FUNDACIÓN INSTITUTO PROFESIONAL DUOC UC

VICERRECTORÍA ACADÉMICA

RESOLUCIÓN Nº03/2026

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.

Comuníquese, publíquese y regístrese.

Santiago, enero 26 de 2026.

ALEJANDRA SILVA LAFOURCADE
DIRECTORA GENERAL DE DESARROLLO
ESTUDIANTIL Y EDUCACIÓN CONTINUA

MAURICIO FARÍAS ARENAS
VICERRECTOR ACADÉMICO

/jmd

PRESENTACIÓN DE DIPLOMADO

Señor:
Gastón Ramos V.
Vicerrector Académico (i)
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 de eClass en su alianza con Educación Continua de Duoc UC.

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

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

DIPLOMADO EN CIBERSEGURIDAD

Resumen:

Diplomado de oferta abierta desarrollado por la Escuela de Informática y Telecomunicaciones en nuestra alianza con eClass.

En un contexto marcado por una acelerada transformación digital y por un fortalecimiento sin precedentes del marco regulatorio chileno, la ciberseguridad se ha convertido en una prioridad estratégica para organizaciones públicas y privadas. La promulgación de la Ley Marco de Ciberseguridad (Ley 21.663), la Ley 21.459 sobre delitos informáticos y las reformas a la Ley de Protección de Datos han configurado una nueva institucionalidad que exige profesionales capaces de comprender, aplicar y gestionar estos marcos legales para proteger la información y la continuidad operacional.

En este escenario, el Diplomado en Ciberseguridad busca dar respuesta a esta necesidad entregando una formación integral que articula los pilares normativos, técnicos y de gestión. El programa aborda en profundidad el marco legal chileno en ciberseguridad y protección de datos, el diseño e implementación de controles y estrategias de gestión de riesgos, el uso de herramientas oficiales y marcos de respuesta ante incidentes, así como el análisis y visualización de grandes volúmenes de datos de seguridad (logs, alertas, eventos SIEM) para la toma de decisiones informada. Junto con ello, incorpora el estudio de amenazas emergentes —como el uso de IA en ciberataques, los ataques a la cadena de suministro y los impactos potenciales de la computación cuántica— para anticipar escenarios de alta criticidad.

Asimismo, el diplomado integra una mirada estratégica y operativa de la ciberseguridad, orientada a que las y los participantes puedan diseñar e implementar políticas, procedimientos y arquitecturas de seguridad —incluyendo enfoques como Zero Trust— alineadas a los objetivos del negocio y a las exigencias regulatorias.

El diplomado tiene una duración de 256 horas cronológicas, en modalidad asincrónica. Para obtener el diplomado, los participantes deberán aprobar los cuatro cursos según la siguiente ponderación:

Nombre de cursos	Horas	% de la nota final de diplomado
ASPECTOS LEGALES DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS	64	25%
SEGURIDAD COMPUTACIONAL EN LA ORGANIZACIÓN	64	25%
VISUALIZACIÓN DE DATOS APLICADA A LA CIBERSEGURIDAD	64	25%
TENDENCIAS Y FUTURO DE LA CIBERSEGURIDAD	64	25%
Total de horas	**256**	**100%**

El diplomado está dirigido a profesionales y técnicos de diversas áreas que requieren fortalecer o incorporar la ciberseguridad en su ámbito laboral. Esto incluye a profesionales y técnicos de áreas de TI, ciberseguridad, redes y sistemas. Además de analistas de SOC, jefes de TI, administradores de plataformas SIEM, Oficiales de Seguridad (CISO), personal de cumplimiento y auditores, así como asesores legales o de riesgo involucrados en el cumplimiento normativo.

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

DuocUC EDUCACIÓN CONTINUA

FICHA ÚNICA DE CREACIÓN DE DIPLOMADOS
PNCT

1. NOMBRE DEL DIPLOMADO

DIPLOMADO EN CIBERSEGURIDAD

2. TOTAL DE HORAS

256 horas

3. POBLACIÓN OBJETIVO

Profesionales y técnicos de áreas de TI, ciberseguridad, redes y sistemas. Esto incluye Analistas de SOC, Jefes de TI, administradores de plataformas SIEM, Oficiales de Seguridad (CISO), personal de cumplimiento y auditores, así como asesores legales o de riesgo involucrados en el cumplimiento normativo.

4. REQUISITOS DE INGRESO

Se recomienda contar con conocimientos básicos en tecnologías de la información (TI), redes de datos, sistemas operativos o fundamentos de ciberseguridad.

5. JUSTIFICACIÓN DE CREACIÓN

La acelerada transformación digital y el nuevo marco normativo chileno han consolidado la ciberseguridad como una prioridad estratégica para el sector público y privado. La promulgación de la Ley Marco de Ciberseguridad (Ley 21.663), la Ley 21.459 sobre delitos informáticos y la reforma a la Ley de Protección de Datos han creado una institucionalidad robusta que exige profesionales capaces de comprender, aplicar y gestionar estos marcos legales. El Diplomado en Ciberseguridad responde a esta necesidad entregando una formación integral que incluye conocimientos actualizados sobre normativas, herramientas oficiales de respuesta ante incidentes, y estrategias prácticas de cumplimiento regulatorio.

El diplomado prepara a las y los profesionales para gestionar la ciberseguridad de forma integral. Aborda el fortalecimiento del marco legal chileno (Ley 21.663) y la protección de datos, la implementación de estrategias técnicas de seguridad organizacional (controles, gestión de riesgos), la capacidad de analizar y visualizar grandes volúmenes de datos de seguridad (logs, alertas SIEM), y la preparación ante amenazas emergentes como la IA en ciberataques, ataques a la cadena de suministro y la computación cuántica.

