fortalecer la protección de sistemas y datos frente a posibles ataques. Además, incluye la gestión de auditorías informáticas y el conocimiento del marco legal vigente, garantizando el cumplimiento de normativas como la Ley de Protección de Datos Personales.

El Diplomado en Ciberseguridad ofrece una formación integral que combina teoría y práctica, brindando herramientas clave para la identificación, prevención y mitigación de riesgos digitales. A lo largo del programa, los participantes aprenderán a aplicar estrategias efectivas de gestión de seguridad, realizar auditorías informáticas y utilizar herramientas avanzadas para detectar vulnerabilidades. Asimismo, se profundiza en la normativa legal, permitiendo a los profesionales garantizar el cumplimiento de regulaciones en sus organizaciones y minimizar riesgos legales asociados a la seguridad de la información.

En un contexto laboral donde la protección de datos es una prioridad, este diplomado responde a la creciente demanda de expertos en ciberseguridad. Las organizaciones requieren profesionales capaces de implementar medidas de defensa ante ataques cibernéticos, gestionar auditorías de seguridad y asegurar el cumplimiento normativo. Este programa prepara a los participantes para enfrentar estos desafíos, potenciando su empleabilidad y aportando soluciones estratégicas a la seguridad digital en empresas e instituciones.

## 6. OBJETIVO GENERAL/ IDENTIFICACIÓN PERFIL DE SALIDA

Aplicar técnicas de ciberseguridad en contextos laborales de acuerdo con estándares y buenas prácticas de la industria.

| 7. UNIDAD ACADÉMICA | 8. FECHA |
|---|---|
| Escuela de Informática y Telecomunicaciones | 3-4-2025 |

## 8. REQUISITOS DE OBTENCIÓN

8.1 - Haber aprobado todos los cursos del diplomado

Aprobar los cinco cursos que componen el diplomado.

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

| Nombre de cada curso | Horas | % de la nota final del diplomado |
|---|---|---|
| Aplicación de técnicas básicas de seguridad informática | 20 | 20% |
| Aplicación de técnicas de gestión de la seguridad informática | 30 | 25% |
| Aplicación de herramientas de ciberseguridad | 30 | 25% |
| Técnicas de Gestión de Auditoría Informática | 25 | 20% |
| Aplicación Del Marco Legal y Ley De Protección De Datos Personales | 15 | 10% |
| | 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 a los cursos | Porcentaje asignado a la actividad evaluativa final |
|---|---|
| 100% | N/A |

## 9. MODALIDAD DE IMPARTICIÓN

| | Modalidad |
|---|---|
| Asincrónico | |
| Presencial | |
| Sincrónico | x |

Ficha Programa No Conducente a Título (PNCT)

| Nombre del curso | Vacantes Educación Continua | Vacantes SENCE | Horas totales | Modalidad factible |
|---|---|---|---|---|
| Aplicación de técnicas básicas de seguridad informática | 20 | 20 | 20 | E-Learning sincrónico |

| Identificación |
|---|
| Código SENCE: 1238076063 |
| Código Curso Duoc UC: |

| Unidad Académica | Subdirector(a) Unidad Académica | Fecha de elaboración |
|---|---|---|
| Escuela de Informática y Telecomunicaciones | Oscar Araya | 10/02/2025 |

| Especialista disciplinar | Diseñador(a) curricular | Diseñador(a) instruccional | Analista instruccional |
|---|---|---|---|
| Elisa Moran | | | Nersianit Sierra |

| Aporte de valor del curso (no SENCE) |
|---|
| En la era digital, la seguridad informática se ha convertido en un pilar fundamental para la protección de datos, infraestructuras tecnológicas y la continuidad operativa de las organizaciones. Con la creciente sofisticación de las amenazas cibernéticas y el aumento en la digitalización de los procesos, es esencial que los profesionales que gestionan información y recursos tecnológicos comprendan los principios básicos de seguridad informática.<br>Este curso proporciona una base sólida en fundamentos de ciberseguridad, normas y estándares de protección, estrategias para salvaguardar datos y prevención ante malware, aspectos clave para mitigar riesgos y reforzar la seguridad en cualquier entorno tecnológico. Al finalizar, los profesionales estarán mejor preparados para reconocer amenazas, implementar medidas preventivas y responder ante incidentes de seguridad, contribuyendo así a la estabilidad y resiliencia de las infraestructuras tecnológicas en sus organizaciones. |

| Caracterización del participante |
|---|
| Administrativos, agentes técnicos de soporte, administradores de redes, sistemas y BBDD, administrativos y técnicos de Data Center. |

| Requisitos de ingreso |
|---|
| • Conocimientos básicos de hardware y software de un computador.<br>• Conocimientos básicos del sistema operativo de dispositivos y entornos de red.<br>• Experiencia laboral de al menos 1 años en gestión de proyectos TI. |

| Requisitos técnicos |
|---|
| 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<br>Resolución de monitor: 1024 x 768 o superior.<br>Navegadores Recomendados: Google Crome (última versión), Mozilla Firefox (última versión), Microsoft Edge<br>Cámara, micrófono, parlantes y/o audífonos<br>Lector de PDF, como Adobe Acrobat Reader (adobe.com) o Foxit Reader (foxit.com)<br>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 |
|---|
| Aplicar procedimientos de seguridad de activos presentes en la infraestructura de la organización según estándares y buenas prácticas. |

| Unidad de aprendizaje | Resultados de aprendizaje | Contenidos | Horas | |
|---|---|---|---|---|
| | | | T | P |
| *Unidad 1: Ciberseguridad* | Identificar conceptos, normas y estándares de seguridad informática según los componentes de la infraestructura organizacional. | 1. **Fundamentos de la seguridad informática**<br>- Triada de la seguridad<br>- Ciberseguridad vs seguridad de la información<br>-Gestión GRC<br>- Amenazas, vulnerabilidades y riesgos<br>- Principios de Need to Know y Least Privilege<br>- Defensa en profundidad<br>-Modelo Deep Defense<br>-Modelo de Zero Trust<br>-Reconocimiento sistemas de la empresa o terceros<br><br>**2. Normas, estándares y recomendaciones de seguridad**<br>- Estándares, políticas y certificaciones de seguridad<br>- Necesidad de estándares<br>- Estándar ISO/IEC 27000 o Norma ISO/IEC 27001 o SGSI o Modelo PDCA<br>- Recomendaciones del NIST (CSF) - PCI DSS<br>-Ley de delitos informáticos.<br>-Ley marco de ciberseguridad.<br>- | 4 | 6 |

| | | | | |
|---|---|---|---|---|
| Unidad 2: Amenazas y ataques | Analizar estrategias y procedimientos de protección de datos considerando las amenazas del malware y las prácticas de la industria. | **3. Seguridad y estrategias de protección de datos**<br>- Clasificación de los datos<br>-Ley de protección de datos personales.<br>-Ley de Transparencia<br><br>**4. Malware**<br>- ¿Qué es el malware?<br>- Ciclo de vida del malware<br>- Evolución y estado actual del malware<br>- Tipos de malware<br>• Virus informáticos<br>• Adware<br>• Spywar<br>• Gusanos<br>• Ramsonware<br>-Herramientas para detección de malware<br>- Cyber Kill Chain<br>-Software antimalware<br>- Métodos de ataque y mitigación<br>- Spamming | 4 | 6 |
| | | **Subtotal** | 8 | 12 |
| | | **Horas totales** | 20 | |