Asimismo, el programa aborda la seguridad desde una perspectiva técnica y operativa, considerando las amenazas actuales y futuras. Desde el diseño de estrategias organizacionales para la protección de datos y la gestión de incidentes, hasta la interpretación de grandes volúmenes de información mediante visualización aplicada, el diplomado forma profesionales capaces de responder eficazmente a un ecosistema de amenazas en constante evolución. El enfoque en tendencias emergentes —como la Inteligencia Artificial, Zero Trust y computación cuántica— permite anticiparse a los desafíos que vienen, entregando a los participantes herramientas para liderar procesos de ciberdefensa en entornos complejos y de alta criticidad.

6. OBJETIVO GENERAL/ IDENTIFICACIÓN PERFIL DE SALIDA

La o el egresado será capaz de gestionar la ciberseguridad de forma integral, aplicando la normativa chilena vigente, diseñando e implementando estrategias de seguridad organizacional (como controles de acceso, gestión de riesgos y auditoría), utilizando técnicas de visualización de datos para la detección y respuesta a incidentes, y analizando amenazas emergentes (como IA, ataques a la cadena de suministro y riesgos cuánticos) para aplicar estrategias proactivas.

7. UNIDAD ACADÉMICA	8. FECHA
Informática y Telecomunicaciones	9-12-2025

9. REQUISITOS DE OBTENCIÓN

9.1 - Haber aprobado todos los cursos del diplomado

La nota mínima de aprobación para cada curso es de 4.0.

9.2 - 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
ASPECTOS LEGALES DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS	64	25%
SEGURIDAD COMPUTACIONAL EN LA ORGANIZACIÓN	64	25%
VISUALIZACIÓN DE DATOS APLICADA A LA CIBERSEGURIDAD	64	25%
TENDENCIAS Y FUTURO DE LA CIBERSEGURIDAD	64	25%
Total de horas	**256**	**100%**

9.3 - Convalidación con programas académicos de Educación Continua

Nombre de cada curso	CC	Horas	% de la nota final del diplomado
Total de horas		**0**	**0%**

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

9.4 - Articulación con programas de Unidad Académica

Nombre de cada programa académico	CC	Horas	% de la nota final del diplomado
Total de horas		**0**	**0%**

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

10. MODALIDAD DE IMPARTICIÓN

	Modalidad
Asincrónico	X
Presencial	
Sincrónico	

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
ASPECTOS LEGALES DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS	50	1	64	Online asincrónica con sesión sincrónica

Identificación
Código SENCE:
Código Curso Duoc UC:

Unidad Académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Informática y Telecomunicaciones	Oscar Araya	17-12-2025

Especialista disciplinar	Analista instruccional
Claudio González P.	Diego Acosta

Aporte de valor del curso (no SENCE)
En Chile, el fortalecimiento de la institucionalidad en ciberseguridad y protección de datos ha adquirido carácter urgente y estratégico. La promulgación de la **Ley Marco de Ciberseguridad (Ley 21.663)** en abril de 2024 establece un nuevo estándar legal para la coordinación, prevención y respuesta ante incidentes digitales, creando la **Agencia Nacional de Ciberseguridad (ANCI)** y definiendo obligaciones concretas para organismos públicos y privados. Esta ley se articula con la **Ley 21.459 sobre delitos informáticos** y la reforma a la **Ley 19.628 sobre protección de datos personales**, conformando un ecosistema normativo robusto que exige preparación técnica, jurídica y ética. El curso “Aspectos legales de ciberseguridad y protección de datos” entrega a las y los participantes una comprensión actualizada y aplicada del marco legal chileno en esta materia, abordando tanto las obligaciones legales como los desafíos éticos que surgen en entornos digitales. Este curso permite a las y los participantes fortalecer su capacidad de respuesta ante vulneraciones legales, aportar valor estratégico a sus organizaciones y contribuir activamente a la construcción de un entorno digital más seguro, ético y resiliente.

Caracterización del participante
Este curso está dirigido a personas que se desempeñan en funciones de cumplimiento normativo, gestión de riesgos, seguridad de la información, tecnologías de la información y asesoría legal en organizaciones públicas y privadas. En particular, está orientado a **encargados de protección de datos, analistas de ciberseguridad, oficiales de cumplimiento, responsables de seguridad TI, asesores jurídicos con foco en entornos digitales y profesionales que lideran procesos de adaptación normativa en materia de ciberseguridad y privacidad.**

Requisitos de ingreso
Se recomienda contar con conocimientos básicos en tecnologías de la información, derecho informático o experiencia laboral en áreas afines. Idealmente haber cursado un módulo introductorio en fundamentos de ciberseguridad o protección de datos.

Requisitos técnicos
Sistema Operativo Windows 10 o superior; iOS 11 o posterior Memoria RAM: mínimo 8 GB, recomendado 16 GB o más Procesador: 4 Cores y velocidad de 2 GHz o superior Tarjeta de sonido Resolución de monitor: 1024 x 768 o superior. Navegadores Recomendados: Google Chrome (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
Aplicar la normativa chilena vigente en ciberseguridad y protección de datos personales en contextos organizacionales, mediante el uso de herramientas legales y digitales, en condiciones de cumplimiento normativo, prevención de riesgos y promoción de una cultura de seguridad digital.

Unidad de aprendizaje	Resultados de aprendizaje	Contenidos	Horas	
			T	P
1. Fundamentos legales de la ciberseguridad	Identificar los principios jurídicos y normativos que sustentan la ciberseguridad en Chile.	• Ley 21.459 sobre delitos informáticos. • Ley 21.663 Marco de Ciberseguridad y Principios de legalidad, proporcionalidad y responsabilidad. • Rol del CSIRT nacional. • Normativa internacional relevante (Budapest, GDPR). • Agencia Nacional de Ciberseguridad (ANCI) • Agencia de Protección de Datos Personales (APDP)	4	6
2. Protección de datos personales	Reconocer los derechos, obligaciones y procedimientos asociados a la protección de datos personales.	• Ley 19.628 y su reforma. • Principios de licitud, finalidad, proporcionalidad. • Consentimiento y derechos ARCO. • Agencia de Protección de Datos.	4	6

3. Responsabilidad legal y gestión de incidentes	Reconocer la normativa vigente ante incidentes de seguridad y vulneraciones de datos.	• Tipificación de delitos informáticos. • Obligaciones de reporte. • Responsabilidad civil, penal y administrativa. • Protocolos de respuesta. • Operadores de importancia vital (OIV)	4	6
4. Cumplimiento normativo y auditoría	Reconocer estrategias de cumplimiento normativo en ciberseguridad y protección de datos.	• Modelos de cumplimiento. • Auditorías legales. • ISO 27001, NIST, CMF. • Evaluación de impacto en protección de datos. • Ley Marco de Ciberseguridad • Ley N.º 21.719 de Protección de Datos Personales	4	6
5. Derechos digitales y ética en el entorno digital	Reconocer los desafíos éticos y legales en el uso de tecnologías digitales.	• Derechos digitales, vigilancia, consentimiento informado. • Inteligencia artificial y sesgos. • Ética del tratamiento de datos.	4	6
6. Herramientas legales y plataformas oficiales	Aplicar herramientas digitales y legales en iniciativas de aseguramiento del cumplimiento normativo.	• Plataforma CMF, CSIRT, Agencia de Protección de Datos. • Simulación de reportes, matrices de cumplimiento, análisis de jurisprudencia.	4	6
7. Seminario	Aplicar estrategias legales y normativas en casos reales de ciberseguridad y protección de datos.	• Evaluación final integradora con simulación de caso, matriz legal, informe de cumplimiento y plan de respuesta.	—	4
		Subtotal	24	40
		Horas totales	64	

Estrategias metodológicas
Metodologías de entrega de contenidos: El curso se desarrollará en modalidad e-learning asincrónica a través del Ambiente Virtual de Aprendizaje (AVA) de eClass. Para esta modalidad, el proceso formativo se desarrollará mediante recursos educativos auto instruccionales tales como videos interactivos, guías interactivas, podcasts, video tutoriales, infografías, PDFs u otros, los cuales presentarán los contenidos de forma contextualizada y representativa según la realidad laboral de los participantes. Los recursos educativos estarán disponibles en versión audiovisual y/o descargable para garantizar flexibilidad en el acceso y aprovechamiento del contenido. Además, se desarrollarán evaluaciones formativas enfocadas en la aplicación práctica de los contenidos, buscando vincular el aprendizaje teórico con situaciones laborales reales: • Videos explicativos y tutoriales

- Infografías legales y normativas
- Podcast con expertos
- Guías interactivas y simulaciones
- Actividades prácticas basadas en casos reales
- Evaluaciones formativas con retroalimentación automatizada

A lo largo del curso, se utilizarán metodologías activas y estrategias de enseñanza-aprendizaje centradas en la participación, la reflexión crítica y la aplicación práctica del marco legal vigente en ciberseguridad y protección de datos. Estas metodologías permitirán a los participantes desenvolverse en escenarios reales y simulados, fortaleciendo su capacidad de análisis, toma de decisiones y adaptación al contexto normativo nacional.

- Se trabajará con **casos reales de vulneraciones de datos** y situaciones legales actuales en el ámbito nacional y latinoamericano, permitiendo a los participantes analizar incidentes, aplicar principios legales clave y evaluar la responsabilidad jurídica en distintos niveles (penal, civil y administrativo). Estas experiencias estarán acompañadas del uso de plataformas oficiales como el CSIRT nacional, la Comisión para el Mercado Financiero (CMF) y la Agencia de Protección de Datos Personales.
- Se incorporarán **simulaciones y ejercicios prácticos**, tales como la respuesta institucional ante un ataque de ransomware, la evaluación de impacto en protección de datos (EIPD), reportes ficticios de incidentes, y auditorías legales internas. Estas simulaciones permitirán a los participantes aplicar las normas legales vigentes —incluyendo la Ley 21.663, Ley 21.459 y la Ley 19.628 reformada— a contextos específicos, desarrollando habilidades de interpretación jurídica y toma de decisiones fundamentada.
- Se utilizarán recursos como **líneas de tiempo interactivas, infografías comparativas, podcasts con expertos, árboles de decisión y guías legales**, para fomentar el aprendizaje autónomo y colaborativo. Estas herramientas facilitarán la comprensión progresiva del marco normativo, su evolución, y las implicancias éticas del ejercicio profesional en el entorno digital.
- Finalmente, se promoverá el **análisis ético y la discusión crítica** mediante debates asincrónicos, análisis de dilemas éticos relacionados con vigilancia, privacidad, inteligencia artificial y sesgos algorítmicos. Los participantes serán desafiados a resolver casos éticos complejos vinculados a la gestión de datos y los derechos digitales, fortaleciendo así su juicio profesional y responsabilidad social.

Para las evaluaciones se utilizará:

- Caso integrador con múltiples dimensiones legales, éticas y técnicas
- Simulación de respuesta ante incidente complejo con matriz legal, informe de obligaciones y plan de respuesta
- Evaluación por rúbrica con retroalimentación formativa
- Foro de reflexión sobre aprendizajes y desafíos futuros

Descripción de unidades: Unidad 1: Fundamentos legales de la ciberseguridad
Esta unidad entrega una visión general del marco normativo que sustenta la ciberseguridad en Chile, abordando leyes clave como la Ley 21.459 sobre delitos informáticos y la Ley 21.663 Marco de Ciberseguridad. Además, se revisan los principios jurídicos fundamentales, tales como legalidad, proporcionalidad y responsabilidad, junto con el rol del CSIRT nacional como entidad coordinadora de incidentes. También se introducen referentes internacionales como el Convenio de Budapest y el GDPR, que permiten contextualizar la legislación chilena en un marco global.

Unidad 2: Protección de datos personales
Esta unidad aborda los principios, derechos y obligaciones fundamentales relacionados con la protección de datos personales en Chile. Se analiza la Ley 19.628 y su reforma, junto con los principios de licitud, finalidad y proporcionalidad en el tratamiento de datos. Asimismo, se profundiza en los derechos ARCO y el consentimiento informado como pilares del resguardo de la privacidad, así como el rol y atribuciones de la Agencia de Protección de Datos. El objetivo es que el participante reconozca estos elementos en contextos reales.