**Estrategias metodológicas**

**Metodologías de entrega de contenidos:** Al término de este curso los participantes podrán: conocer la infraestructura de la organización para determinar cuáles son los procedimientos de seguridad que pueden implementar. El curso se desarrollará en modalidad *e-learning sincrónica a través del Ambiente Virtual de Aprendizaje de Duoc UC*. La estrategia metodológica será interactiva-expositiva, es decir, el facilitador presentará contenidos utilizando distintos recursos educativos tales como presentación power point, material audiovisual, recursos interactivos u otro tipo de documento, además desarrollará actividades enfocadas a la aplicación práctica de los contenidos. Entre los métodos de enseñanza y aprendizaje que se utilizarán, está la definición de conceptos clave, análisis de casos, resolución de problemas y ejercicios de aplicación donde los participantes deberán desarrollar actividades en forma individual o grupal. El desarrollo de los contenidos se dividirá en sesiones, cada una se realizará a través de una secuencia didáctica compuesta por cuatro momentos: Activación, Demostración, Aplicación e Integración.

**Descripción de unidades:**

**Unidad 1:** Esta unidad introduce los fundamentos de la seguridad informática, incluyendo modelos de defensa, gestión de riesgos y principios de acceso seguro. Además, se exploran normas y estándares clave como ISO/IEC 27001, el marco NIST y leyes de ciberseguridad, esenciales para la protección de la infraestructura organizacional. En cada una de las sesiones se aplicarán horas de laboratorio que se realizarán en vivo con el docente, a través de prácticas guiadas en los diferentes softwares y páginas.
**Unidad 2:** Se analizan estrategias de protección de datos y las principales amenazas cibernéticas, con un enfoque en malware, su ciclo de vida y métodos de detección. También se estudian regulaciones sobre

privacidad y técnicas de mitigación de ataques, permitiendo una respuesta eficaz ante riesgos digitales. En cada una de las sesiones se aplicarán horas de laboratorio que se realizarán en vivo con el docente, a través de prácticas guiadas en los diferentes softwares y páginas.

| **Estrategias evaluativas** | | |
|---|---|---|
| **Indicadores de logro** | **Instrumentos de evaluación** | **Normas de aprobación** |
| **Unidad 1** | | |
| • Identifica los componentes de la triada de seguridad según los fundamentos informáticos.<br>• Identifica causas y consecuencias de problemáticas de seguridad en TI.<br>• Reconoce las normas y estándares recomendadas para la seguridad informática.<br>• Menciona recomendaciones y buenas prácticas en la seguridad de los sistemas comprometidos. | La evaluación de la unidad 1 se espera que los participantes puedan desarrollar una actividad estilo cuestionario de 20 preguntas de selección simple, donde se espera que lean un caso de estudio y respondan según corresponda.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con Claves. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |
| **Unidad 2** | | |
| • Describe vulnerabilidades en un entorno de seguridad informática, considerando la precisión y la entrega completa de los datos solicitados.<br>• Analiza dominios sospechosos en relación con malware.<br>• Identifica el nivel de riesgo, hashes y tipos de archivos asociados a los dominios sospechosos.<br>• Describe las fases de Cyber Kill Chain según las fases y la relación con los incidentes de seguridad. | Los participantes a partir de un caso o una contextualización deberán realizar un dominio y analizar los procedimientos de protección de datos que se pueden realizar teniendo en cuenta las amenazas y las prácticas de la industria.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con una rúbrica. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |

| Requisito de aprobación | |
|---|---|
| Modalidad presencial y e-learning sincrónico | Asistencia Mínima de 75% de las horas totales del curso y nota mínima de aprobación 4.0 |
| Modalidad e-learning asincrónica | NA |

| Recursos para la implementación | | | | | |
|---|---|---|---|---|---|
| **Infraestructura** | **Indicar sede** | **Equipos y herramientas** | | **Material didáctico** | |
| Acceso a Aula Virtual Blackboard. | Curso de modalidad remota sincrónica | NA | Computadores con sistema operativo Windows, conexión a Internet y software específico instalado: rastreador de puertos (NMAP), analizador de protocolos (Wireshark), escáner de vulnerabilidades (NESSUS). | NA | Presentación de power point.<br><br>Evaluaciones |

| Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Unidad Académica) |
|---|
| 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** | **Aplicación de Técnicas Básicas de Seguridad Informática** |
| | Aplicación de Técnicas de Gestión de La Seguridad Informática |
| | Aplicación de Herramientas de Ciberseguridad |
| | Visión General de la Seguridad Informática |
| | Aplicación Del Marco Legal y Ley De Protección De Datos Personales |

| Otros cursos relacionados con la temática |
|---|
| NA |

| Recursos docentes: Perfil desarrollador | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable master o diplomados enfocados a la ciberseguridad y la seguridad ofensiva.<br>• Formación en conectividad y redes. |
| **Requisitos relativos a las habilidades** | • Deseable experiencia comprobable en diseño y ejecución de estrategias de seguridad y gobernanza de TI en organizaciones. |
| **Requisitos relativos a la experiencia** | Experiencia en proyectos de seguridad en TI como analista de seguridad, habilidades de relatoría, Certificaciones deseables CEH, eJPT o equivalentes. |

| Recursos docentes: Perfil relator | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable master o diplomados enfocados a la ciberseguridad y la seguridad ofensiva.<br>• Formación en conectividad y redes. |
| **Requisitos relativos a las habilidades** | Deseable conocimiento en normativas y estándares de seguridad (ISO/IEC 27001, NIST, PCI DSS) y en herramientas de análisis de malware y detección de amenazas. |
| **Requisitos relativos a la experiencia** | Experiencia en proyectos de seguridad en TI como analista de seguridad, habilidades de relatoría. |

| Nombre del curso | Vacantes Educación Continua | Vacantes SENCE | Horas totales | Modalidad factible |
|---|---|---|---|---|
| Aplicación de técnicas de gestión de la seguridad informática | 20 | 20 | 30 | E-Learning sincrónico |

| Identificación |
|---|
| Código SENCE: 1238076064 |
| Código Curso Duoc UC: |

| Unidad Académica | Subdirector(a) Unidad Académica | Fecha de elaboración |
|---|---|---|
| Escuela de Informática y Telecomunicaciones | Oscar Araya | 10/02/2025 |

| Especialista disciplinar | Diseñador(a) curricular | Diseñador(a) instruccional | Analista instruccional |
|---|---|---|---|
| Elisa Moran | | | Nersianit Sierra |