Unidad 3: Responsabilidad legal y gestión de incidentes
En esta unidad se revisa la normativa vigente frente a incidentes de ciberseguridad y vulneraciones de datos, abordando la tipificación de delitos informáticos, las obligaciones de reporte ante autoridades como el CSIRT y la CMF, y las distintas dimensiones de responsabilidad legal: penal, civil y administrativa. Se busca que el participante reconozca los marcos de acción ante incidentes y desarrolle criterios para actuar conforme a la legislación vigente.

Unidad 4: Cumplimiento normativo y auditoría
Esta unidad presenta los principales enfoques y modelos para implementar estrategias de cumplimiento normativo en ciberseguridad y protección de datos. Se revisan marcos como ISO 27001, NIST y los lineamientos de la CMF, junto con metodologías de auditoría legal interna. Además, se aborda la evaluación de impacto en protección de datos (EIPD) como herramienta clave para anticipar riesgos legales. El propósito es que el participante comprenda cómo estructurar y evaluar procesos de cumplimiento en su organización.

Unidad 5: Derechos digitales y ética en el entorno digital
Esta unidad promueve la reflexión sobre los dilemas éticos y legales asociados al uso de tecnologías emergentes. Se abordan temas como los derechos digitales, la vigilancia estatal, el consentimiento informado, y los sesgos en inteligencia artificial. A través del análisis crítico, el participante será capaz de evaluar situaciones complejas que involucren el uso de datos personales y la toma de decisiones automatizadas, considerando principios éticos y normativos.

Unidad 6: Herramientas legales y plataformas oficiales
En esta última unidad, se exploran las herramientas prácticas y plataformas oficiales disponibles para la gestión normativa en ciberseguridad y protección de datos. Se trabaja con sitios como el de la CMF, CSIRT y la Agencia de Protección de Datos, realizando simulaciones de reportes, elaboración de matrices de cumplimiento y búsqueda de normativas y jurisprudencia. El objetivo es que el participante se familiarice con los recursos digitales disponibles para apoyar su gestión legal en entornos organizacionales reales.

Estrategias evaluativas		
Indicadores de logro	**Instrumentos de evaluación**	**Normas de aprobación**
Unidad 1		
Identifica los principios de legalidad, proporcionalidad y responsabilidad en el contexto de la ciberseguridad. Reconoce los elementos clave de aplicación de la Ley 21.459 en casos de delitos informáticos. Identifica el rol del CSIRT nacional y su función en la gestión de incidentes de seguridad. Reconoce la relación de los tratados internacionales relevantes (Convención de Budapest, GDPR, ARCO) con el marco normativo chileno en contextos de ciberseguridad. Reconoce diferencias entre los tipos de responsabilidad legal (civil, penal, administrativa) en incidentes de ciberseguridad.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 2		
Reconoce los principios de licitud, finalidad y proporcionalidad establecidos en la Ley 19.628 y su reforma. Reconoce la aplicación práctica de derechos ARCO (Acceso, Rectificación, Cancelación, Oposición) y su aplicación práctica. Reconoce el rol y atribuciones de la Agencia de Protección de Datos en Chile en problemáticas de ciberseguridad.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**

Reconoce las diferencias entre consentimiento informado, tratamiento legítimo y vulneración de derechos en contextos de ciberseguridad.		
Unidad 3		
Identifica los delitos informáticos tipificados en la Ley 21.459 en contextos relacionados a incidentes reales. Reconoce las obligaciones legales de reporte ante vulneraciones de datos personales. Reconoce diferencias entre responsabilidad civil, penal y administrativa en el contexto de ciberseguridad. Reconoce protocolos de respuesta ante incidentes, considerando normativa nacional e institucional. Reconoce la relación de la gestión de incidentes con marcos normativos como CSIRT, Agencia de Protección de Datos y estándares internacionales en contextos organizacionales.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 4		
Identifica los principales modelos de cumplimiento normativo aplicables en Chile (ISO 27001, NIST, CMF) en materias de ciberseguridad. Reconoce los elementos clave de una auditoría legal en ciberseguridad y protección de datos en contextos organizacionales. Reconoce el uso de matrices de cumplimiento que integren obligaciones legales, estándares técnicos y riesgos operacionales.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**

Reconoce la relación entre los resultados de auditoría con acciones correctivas y planes de mejora continua en contextos organizacionales. Reconoce el uso de lenguaje técnico-jurídico adecuado en informes de cumplimiento y evaluación de impacto.		
Unidad 5		
Reconoce los principales derechos digitales en el contexto chileno e internacional. Identifica prácticas de vigilancia, recolección de datos y tratamiento automatizado de probable vulneración a derechos fundamentales. Reconoce diferencias entre consentimiento informado, manipulación algorítmica y uso legítimo de datos personales en contextos organizacionales. Reconoce fundamentos normativos y éticos correctos de resolución de dilemas digitales reales o simulados. Reconoce los principios éticos (autonomía, justicia, no maleficencia) de marcos legales vigentes en Chile y estándares internacionales en contextos de problemáticas de ciberseguridad.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 6		
Identifica las funciones y recursos clave de plataformas oficiales como CMF, CSIRT y la Agencia de	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección	Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con

Protección de Datos frente a problemáticas de ciberseguridad. Reconoce los formatos y procedimientos de reporte exigidos por organismos reguladores en casos de incidentes o vulneraciones. Aplica matrices de cumplimiento y de reporte en contextos organizacionales simulados. Reconoce el uso de herramientas digitales para generar informes normativos, evaluar riesgos y documentar obligaciones legales.	única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán con claves.	notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 10% de la calificación final.**
Evaluación Final		
Analiza un caso real o simulado de incidente de seguridad, identificando vulneraciones legales y normativas. Elabora una matriz legal que vincule obligaciones normativas con acciones técnicas y organizacionales. Redacta un informe de cumplimiento que incluya diagnóstico, riesgos legales, y recomendaciones normativas. Redacta reportes y simulaciones con lenguaje técnico-jurídico adecuado, cumpliendo con exigencias formales y éticas. Aplica técnicas de diseño un plan de respuesta ante incidentes, considerando protocolos oficiales y exigencias regulatorias. Aplica correctamente la legislación chilena vigente (Ley 21.459, Ley 19.628 reformada) y estándares internacionales (GDPR, ISO 27001) en el caso simulado.	La evaluación final consistirá en el análisis de un caso práctico (real o simulado) de un incidente de ciberseguridad. El participante deberá elaborar una matriz de cumplimiento normativo, redactar un informe de obligaciones legales y diseñar un plan de respuesta al incidente, aplicando la legislación chilena vigente (Leyes 21.663, 21.459, 19.628) y estándares relevantes. Se evaluará con 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Esta evaluación representa el 60% de la calificación final.**

Utiliza lenguaje técnico-jurídico adecuado en la presentación escrita y oral del caso. Integra principios éticos y derechos digitales en la propuesta de solución, demostrando reflexión crítica.		

Requisito de aprobación	
Modalidad asincrónica	Nota mínima de aprobación 4.0

Recursos para la implementación					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
N/A	N/A	1 1 1	Plataforma AVA Computador Informacion Oficial: CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática). CMF (Comisión para el Mercado Financiero). Agencia de Protección de Datos.	1 1 1 6	El curso estará disponible en http://cursos.eclass.com/ . Seleccionar la opción RUT en TIPO DE DOCUMENTO. La guía de uso de la plataforma se encuentra en Http://cursos.eclass.com, en la pestaña Información correspondiente al curso. Inducción tecnológica/metodológica, estará disponible en http://cursos.eclass.com Unidades publicadas en el sitio Http://cursos.eclass.com/ Están escritas en lenguaje claro y contienen gráfica para facilitar la comprensión por parte de los alumnos.

				6 6	Actividades de aplicación publicadas en el sitio http://cursos.eclass.com/ Resumen y glosario de contenido publicados en el sitio Http://Cursos.Eclass.Com/

Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Unidad Académica)
Máximo tres años

Diplomado	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
DIPLOMADO EN CIBERSEGURIDAD	Aspectos legales de ciberseguridad y protección de datos
	Seguridad computacional en la organización
	Visualización de datos aplicada
	Tendencias y Futuro de la Ciberseguridad

Convalidación		
Diplomado	**Curso**	**Código**
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A

Articulación		
Programa	**Escuela**	**Código**
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A

Otros cursos relacionados con la temática
N/A
N/A
N/A

Perfil: Especialista disciplinar diseñador(a)	
Requisitos relativos a la educación	Universitario con postítulo
Requisitos relativos a la formación	Profesionales y técnicos de las áreas de Tecnologías de la Información, Seguridad de la Información, Cumplimiento (Compliance), Auditoría, Riesgo Operacional y áreas legales que busquen comprender y aplicar el marco

	normativo chileno en ciberseguridad y protección de datos. Cargos como Jefes de TI, Oficiales de Seguridad (CISO), Analistas de Seguridad, Auditores de Sistemas, Encargados de Protección de Datos (DPO), abogados o asesores legales.
Requisitos relativos a las habilidades	**Diseño instruccional especializado**: capacidad para estructurar programas formativos integrando normativa ambiental, sistemas de gestión, herramientas de cumplimiento, evaluación de impacto y metodologías de monitoreo y control de riesgos. **Análisis y síntesis normativa y técnica**: habilidad para interpretar y adaptar legislación, estándares de gestión ambiental y metodologías técnicas, transformándolos en contenidos didácticos aplicables a contextos laborales reales. **Elaboración de materiales educativos**: capacidad en la creación de guías, presentaciones, casos prácticos, actividades evaluativas y recursos interactivos que faciliten la aplicación de los contenidos. **Actualización técnica**: capacidad para integrar en los contenidos cambios normativos, tendencias y buenas prácticas internacionales en gestión y sostenibilidad ambiental.
Requisitos relativos a la experiencia	Al menos 5 años de experiencia laboral en cargos relacionados a Ingeniería Informática, Derecho, Seguridad de la Información o afín integrando normativas de derecho informático, ciberseguridad, protección de datos, auditoría de sistemas, etc.

Perfil: Especialista disciplinar facilitador(a)	
Requisitos relativos a la educación	Universitario con postítulo.
Requisitos relativos a la formación	Formación en áreas de TI, seguridad informática, auditoría, cumplimiento normativo, gestión de riesgos, legaltech o carrera afín, con sólida base académica en normativa de ciberseguridad (Ley 21.459) , protección de datos personales (Ley 19.628) , sistemas de gestión y auditoría (ISO 27001, NIST) , evaluación de impacto en protección de datos y gestión de incidentes. Deseable diplomado, magíster o cursos de especialización en ciberseguridad, derecho informático, protección de datos o certificaciones de cumplimiento (por ejemplo: ISO 27001).
Requisitos relativos a las habilidades	Dominio integral de la temática: Manejo sólido y actualizado de la normativa chilena (Ley 21.459 sobre delitos informáticos, Ley 19.628 y su reforma), procesos de implementación y auditoría (ISO 27001, NIST), metodologías de evaluación de impacto en protección de datos y estrategias de gestión de incidentes. Habilidades comunicacionales: Capacidad para explicar contenidos técnicos y jurídicos complejos (ej. tipificación de delitos, principios de licitud, derechos ARCO) de forma clara, adaptándolos a diferentes perfiles laborales (TI, auditoría, legaltech, etc.).