| Aporte de valor del curso (no SENCE) |
|---|
| En un mundo digitalizado, la seguridad informática es clave para proteger datos y sistemas. Las empresas requieren técnicas avanzadas para mitigar riesgos y responder a ciberataques. La demanda de expertos crece ante amenazas constantes y regulaciones más estrictas.<br><br>Implementarlas es un reto por la evolución de amenazas y la falta de conciencia empresarial. Contar con estas habilidades mejora la prevención de incidentes y aumenta la empleabilidad. La actualización constante es esencial para destacar en el mercado laboral.<br><br>Este curso ofrece práctica con casos reales y herramientas actualizadas. Se basa en estándares internacionales y certificaciones reconocidas. Además, brinda acceso a expertos y aplica metodologías innovadoras. |

| Caracterización del participante |
|---|
| Administrativos, agentes técnicos de soporte, administradores de redes, sistemas y BBDD, administrativos y técnicos de Data Center. |

| Requisitos de ingreso |
|---|
| • Conocimientos básicos de hardware y software de un computador.<br>• Conocimientos básicos del sistema operativo de dispositivos y entornos de red.<br>• Experiencia laboral de al menos 1 años en gestión de proyectos TI. |

| Requisitos técnicos |
|---|
| 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<br>Resolución de monitor: 1024 x 768 o superior.<br>Navegadores Recomendados: Google Crome (última versión), Mozilla Firefox (última versión), Microsoft Edge<br>Cámara, micrófono, parlantes y/o audífonos<br>Lector de PDF, como Adobe Acrobat Reader (adobe.com) o Foxit Reader (foxit.com)<br>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 |
|---|
| Aplicar técnicas de ciberseguridad en plataformas y redes de comunicación según los estándares establecidos. |

| Unidad de aprendizaje | Resultados de aprendizaje | Contenidos | Horas | |
|---|---|---|---|---|
| | | | T | P |
| *Unidad 1: Gestión de la Ciberseguridad* | Identificar soluciones y tecnologías de segurización de acuerdo con estándares y buenas prácticas de la industria. | 1. **Gestión de la seguridad en la arquitectura TI:**<br>- Elementos de la arquitectura TI<br>-Ciberamenazas y vuelnerabilidades<br>- Fundamentos de la seguridad en la arquitectura TI:<br>• Sistemas de información o bases de datos<br>• Sistemas operativos<br>- Los controles CIS y su implementación<br><br>2**. Gestión de identidades y accesos**<br>- Autenticación y autorización<br>- Autenticación robusta<br>- Métodos de control de acceso<br>- Tecnologías de gestión de accesos (Infraestructura de llave pública PKI, Oauth, OpenID, SAML, SPML)<br>-Gobierno de identidad<br>- Componentes comunes en arquitecturas de identidad centralizada | 8 | 10 |

| | | | | |
|---|---|---|---|---|
| Unidad 2: *Seguridad en Infraestructura y software* | Aplicar técnicas de seguridad informática de acuerdo con estándares y buenas prácticas de la industria. | 3. **Seguridad en infraestructuras TI**<br>- Seguridad en entornos Cloud<br>- Mecanismos de Control de Acceso a Red (NAC)<br>- Protocolos de seguridad<br>- Segurización de dispositivos (Hardening)<br>- Seguridad en bases de datos<br>- Seguridad de sistemas operativos<br>- Seguridad en redes Wifi<br>- Gestión de los accesos web<br>- DevSecOps.<br>- Etapas del ciclo de vida del desarrollo.<br>-Desarrollo Seguridad y Operación segura. | 5 | 7 |
| | | **Subtotal** | 13 | 17 |
| | | **Horas totales** | 30 | |

**Estrategias metodológicas**

**Metodologías de entrega de contenidos:** Al término de este curso los participantes podrán: gestionar la ciberseguridad en infraestructuras y software, siguiendo estándares y buenas prácticas de la industria. El curso se desarrollará en modalidad *e-learning sincrónica a través del Ambiente Virtual de Aprendizaje de Duoc UC*. La estrategia metodológica será interactiva-expositiva, es decir, el facilitador presentará contenidos utilizando distintos recursos educativos tales como presentación power point, material audiovisual, recursos interactivos u otro tipo de documento, además desarrollará actividades enfocadas a la aplicación práctica de los contenidos. Entre los métodos de enseñanza y aprendizaje que se utilizarán, está la definición de conceptos clave, análisis de casos, resolución de problemas y ejercicios de aplicación donde los participantes deberán desarrollar actividades en forma individual o grupal. El desarrollo de los contenidos se dividirá en sesiones, cada una se realizará a través de una secuencia didáctica compuesta por cuatro momentos: Activación, Demostración, Aplicación e Integración.

**Descripción de unidades:**

**Unidad 1:** En esta unidad, se analizan soluciones y tecnologías de ciberseguridad siguiendo estándares de la industria. Se practican la identificación de vulnerabilidades en la arquitectura TI, la implementación de controles CIS y la configuración segura de sistemas. Además, se aplican métodos de autenticación robusta, gestión de accesos con PKI, OAuth y SAML, y estrategias de gobierno de identidad para fortalecer la seguridad.

**Unidad 2:** En esta unidad, se aplican técnicas de seguridad en infraestructuras y software siguiendo estándares de la industria. Se practican medidas de hardening, control de acceso a redes, protección en entornos cloud y gestión segura de bases de datos y sistemas operativos. Además, se implementan estrategias DevSecOps para integrar seguridad en el desarrollo de software y operación segura.

| Estrategias evaluativas | | |
|---|---|---|
| **Indicadores de logro** | **Instrumentos de evaluación** | **Normas de aprobación** |
| **Unidad 1** | | |
| • Identifica los principios de seguridad en la arquitectura TI.<br>• Comprende conceptos claves relacionados a la seguridad TI.<br>• Identifica la implementación de los controles CIS según corresponda.<br>• Reconoce los métodos de control de acceso según corresponde.<br>• Reconoce los componentes comunes en arquitecturas de identidad centralizada. | La evaluación de la unidad 1 se espera que los participantes puedan desarrollar una actividad estilo cuestionario de 24 preguntas de selección simple, donde se espera que lean un caso de estudio y respondan según corresponda.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con Claves. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |
| **Unidad 2** | | |
| • Propone mejoras de seguridad a la arquitectura TI de acuerdo al contexto.<br>• Construye un modelo de defense in Depth según sus etapas, defensas y representación gráfica.<br>• Aplica la segurización de dispositivos según el hardening del caso.<br>• Aplica la seguridad de software considerando los controles e impacto asociado. | Los participantes a partir de un caso o una contextualización deberán aplicar técnicas de seguridad de dispositivos y de software.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con una rúbrica. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |

| Requisito de aprobación | |
|---|---|
| Modalidad presencial y e-learning sincrónico | Asistencia Mínima de 75% de las horas totales del curso y nota mínima de aprobación 4.0 |
| Modalidad e-learning asincrónica | NA |

| Recursos para la implementación | | | | | |
|---|---|---|---|---|---|
| **Infraestructura** | **Indicar sede** | **Equipos y herramientas** | | **Material didáctico** | |
| Acceso a Aula Virtual Blackboard. | Curso de modalidad | NA | Computadores con sistema operativo Windows, conexión | NA | Presentación de power point. |

| | | | | | |
|---|---|---|---|---|---|
| | remota sincrónica | | a Internet y software específico instalado: Programas/librerías de cifrado (OpenSSL y herramientas basadas en PGP), Packet-Tracer. | | Evaluaciones |

| **Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Unidad Académica)** |
|---|
| 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** | Aplicación de Técnicas Básicas de Seguridad Informática |
| | **Aplicación de Técnicas de Gestión de La Seguridad Informática** |
| | Aplicación de Herramientas de Ciberseguridad |
| | Visión General de la Seguridad Informática |
| | Aplicación Del Marco Legal y Ley De Protección De Datos Personales |

| **Otros cursos relacionados con la temática** |
|---|
| NA |

| **Recursos docentes: Perfil desarrollador** | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable Certificaciones en ciberseguridad (CISSP, CISM, CEH, CompTIA Security+, ISO 27001, entre otras). |
| **Requisitos relativos a las habilidades** | • Deseable experiencia comprobable en diseño y ejecución de estrategias de seguridad y gobernanza de TI en organizaciones. |
| **Requisitos relativos a la experiencia** | • Deseable al menos 3 años de experiencia en ciberseguridad, administración de infraestructuras seguras o desarrollo seguro.<br>• Experiencia en implementación de controles de seguridad y evaluación de vulnerabilidades. |

| Recursos docentes: Perfil relator | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable master o diplomados enfocados a la ciberseguridad y la seguridad ofensiva.<br>• Deseable Certificaciones en ciberseguridad (CISSP, CISM, CEH, CompTIA Security+, ISO 27001, entre otras). |
| **Requisitos relativos a las habilidades** | • Dominio de gestión de seguridad en infraestructuras TI, hardening y DevSecOps.<br>• Conocimientos en gestión de identidades, control de accesos y protección de redes y sistemas.<br>• Capacidad para aplicar metodologías prácticas y basadas en estándares internacionales. |
| **Requisitos relativos a la experiencia** | • Deseable al menos 2 años de experiencia en ciberseguridad, administración de infraestructuras o desarrollo seguros.<br>• Deseable antecedentes en docencia, formación corporativa o capacitaciones técnicas en seguridad informática. |

Ficha Programa No Conducente a Título (PNCT)

| Nombre del curso | Vacantes Educación Continua | Vacantes SENCE | Horas totales | Modalidad factible |
|---|---|---|---|---|
| Aplicación de herramientas de ciberseguridad | 20 | 20 | 30 | E-Learning sincrónico |

| Identificación |
|---|
| Código SENCE: 1238076065 |
| Código Curso Duoc UC: |

| Unidad Académica | Subdirector(a) Unidad Académica | Fecha de elaboración |
|---|---|---|
| Escuela de Informática y Telecomunicaciones | Oscar Araya | 17/02/2025 |

| Especialista disciplinar | Diseñador(a) curricular | Diseñador(a) instruccional | Analista instruccional |
|---|---|---|---|
| Elisa Moran | | | Nersianit Sierra |

**Aporte de valor del curso (no SENCE)**

En un mundo altamente digitalizado, la gestión de la seguridad de la información es esencial para proteger datos y mitigar ciberataques. Empresas de todos los sectores requieren profesionales capacitados en análisis de amenazas y respuesta a incidentes. La demanda de expertos en ciberseguridad sigue en aumento debido al crecimiento constante de las amenazas.

Sin embargo, la rápida evolución de las vulnerabilidades y la falta de protocolos efectivos dificultan la protección de los sistemas. Contar con habilidades en análisis de malware, detección de intrusiones y respuesta a incidentes es clave para minimizar riesgos. La formación en normativas y herramientas especializadas mejora la empleabilidad en este campo.

Este curso se diferencia por su enfoque práctico en análisis de vulnerabilidades, uso de herramientas actualizadas y estrategias basadas en estándares internacionales. Además, ofrece capacitación en la confección de playbooks y gestión de incidentes, proporcionando conocimientos aplicables de inmediato en entornos empresariales.

**Caracterización del participante**

Administrativos, agentes técnicos de soporte, administradores de redes, sistemas y BBDD, administrativos y técnicos de Data Center.

**Requisitos de ingreso**

- Conocimientos básicos de hardware y software de un computador.
- Conocimientos básicos del sistema operativo de dispositivos y entornos de red.

- Experiencia laboral de al menos 1 años en gestión de proyectos TI.

| Requisitos técnicos |
|---|
| 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<br>Resolución de monitor: 1024 x 768 o superior.<br>Navegadores Recomendados: Google Crome (última versión), Mozilla Firefox (última versión), Microsoft Edge<br>Cámara, micrófono, parlantes y/o audífonos<br>Lector de PDF, como Adobe Acrobat Reader (adobe.com) o Foxit Reader (foxit.com)<br>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 |
|---|
| Usar herramientas de ciberseguridad ante las amenazas y vulnerabilidades presentes en la infraestructura TI. |

| Unidad de aprendizaje | Resultados de aprendizaje | Contenidos | Horas | |
|---|---|---|---|---|
| | | | T | P |
| *Unidad 1: Herramientas y técnicas de análisis de vulnerabilidades* | Identificar características relevantes de las amenazas y vulnerabilidades presentes en la infraestructura TI. | 1.**Análisis y gestión de vulnerabilidades**<br>• Clasificación de Vulnerabilidades (CVSS 4)<br>• Herramientas y técnicas de análisis de vulnerabilidades<br>• Proceso de gestión de parches<br><br>**2. Monitoreo, detección de amenazas e intrusiones**<br>• Amenazas y contramedidas a nivel de red<br>• Amenazas y contramedidas a nivel de Software (Owasp TO10)<br>• Metodologías de detección de intrusiones<br>• Técnicas de detección de intrusiones en hosts y redes<br>• Movimiento lateral<br>• Modelo ATT&CK | 8 | 12 |

| | | | | |
|---|---|---|---|---|
| Unidad 2: | Aplicar procedimiento de respuestas ante incidentes de TI (Playbook) según los estándares del CSIRT y la planificación de la organización. | **3.Respuesta a Incidentes**<br>• ¿Qué es un incidente de seguridad?<br>• Equipo de Respuesta a Incidentes CSIRT. Procesos del CSIRT.<br>• Herramientas de soporte del CSIRT.<br>• ISO 27035.<br>• NIST SP800-61r2.<br>• Definición de un plan de respuesta a incidentes.<br>• Confección de Playbooks.<br>• Vectores de ataque<br>• Ransomware<br>• Contención de daños.<br>• Análisis de causa raíz. | 4 | 6 |
| | | **Subtotal** | 12 | 18 |
| | | **Horas totales** | 30 | |