	Facilitación del aprendizaje: Experiencia en el uso de metodologías participativas como análisis de casos reales (filtraciones, ransomware), aprendizaje basado en problemas (ABP) y simulaciones que promuevan la transferencia de conocimientos al entorno laboral. Capacidad de resolución de consultas técnicas: Habilidad para responder y orientar sobre problemáticas reales en cumplimiento normativo, gestión de vulneraciones de datos y uso de plataformas oficiales (CSIRT, CMF).
Requisitos relativos a la experiencia	Experiencia mínima de 5 años en la implementación y/o supervisión de modelos de cumplimiento, auditorías legales, gestión de incidentes, evaluación de impacto en protección de datos y cumplimiento normativo (ISO 27001, NIST, CMF) en proyectos u operaciones reales. Experiencia previa como facilitador en programas de capacitación en temáticas de ciberseguridad, protección de datos o derecho informático. Experiencia en la creación o adaptación de materiales educativos prácticos y casos aplicados, como análisis de casos reales (filtraciones, ransomware) y simulaciones.

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
SEGURIDAD COMPUTACIONAL EN LA ORGANIZACIÓN	50	1	64	Online asincrónica con sesión sincrónica

Identificación
Código SENCE:
Código Curso Duoc UC:

Unidad Académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Informática y Telecomunicaciones	Oscar Araya	17-12-2025

Especialista disciplinar	Analista instruccional
Claudio González P.	Diego Acosta

Aporte de valor del curso (no SENCE)
En el contexto actual de transformación digital, los datos se han convertido en el activo más crítico de las organizaciones. La creciente interconectividad, el teletrabajo, el IoT y la dependencia de servicios en la nube han expandido exponencialmente la superficie de ataque. Amenazas como el **ransomware**, el **phishing** y las **fugas de datos** son cada vez más sofisticadas, poniendo en riesgo la continuidad del negocio, la reputación corporativa y la confianza del cliente. Esto, sumado a regulaciones de **protección de datos** cada vez más estrictas, convierte a la ciberseguridad en un pilar estratégico de la gestión empresarial. El curso **Seguridad Computacional en la Organización** entrega a las y los participantes las herramientas necesarias para **diseñar, implementar, gestionar y auditar** una estrategia de seguridad de la información. El programa tiene un enfoque práctico en la **identificación de vulnerabilidades**, el **análisis de riesgos**, la implementación de **controles de acceso**, la **gestión de incidentes** y la **criptografía**. Además, se pone énfasis en el 'factor humano', desarrollando estrategias de **concientización (awareness)** para todo el personal, vinculando la seguridad técnica con los objetivos del negocio y el **cumplimiento normativo**. Al finalizar, las y los participantes estarán capacitados para **liderar procesos de ciberseguridad**, implementar **políticas de seguridad** efectivas, preparar a la organización para **auditorías internas y externas**, y fomentar una **cultura de seguridad resiliente**. Esto fortalece su perfil profesional y genera valor tangible al **proteger los activos de información**, asegurar la **continuidad operacional** e impulsar la **confianza digital** de la organización.

Caracterización del participante
Este curso está dirigido a personas que ocupan cargos vinculados a la gestión tecnológica y operativa de la seguridad de la información dentro de las organizaciones. En particular, está orientado a **analistas de seguridad TI, encargados de infraestructura tecnológica, responsables de continuidad operativa, supervisores de soporte técnico, administradores de sistemas, jefaturas de tecnologías de la información, y coordinadores de cumplimiento normativo en ciberseguridad**. También pueden

participar personas que lideren procesos de digitalización o transformación tecnológica que requieran integrar la seguridad computacional en la estrategia del negocio.

Requisitos de ingreso
Se recomienda que los participantes cuenten con **conocimientos básicos en tecnologías de la información (TI)**, administración de sistemas operativos o redes computacionales. Se sugiere como requisito mínimo la **formación previa en fundamentos de informática** o experiencia laboral equivalente que permita comprender la arquitectura de sistemas y redes. Esto asegurará que puedan aprovechar al máximo los contenidos del curso, facilitando su integración y aplicación práctica en escenarios reales.

Requisitos técnicos
Sistema Operativo Windows 10 o superior; iOS 11 o posterior Memoria RAM: mínimo 8 GB, recomendado 16 GB o más Procesador: 4 Cores y velocidad de 2 GHz o superior Tarjeta de sonido Resolución de monitor: 1024 x 768 o superior. Navegadores Recomendados: Google Chrome (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
Aplicar estrategias y herramientas de seguridad de la información en iniciativas de protección de los activos digitales de la organización, en condiciones de gestión de riesgos, prevención de incidentes y fortalecimiento de la continuidad operativa de entornos tecnológicos interconectados y regulados.

Unidad de aprendizaje	Resultados de aprendizaje	Contenidos	Horas	
			T	P
Unidad 1: Fundamentos de la Seguridad Computacional	Identificar los principios de la seguridad de la información y el panorama de amenazas actual, considerando el marco ético y legal.	• Conceptos clave: Confidencialidad, Integridad y Disponibilidad (Tríada CIA). • Panorama de amenazas: Malware (virus, ransomware), Phishing, Ingeniería Social, Ataques DoS/DDoS. • Definición de activos de información y su valor. • Marco ético y legal de la seguridad de la información. • Deep Defense • Zero Trust	4	6