**Estrategias metodológicas**

**Metodologías de entrega de contenidos:** Al término de este curso los participantes podrán usar la dirección y la gestión de sistemas de seguridad de la información en empresas, con el fin de promover e implementar estrategias capaces de blindar datos, información y el conocimiento de la organización, de acuerdo con estándares, normativas y buenas prácticas de la industria. El curso se desarrollará en modalidad *e-learning sincrónica a través del Ambiente Virtual de Aprendizaje de Duoc UC*. La estrategia metodológica será interactiva-expositiva, es decir, el facilitador presentará contenidos utilizando distintos recursos educativos tales como presentación power point, material audiovisual, recursos interactivos u otro tipo de documento, además desarrollará actividades enfocadas a la aplicación práctica de los contenidos. Entre los métodos de enseñanza y aprendizaje que se utilizarán, está la definición de conceptos clave, análisis de casos, resolución de problemas y ejercicios de aplicación donde los participantes deberán desarrollar actividades en forma individual o grupal. El desarrollo de los contenidos se dividirá en sesiones, cada una se realizará a través de una secuencia didáctica compuesta por cuatro momentos: Activación, Demostración, Aplicación e Integración.

**Descripción de unidades:**

**Unidad 1:** Los participantes aplicarán técnicas para identificar, clasificar y gestionar vulnerabilidades en la infraestructura TI. Se realizarán prácticas de análisis con herramientas especializadas, detección de amenazas en redes y software (OWASP Top 10), y simulaciones de ataques basadas en el modelo ATT&CK. También se trabajará en la gestión de parches y la implementación de contramedidas para fortalecer la seguridad.

**Unidad 2:** Se abordarán procedimientos para mitigar intrusiones y minimizar daños en entornos empresariales. Se practicarán la configuración y operación de equipos CSIRT, la aplicación de normativas como ISO 27035 y NIST SP800-61r2, y la confección de playbooks para distintos escenarios de ataque. Además, se realizarán ejercicios de análisis de causa raíz y contención de incidentes en entornos simulados.

| Estrategias evaluativas | | |
|---|---|---|
| **Indicadores de logro** | **Instrumentos de evaluación** | **Normas de aprobación** |
| **Unidad 1** | | |
| • Identifica la funcionalidad e importancia del CVSS en el contexto TI.<br>• Clasifica las categorías de las técnicas y tácticas utilizadas por los atacantes.<br>• Reconoce el objetivo de la gestión de vulnerabilidades según cada acción.<br>• Reconoce los procesos de. monitoreo, detección de amenazas e intrusiones | La evaluación de la unidad 1 se espera que los participantes puedan desarrollar una actividad estilo cuestionario de 24 preguntas de selección simple, donde se espera que lean un caso de estudio y respondan según corresponda.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con Claves. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |
| **Unidad 2** | | |
| • Describe las etapas del proceso e información relevante del caso.<br>• Desarrolla el playbook del incidente considerando los aspectos relevantes.<br>• Describe los vectores asociados al ransomware considerando el caso propuesto.<br>• Aplica herramientas de soporte del CSIRT según el contexto dado. | Los participantes a partir de un caso o una contextualización deberán desarrollar un Paybook y en base a ello, definir criterios que ayuden con la identificación de pasos acerca la atención del incidente.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con una rúbrica. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |

| Requisito de aprobación | |
|---|---|
| Modalidad presencial y e-learning sincrónico | Asistencia Mínima de 75% de las horas totales del curso y nota mínima de aprobación 4.0 |
| Modalidad e-learning asincrónica | NA |

| Recursos para la implementación | | | |
|---|---|---|---|
| **Infraestructura** | **Indicar sede** | **Equipos y herramientas** | **Material didáctico** |

| | | | | | |
|---|---|---|---|---|---|
| Acceso a Aula Virtual Blackboard. | Curso de modalidad remota sincrónica | NA | Computadores con sistema operativo Windows, conexión a Internet. Máquinas virtuales para Windows Server 2012-2016, RHEL 6-7. | NA | Presentación de power point.<br><br>Evaluaciones |

| **Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Unidad Académica)** |
|---|
| 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** | Aplicación de Técnicas Básicas de Seguridad Informática |
| | Aplicación de Técnicas de Gestión de La Seguridad Informática |
| | **Aplicación de Herramientas de Ciberseguridad** |
| | Visión General de la Seguridad Informática |
| | Aplicación Del Marco Legal y Ley De Protección De Datos Personales |

| **Otros cursos relacionados con la temática** |
|---|
| NA |

| **Recursos docentes: Perfil desarrollador** | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable Certificaciones en ciberseguridad (CEH, CISSP, OSCP, CompTIA Security+, ISO 27001). |
| **Requisitos relativos a las habilidades** | • Conocimiento en respuesta a incidentes, CSIRT y normativas como ISO 27035 y NIST SP800-61r2.<br>• Capacidad para desarrollar estrategias de seguridad y confección de playbooks. |

| | |
|---|---|
| **Requisitos relativos a la experiencia** | • Deseable al menos 3 años de experiencia en análisis de malware, gestión de incidentes y ciberseguridad.<br>• Deseable experiencia en monitoreo de amenazas, mitigación de ataques y gestión de parches. |

| **Recursos docentes: Perfil relator** | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable master o diplomados enfocados a la ciberseguridad y la seguridad ofensiva.<br>• Deseable Certificaciones en ciberseguridad (CEH, CISSP, OSCP, CompTIA Security+, ISO 27001).<br>• Deseables antecedentes en docencia, formación corporativa o capacitaciones técnicas en seguridad informática. |
| **Requisitos relativos a las habilidades** | • Conocimiento en respuesta a incidentes, CSIRT y normativas como ISO 27035 y NIST SP800-61r2. |
| **Requisitos relativos a la experiencia** | • Deseable al menos 2 años de experiencia en ciberseguridad, administración de infraestructuras o desarrollo seguros. |

| Nombre del curso | Vacantes Educación Continua | Vacantes SENCE | Horas totales | Modalidad factible |
|---|---|---|---|---|
| Técnicas de Gestión de Auditoría Informática | 20 | 20 | 25 | E-Learning sincrónico |

| Identificación |
|---|
| Código SENCE: 1238076066 |
| Código Curso Duoc UC: |

| Unidad Académica | Subdirector(a) Unidad Académica | Fecha de elaboración |
|---|---|---|
| Escuela de Informática y Telecomunicaciones | Oscar Araya | 10/02/2025 |

| Especialista disciplinar | Diseñador(a) curricular | Diseñador(a) instruccional | Analista instruccional |
|---|---|---|---|
| Elisa Moran | | | Nersianit Sierra |

| Aporte de valor del curso (no SENCE) |
|---|
| Sin duda que la información se ha convertido en el activo más valioso para muchas de las organizaciones, en la actualidad los datos se constituyen como un elemento esencial para generar competitividad y elevados márgenes de rentabilidad para los negocios modernos.<br><br>Luego, las empresas, independientemente de su tamaño, están realizando grandes esfuerzos en custodiar la información desde su origen hasta su aprovechamiento para las operaciones y para la toma de decisiones.<br><br>Este curso se desarrolla como consecuencia principalmente de la relevancia que han tomado en la actualidad tanto la gestión, el almacenamiento y la transmisión de información y de grandes volúmenes de datos en las organizaciones, ya sean estas de carácter público o privado, en los distintos sectores de la industria, como el Financiero, Retail, Salud, Defensa, Proveedores de servicios, etc.<br><br>Luego, en este contexto, los procesos de evaluación y adquisición de soluciones tecnológicas de seguridad, las auditorias de seguridad y las técnicas de análisis forense se vuelven cada vez más importantes como herramientas de verificación y protección de la información en la organización. |

| Caracterización del participante |
|---|
| Administrativos, agentes técnicos de soporte, administradores de redes, sistemas y BBDD, administrativos y técnicos de Data Center. |

| Requisitos de ingreso |
|---|
| • Conocimientos básicos de hardware y software de un computador.<br>• Conocimientos básicos del sistema operativo de dispositivos y entornos de red. |

- Experiencia laboral de al menos 1 años en gestión de proyectos TI.

| Requisitos técnicos |
|---|
| 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<br>Resolución de monitor: 1024 x 768 o superior.<br>Navegadores Recomendados: Google Crome (última versión), Mozilla Firefox (última versión), Microsoft Edge<br>Cámara, micrófono, parlantes y/o audífonos<br>Lector de PDF, como Adobe Acrobat Reader (adobe.com) o Foxit Reader (foxit.com)<br>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 |
|---|
| Aplicar procedimientos de seguridad, auditoría e informática forense de acuerdo con estándares y buenas prácticas de la industria. |

| Unidad de aprendizaje | Resultados de aprendizaje | Contenidos | Horas | |
|---|---|---|---|---|
| | | | T | P |
| *Unidad 1: Evaluación y selección de sistemas de seguridad* | Identificar características e indicadores de los sistemas de seguridad según los procesos y estándares establecidos. | **1. Evaluación y selección de sistemas de seguridad**<br>- Soluciones en seguridad de la información<br>- Tecnologías de seguridad de la información<br>- Características EDR<br>- Riesgos y vulnerabilidades en la cadena de suministros<br>- Evaluación de soluciones y tecnologías de seguridad | 3 | 5 |
| Unidad 2: Auditoria de sistemas e informática forense | Aplicar auditoría e informática forense de acuerdo con estándares y buenas prácticas de la industria. | **2. Auditoria de sistemas**<br>- Seguridad interna y perimetral<br>-Navegación segura<br>-Gestión de conexiones seguras<br>-Detección de intrusos<br>-Autenticación<br>- Auditoria web<br>- Principales iniciativas de OWASP<br>- Seguridad en la configuración del servidor<br>- Acreditaciones y certificaciones<br>- Certified Information Systems Auditor (CISA)<br>- Gestión de remediaciones | 6 | 11 |

| | | | | |
|---|---|---|---|---|
| | | - Certified Information Security Manager (CISM)<br>-Certified Information Systems Security Professional (CISSP)<br><br>**3. Informática forense**<br>- Preservación de la evidencia digita<br>-Legislación y normativas<br>- Diferencias entre informática forense y ciberseguridad<br>- Fundamentos de la informática forense<br>- Adquisición forense<br>- Análisis forense<br>- Artefactos forenses comunes en sistemas operativos<br>- Análisis de encabezados (Headers)<br>- Análisis de correo electrónico<br>- Análisis de memoria | | |
| | | | **Subtotal** | 9 | 16 |
| | | | **Horas totales** | 25 | |

| **Estrategias metodológicas** |
|---|
| **Metodologías de entrega de contenidos:** Al término de este curso los participantes podrán: Aplicar soluciones tecnológicas, auditoria e informática forense para su adecuada gestión en la infraestructura ti de la organización, que permitan asegurar la continuidad operacional de los servicios de la misma, de acuerdo con estándares y buenas prácticas de la industria. El curso se desarrollará en modalidad *e-learning sincrónica a través del Ambiente Virtual de Aprendizaje de Duoc UC*. La estrategia metodológica será interactiva-expositiva, es decir, el facilitador presentará contenidos utilizando distintos recursos educativos tales como presentación power point, material audiovisual, recursos interactivos u otro tipo de documento, además desarrollará actividades enfocadas a la aplicación práctica de los contenidos. Entre los métodos de enseñanza y aprendizaje que se utilizarán, está la definición de conceptos clave, análisis de casos, resolución de problemas y ejercicios de aplicación donde los participantes deberán desarrollar actividades en forma individual o grupal. El desarrollo de los contenidos se dividirá en sesiones, cada una se realizará a través de una secuencia didáctica compuesta por cuatro momentos: Activación, Demostración, Aplicación e Integración.<br><br>**Descripción de unidades:**<br><br>**Unidad 1:** Se analizan tecnologías y soluciones de seguridad de la información, incluyendo EDR y evaluación de vulnerabilidades en la cadena de suministro. Prácticas: Implementación y comparación de herramientas de seguridad, identificación de riesgos y análisis de tecnologías de protección.<br><br>**Unidad 2:** Se aplican auditorías de seguridad y procesos forenses según estándares de la industria, abordando OWASP, autenticación y certificaciones como CISA y CISSP. Prácticas: Simulación de auditorías |

| |
|---|
| web, detección de intrusos, análisis de evidencias digitales, adquisición forense y análisis de memoria y correos electrónicos. |

| **Estrategias evaluativas** | | |
|---|---|---|
| **Indicadores de logro** | **Instrumentos de evaluación** | **Normas de aprobación** |
| **Unidad 1** | | |
| • Identifica el tipo de cifrado según su utilidad.<br>• Identifica soluciones tecnológicas según el objetivo de la empresa.<br>• Reconoce la importancia del sistema informático según el contexto organizacional.<br>• Reconoce indicadores de gestión aplicado en sistemas informáticos. | La evaluación de la unidad 1 se espera que los participantes puedan desarrollar una actividad estilo cuestionario de 20 preguntas de selección simple, donde se espera que lean un caso de estudio y respondan según corresponda.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con Claves. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |
| **Unidad 2** | | |
| • Desarrolla propuestas de seguridad perimetral considerando el impacto en la implementación.<br>• Describe los pasos relevantes de la implementación de un SGSI.<br>• Explica el análisis forense y de adquisición considerando la presentación a las autoridades.<br>• Aplica procedimientos de seguridad en fuentes de correo electrónico. | Los participantes a partir de un caso o una contextualización deberán aplicar técnicas de seguridad utilizando informática forense y de adquisición.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con una rúbrica. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |

| **Requisito de aprobación** | |
|---|---|
| Modalidad presencial y e-learning sincrónico | Asistencia Mínima de 75% de las horas totales del curso y nota mínima de aprobación 4.0 |
| Modalidad e-learning asincrónica | NA |

| **Recursos para la implementación** | | | |
|---|---|---|---|
| **Infraestructura** | **Indicar sede** | **Equipos y herramientas** | **Material didáctico** |

| | | | | | |
|---|---|---|---|---|---|
| Acceso a Aula Virtual Blackboard. | Curso de modalidad remota sincrónica | NA | Computadores con sistema operativo Windows, conexión a Internet y software específico instalado: Programas/librerías de cifrado (OpenSSL y herramientas basadas en PGP), Packet-Tracer. | NA | Presentación de power point.<br><br>Evaluaciones |

| **Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Unidad Académica)** |
|---|
| 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** | Aplicación de Técnicas Básicas de Seguridad Informática |
| | Aplicación de Técnicas de Gestión de La Seguridad Informática |
| | Aplicación de Herramientas de Ciberseguridad |
| | **Técnicas de Gestión de Auditoría Informática** |
| | Aplicación Del Marco Legal y Ley De Protección De Datos Personales |

| **Otros cursos relacionados con la temática** |
|---|
| NA |

| **Recursos docentes: Perfil desarrollador** | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable Certificaciones en ciberseguridad (CISSP, CISM, CEH, CompTIA Security+, ISO 27001, entre otras). |
| **Requisitos relativos a las habilidades** | • Deseable dominio de tecnologías de seguridad, auditoría de sistemas y análisis forense digital. |

| | |
|---|---|
| **Requisitos relativos a la experiencia** | • Deseable al menos 3 años en ciberseguridad, auditoría de sistemas o informática forense.<br>• Experiencia en implementación de soluciones de seguridad, evaluaciones de vulnerabilidades y gestión de incidentes. |

| **Recursos docentes: Perfil relator** | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable master o diplomados enfocados a la ciberseguridad y la seguridad ofensiva.<br>• Deseable Certificaciones en ciberseguridad (CISSP, CISM, CEH, CompTIA Security+, ISO 27001, entre otras). |
| **Requisitos relativos a las habilidades** | • Deseable conocimientos en evaluación de riesgos, gestión de remediaciones y estándares OWASP. |
| **Requisitos relativos a la experiencia** | • Deseable al menos 2 años de experiencia en ciberseguridad, administración de infraestructuras o desarrollo seguros.<br>• Deseables antecedentes en docencia, formación corporativa o capacitaciones técnicas en seguridad informática. |

| Nombre del curso | Vacantes Educación Continua | Vacantes SENCE | Horas totales | Modalidad factible |
|---|---|---|---|---|
| Aplicación del marco legal y ley de protección de datos personales | 20 | 20 | 15 | E-Learning sincrónico |

| Identificación |
|---|
| Código SENCE: 1238076376 |
| Código Curso Duoc UC: |

| Unidad Académica | Subdirector(a) Unidad Académica | Fecha de elaboración |
|---|---|---|
| Escuela de Informática y Telecomunicaciones | Oscar Araya | 10/02/2025 |

| Especialista disciplinar | Diseñador(a) curricular | Diseñador(a) instruccional | Analista instruccional |
|---|---|---|---|
| Ricardo Garaté | | | Nersianit Sierra |

| Aporte de valor del curso (no SENCE) |
|---|
| Sin duda que la información se ha convertido en el activo más valioso para muchas de las organizaciones, en la actualidad los datos se constituyen como un elemento esencial para generar competitividad y elevados márgenes de rentabilidad para los negocios modernos.<br><br>Luego, las empresas, independientemente de su tamaño, están realizando grandes esfuerzos en custodiar la información desde su origen hasta su aprovechamiento para las operaciones y para la toma de decisiones. Este curso se desarrolla como consecuencia principalmente de la relevancia que han tomado en la actualidad tanto la gestión, el almacenamiento y la transmisión de información y de grandes volúmenes de datos en las organizaciones, ya sean estas de carácter público o privado, en los distintos sectores de la industria, como el Financiero, Retail, Salud, Defensa, Proveedores de servicios, etc.<br><br>Luego, en este contexto, el marco legal y la protección de los datos personales se vuelven cada vez más importantes como parte de las premisas y directrices que persiguen la protección de la información, por ejemplo, de clientes y personal de la organización. |

| Caracterización del participante |
|---|
| Administrativos, agentes técnicos de soporte, administradores de redes, sistemas y BBDD, administrativos y técnicos de Data Center. |

| Requisitos de ingreso |
|---|
| • Conocimientos básicos de hardware y software de un computador.<br>• Conocimientos básicos del sistema operativo de dispositivos y entornos de red.<br>• Experiencia laboral de al menos 1 años en gestión de proyectos TI. |

| Requisitos técnicos |
|---|
| 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<br>Resolución de monitor: 1024 x 768 o superior.<br>Navegadores Recomendados: Google Crome (última versión), Mozilla Firefox (última versión), Microsoft Edge<br>Cámara, micrófono, parlantes y/o audífonos<br>Lector de PDF, como Adobe Acrobat Reader (adobe.com) o Foxit Reader (foxit.com)<br>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 |
|---|
| Aplicar técnicas de preservación de datos personales según leyes nacionales e internacionales de la seguridad de la información. |

| Unidad de aprendizaje | Resultados de aprendizaje | Contenidos | Horas | |
|---|---|---|---|---|
| | | | T | P |
| *Unidad 1: Marco legal y regulatorio* | Identificar el marco legal y regulatorio de la seguridad de la información considerando las entidades nacionales e internacionales. | **1. Marco legal y regulatorio**<br>- Generalidades del ciberespacio<br>-Derechos informáticos y digitales<br>- Seguridad de la información en la empresa<br>- Norma de seguridad de la información (ISO 27.001)<br><br>**2. Marco normativo internacional:**<br>- Convenio de Budapest<br>- Reglamento General de Protección de Datos Personales de la UE<br>-Reglamento de inteligencia artificial de la UE).<br><br>**3. Estrategia de transformación Digital de Chile 2035**<br>- Política Nacional de Ciberseguridad.<br>- Política Nacional de Inteligencia Artificial.<br>-Ley Marco de Ciberseguridad (Ley Nº 21.663)<br><br>**4. Agencia Nacional de Ciberseguridad**<br>(Funciones, responsabilidades, servicios esenciales, operadores de importancia vital, | 4 | 4 |

| | | | | |
|---|---|---|---|---|
| | | infracciones, sanciones y plazos para informar incidentes).<br>**5. Los delitos informáticos**<br>- Ley relativas al delito informático (Ley N°21.459)<br>-Ley de propiedad intelectual N° 17.336<br>-Ley de Firma digital (Ley 19.799)<br>-Contratos electrónicos e informáticos.<br><br>**6. Las TIC en el contexto de las relaciones laborales** | | |
| *Unidad 2: Protección de datos personales* | Aplicar técnicas de preservación de datos personales según la ley de protección de datos personales. | **7. Protección de datos personales**<br>- Datos de carácter personal<br>- Datos sensibles<br>- Ley de tratamiento de datos personales (Ley 20.575)<br>- Ley de protección de datos personales (Ley 19.628)<br>- Principios y derechos de la LPDP chilena<br><br>**8. Agencia de protección de datos**<br>- Personales (funciones, responsabilidades, servicios esenciales, operadores de importancia vital, infracciones, sanciones y plazos para informar incidentes).<br>- Consentimiento y tratamiento de datos<br>- Regulación y derechos del titular de datos<br>-Privacidad en la nube | 3 | 4 |
| | | **Subtotal** | 7 | 8 |
| | | **Horas totales** | 15 | |

| **Estrategias metodológicas** |
|---|
| **Metodologías de entrega de contenidos:** Al término de este curso los participantes podrán: gestionar la ciberseguridad en infraestructuras y software, siguiendo estándares y buenas prácticas de la industria. El curso se desarrollará en modalidad *e-learning sincrónica a través del Ambiente Virtual de Aprendizaje de Duoc UC*. La estrategia metodológica será interactiva-expositiva, es decir, el facilitador presentará contenidos utilizando distintos recursos educativos tales como presentación power point, material audiovisual, recursos interactivos u otro tipo de documento, además desarrollará actividades enfocadas a la aplicación práctica de los contenidos. Entre los métodos de enseñanza y aprendizaje que se utilizarán, está la definición de conceptos clave, análisis de casos, resolución de problemas y ejercicios de aplicación donde los participantes deberán desarrollar actividades en forma individual o grupal. El desarrollo de los contenidos se dividirá en sesiones, cada una se realizará a través de una secuencia didáctica compuesta por cuatro momentos: Activación, Demostración, Aplicación e Integración.<br><br>**Descripción de unidades:** |

**Unidad 1:** En esta unidad, los participantes conocerán el marco normativo que rige la seguridad de la información, abordando normativas internacionales como el Convenio de Budapest y el RGPD, así como leyes nacionales sobre ciberseguridad, delitos informáticos y propiedad intelectual. Prácticas: Análisis de casos legales en seguridad de la información, evaluación de contratos electrónicos y revisión de políticas empresariales según la normativa vigente.

**Unidad 2:** Se explorarán las leyes de protección de datos personales, incluyendo la Ley 19.628 y la Ley 20.575, con un enfoque en derechos, consentimiento y regulación de la privacidad en entornos digitales. Prácticas: Simulación de cumplimiento normativo en empresas, evaluación de políticas de privacidad en la nube y análisis de procedimientos para el tratamiento seguro de datos personales.

| **Estrategias evaluativas** | | |
|---|---|---|
| **Indicadores de logro** | **Instrumentos de evaluación** | **Normas de aprobación** |
| **Unidad 1** | | |
| • Identifica los mecanismos de protección del Convenio de Budapest y RGPDP de la UE.<br>• Identifica la importancia y las característica del derecho digital.<br>• Reconoce los principios del derecho informático según los procesos regulatorios. | La evaluación de la unidad 1 se espera que los participantes puedan desarrollar una actividad estilo cuestionario de 15 preguntas de selección simple, donde se espera que lean un enunciado y respondan según corresponda.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con Claves. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |
| **Unidad 2** | | |
| • Menciona los actos ilícitos presentados en el caso de estudio.<br>• Clasifica los datos personales según la normativa.<br>• Aplica los principios de la Ley de Protección de datos personales según los estándares establecidos. | Los participantes a partir de un caso o una contextualización deberán analizar e identificar los actos ilícitos y sugerir la aplicación de la Ley de Protección de datos personales.<br><br>La evaluación será individual, se desarrollará en la plataforma con retroalimentación automática y se corregirá con una rúbrica. | Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación.<br><br>Ponderación: 50% |

| **Requisito de aprobación** |
|---|

| | |
|---|---|
| Modalidad presencial y e-learning sincrónico | Asistencia Mínima de 75% de las horas totales del curso y nota mínima de aprobación 4.0 |
| Modalidad e-learning asincrónica | NA |

| Recursos para la implementación | | | | | |
|---|---|---|---|---|---|
| **Infraestructura** | **Indicar sede** | **Equipos y herramientas** | | **Material didáctico** | |
| Acceso a Aula Virtual Blackboard. | Curso de modalidad remota sincrónica | NA | Computadores con sistema operativo Windows, conexión a Internet. | NA | Presentación de power point.<br><br>Evaluaciones |

| **Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Unidad Académica)** |
|---|
| 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** | Aplicación de Técnicas Básicas de Seguridad Informática |
| | Aplicación de Técnicas de Gestión de La Seguridad Informática |
| | Aplicación de Herramientas de Ciberseguridad |
| | Técnicas de Gestión de Auditoría Informática |
| | **Aplicación Del Marco Legal y Ley De Protección De Datos Personales** |

| **Otros cursos relacionados con la temática** |
|---|
| NA |

| **Recursos docentes: Perfil desarrollador** | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable Certificaciones en ciberseguridad (CISSP, CISM, CEH, CompTIA Security+, ISO 27001, entre otras). |
| **Requisitos relativos a las habilidades** | • Deseable experiencia comprobable en diseño y ejecución de estrategias de seguridad y gobernanza de TI en organizaciones. |

| | |
|---|---|
| **Requisitos relativos a la experiencia** | • Deseable al menos 3 años de experiencia en ciberseguridad, administración de infraestructuras seguras o desarrollo seguro.<br>• Experiencia en implementación de controles de seguridad y evaluación de vulnerabilidades. |

| **Recursos docentes: Perfil relator** | |
|---|---|
| **Requisitos relativos a la educación** | Ingeniero en informática, ingeniero en redes, ingeniero en seguridad informática, ingeniero de sistemas y/o profesiones afines. |
| **Requisitos relativos a la formación** | • Deseable master o diplomados enfocados a la ciberseguridad y la seguridad ofensiva.<br>• Deseable Certificaciones en ciberseguridad (CISSP, CISM, CEH, CompTIA Security+, ISO 27001, entre otras). |
| **Requisitos relativos a las habilidades** | • Dominio de gestión de seguridad en infraestructuras TI, hardening y DevSecOps.<br>• Conocimientos en gestión de identidades, control de accesos y protección de redes y sistemas.<br>• Capacidad para aplicar metodologías prácticas y basadas en estándares internacionales. |
| **Requisitos relativos a la experiencia** | • Deseable al menos 2 años de experiencia en ciberseguridad, administración de infraestructuras o desarrollo seguros.<br>• Deseable antecedentes en docencia, formación corporativa o capacitaciones técnicas en seguridad informática. |