Unidad 2: Gestión de Riesgos y Políticas de Seguridad	Reconocer riesgos de seguridad en contextos de desarrollo de políticas organizacionales.	• Metodologías de análisis y gestión de riesgos (ISO 27005). • Identificación de activos, amenazas y vulnerabilidades. • Cálculo del riesgo (impacto y probabilidad). • Desarrollo de Políticas de Seguridad de la Información (PSI). • Roles y responsabilidades en la seguridad.	4	6
Unidad 3: Controles de Acceso y Seguridad de Redes	Reconocer controles técnicos de protección de acceso a redes y sistemas en contextos corporativos y organizacionales.	• Modelos de control de acceso (DAC, MAC, RBAC). • Autenticación: Contraseñas, Biometría, Doble Factor (MFA). • Seguridad perimetral: Firewalls y Zonas Desmilitarizadas (DMZ). • Redes Privadas Virtuales (VPN). • Seguridad en redes inalámbricas (WiFi). • Sistemas de Detección y Prevención de Intrusos (IDS/IPS).	4	6
Unidad 4: Criptografía y Seguridad de Datos	Reconocer las técnicas de criptografía en iniciativas de protección de datos en reposo y en tránsito.	• Conceptos de criptografía: simétrica y asimétrica. • Funciones HASH y firmas digitales. • Infraestructura de Clave Pública (PKI) y certificados digitales. • Encriptación de datos en reposo (discos duros, bases de datos). • Encriptación de datos en tránsito (SSL/TLS). • Prevención de Fuga de Datos (DLP).	4	6
Unidad 5: Seguridad Operacional y Respuesta a Incidentes	Reconocer planes de respuesta y continuidad del negocio ante incidentes propios del contexto organizacional.	• Gestión de parches y vulnerabilidades. • Monitoreo, logging y auditoría de eventos (SIEM). • Creación de un Plan de Respuesta a Incidentes (IRP). • Fases de la respuesta: preparación, detección, contención, erradicación, recuperación. • Plan de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP).	4	6

Unidad 6: Auditoría y Cultura de Seguridad	Aplicar pruebas a los controles de seguridad dentro de estrategias de promoción una cultura de concientización.	• Tipos de auditorías de seguridad: internas y externas. • Pruebas de penetración (Pentesting) y Hacking Ético. • Marcos de referencia y normativas (ISO 27001, NIST). • Creación de programas de concientización y capacitación. • Simulación de campañas anti-phishing.	4	6
Unidad 7: Seminario - Proyecto Integrador	Aplicar los conocimientos adquiridos en el diseño de un plan de seguridad integral para un caso de estudio.	• Evaluación final: Desarrollo de un proyecto integrador. • Análisis de caso práctico: Simulación de una organización. • Diseño de política de seguridad y plan de respuesta a incidentes.		4
		Subtotal	24	40
		Horas totales	64	

Estrategias metodológicas
Metodologías de entrega de contenidos: El curso se desarrollará en modalidad e-learning asincrónica a través del Ambiente Virtual de Aprendizaje (AVA) de eClass. Para esta modalidad, el proceso formativo se desarrollará mediante recursos educativos auto instruccionales tales como videos interactivos, guías interactivas, podcasts, video tutoriales, infografías, PDFs u otros, los cuales presentarán los contenidos de forma contextualizada y representativa según la realidad laboral de los participantes. Los recursos educativos estarán disponibles en versión audiovisual y/o descargable para garantizar flexibilidad en el acceso y aprovechamiento del contenido. Además, se desarrollarán evaluaciones formativas enfocadas en la aplicación práctica de los contenidos, buscando vincular el aprendizaje teórico con situaciones laborales reales. **Para fomentar una comprensión profunda y aplicada, se implementarán estrategias metodológicas activas de enseñanza-aprendizaje, tales como:** **Resolución de problemas:** Los participantes resolverán incidentes de seguridad simulados y problemas reales que puedan enfrentar en sus entornos laborales. **Análisis de casos:** Se utilizarán casos de estudio basados en brechas de seguridad reales (ej. ataques de ransomware famosos) para analizar qué falló y cómo podría haberse prevenido.

Simulaciones: Los participantes tendrán la oportunidad de utilizar herramientas de seguridad en entornos controlados (sandboxes) y participar en simulaciones de ataques (ej. campañas de phishing) para entender la perspectiva del atacante y del defensor.

Aprendizaje basado en problemas: Se presentarán escenarios empresariales donde los participantes deberán diseñar políticas de seguridad y planes de respuesta aplicando los conocimientos adquiridos.

Descripción de unidades:

Unidad 1: Esta unidad ofrece una visión general sobre la Seguridad Computacional, explicando sus principios (Tríada CIA), objetivos y el panorama de amenazas actual. Se introducirán los conceptos éticos y legales fundamentales.

Unidad 2: En esta unidad se detallan los pasos para realizar una gestión de riesgos de seguridad, incluyendo la identificación de activos, amenazas y vulnerabilidades, y la formulación de una Política de Seguridad de la Información (PSI).

Unidad 3: Esta unidad se centra en los controles técnicos para proteger la infraestructura, abordando la gestión de identidades y accesos (MFA), y la seguridad perimetral y de redes (Firewalls, VPNs, IDS/IPS).

Unidad 4: En esta unidad, los estudiantes aprenderán sobre las herramientas criptográficas para proteger la información tanto en reposo como en tránsito, incluyendo la gestión de certificados digitales (PKI) y estrategias de DLP.

Unidad 5: Se explicará el proceso de gestión de la seguridad en el día a día (operaciones), incluyendo la gestión de parches, el monitoreo y la creación de planes de Respuesta a Incidentes (IRP) y Continuidad del Negocio (BCP).

Unidad 6: La unidad final aborda la importancia de la verificación y la mejora continua a través de auditorías y pruebas de penetración. Se analizarán marcos normativos (ISO 27001) y la importancia del factor humano a través de la cultura de seguridad.

Estrategias evaluativas		
Indicadores de logro	**Instrumentos de evaluación**	**Normas de aprobación**
Unidad 1		
Identifica los principios (CIA) de la seguridad de la información. Reconoce los principales tipos de amenazas y vectores de ataque. Reconoce el marco ético y legal asociado a la gestión de la información.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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.

		Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 2		
Reconoce metodologías básicas de análisis de riesgo en contextos organizacionales. Identifica vulnerabilidades y amenazas en un escenario dado. Reconoce los componentes clave de una Política de Seguridad de la Información en contextos organizacionales.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 3		
Reconoce los diferentes modelos de control de acceso en estrategias de seguridad computacional. Reconoce la función de herramientas como firewalls, VPNs e IDS/IPS en estrategias de seguridad computacional. Reconoce la importancia del uso de autenticación multifactor (MFA) como medida de seguridad personal.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 4		
Reconoce la diferencia entre criptografía simétrica y asimétrica en estrategias de ciberseguridad.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección	Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con

Reconoce el uso de certificados digitales y firmas electrónicas como medidas de ciberseguridad. Identifica técnicas de protección de datos en reposo y en tránsito como medidas de ciberseguridad.	única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán con claves.	notas entre 1.0 y 7.0, siendo 4.0 el mínimo requerido para la aprobación. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 5		
Reconoce las características de las fases de un Plan de Respuesta a Incidentes (IRP) en contextos de ciberseguridad organizacional. Reconoce la importancia del monitoreo y gestión de vulnerabilidades en contextos de ciberseguridad organizacional. Selecciona de forma correcta un Plan de Continuidad del Negocio (BCP) y uno de Recuperación ante Desastres (DRP) ante situaciones de incertidumbre operacional.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 6		
Identifica el propósito de una auditoría de seguridad y pentesting como medio de prevención de riesgos. Reconoce el uso de los dominios principales de la norma ISO 27001 en contextos de ciberseguridad. Aplica estrategias de fomento de una cultura de concientización en seguridad en una organización.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 10% de la calificación final.**

Evaluación Final		
Aplica técnicas de diseño un plan de seguridad integral en un caso de estudio. Aplica una metodología de gestión de riesgos a una organización simulada. Propone controles técnicos y administrativos alineados a una política de seguridad. Aplica técnicas de desarrollo del esquema de un Plan de Respuesta a Incidentes en un contexto simulado.	La evaluación final del curso tendrá una finalidad sumativa y se llevará a cabo a través de heteroevaluación. Los participantes deberán desarrollar un **Proyecto Integrador** de manera individual, basado en un caso de estudio. Los participantes deberán elaborar un **Plan Director de Seguridad** para una organización ficticia, demostrando su capacidad para aplicar los conocimientos adquiridos. El plan debe incluir:" 1. Análisis de Riesgos (activos, amenazas, vulnerabilidades). 2. Propuesta de Política de Seguridad de la Información. 3. Definición de controles técnicos y administrativos prioritarios. 4. Esquema de un Plan de Respuesta a Incidentes para una amenaza clave (ej. ransomware). Los resultados serán evaluados de acuerdo con una rúbrica detallada.	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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Esta evaluación representa el 60% de la calificación final.**

Requisito de aprobación	
Modalidad asincrónica	Nota mínima de aprobación 4.0

Recursos para la implementación					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
N/A	N/A	1 1	Plataforma LMS (AVA) Computador	1 1	El curso estará disponible en http://cursos.eclass.com/ . Seleccionar la opción RUT en TIPO DE DOCUMENTO. La guía de uso de la plataforma se encuentra en Http://cursos.eclass.com, en la pestaña

				1 6 6 6	Información correspondiente al curso. Inducción tecnológica/metodológica, estará disponible en http://cursos.eclass.com Unidades publicadas en el sitio Http://cursos.eclass.com/ Están escritas en lenguaje claro y contienen gráfica para facilitar la comprensión por parte de los alumnos. Actividades de aplicación publicadas en el sitio http://cursos.eclass.com/ Resumen y glosario de contenido publicados en el sitio Http://Cursos.Eclass.Com/

Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Unidad Académica)
Máximo tres años

Diplomado	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
DIPLOMADO EN CIBERSEGURIDAD	Aspectos legales de ciberseguridad y protección de datos
	Seguridad computacional en la organización
	Visualización de datos aplicada
	Tendencias y Futuro de la Ciberseguridad

Convalidación		
Diplomado	**Curso**	**Código**
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A

Articulación

Programa	Escuela	Código
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A

Otros cursos relacionados con la temática
N/A
N/A
N/A

Perfil: Especialista disciplinar diseñador(a)	
Requisitos relativos a la educación	Universitario con postítulo
Requisitos relativos a la formación	Formación en Ingeniería en Informática, Ciberseguridad, Telecomunicaciones o carrera afín, con sólida base académica en seguridad de la información, gestión de riesgos TI y arquitectura de redes. Diplomado, magíster o certificaciones de industria (ej: CISSP, CISM, CompTIA Security+).
Requisitos relativos a las habilidades	**Diseño instruccional especializado:** capacidad para estructurar programas formativos integrando análisis de riesgos, controles técnicos, respuesta a incidentes y cumplimiento normativo. **Análisis y síntesis normativa y técnica:** habilidad para interpretar y adaptar estándares (ISO 27001, NIST) y metodologías técnicas, transformándolos en contenidos didácticos aplicables. **Elaboración de materiales educativos:** capacidad en la creación de guías, presentaciones, casos prácticos, laboratorios simulados y actividades evaluativas. **Actualización técnica:** capacidad para integrar en los contenidos cambios en el panorama de amenazas, nuevas tecnologías y buenas prácticas en ciberseguridad.
Requisitos relativos a la experiencia	Experiencia mínima de 5 años en el diseño de programas o cursos de ciberseguridad, gestión de riesgos TI, o auditoría de sistemas. Experiencia en desarrollo de contenidos educativos con enfoque aplicado y contextualizado a operaciones reales de TI.

Perfil: Especialista disciplinar facilitador(a)	
Requisitos relativos a la educación	Universitario con postítulo.
Requisitos relativos a la formación	Formación en Ingeniería en Informática, Ciberseguridad, Telecomunicaciones o carrera afín, con conocimientos actualizados en gestión de incidentes, hacking ético, normativas de seguridad y gestión de riesgos. Diplomado, magíster o certificaciones de industria (ej: CISSP, CISM, CEH).

Requisitos relativos a las habilidades	**Dominio integral de la temática:** manejo sólido y actualizado de técnicas de ataque y defensa, implementación y auditoría de controles de seguridad, y metodologías de respuesta a incidentes. **Habilidades comunicacionales:** capacidad para explicar contenidos técnicos complejos (criptografía, redes) de forma clara, adaptándolos a diferentes perfiles laborales. **Facilitación del aprendizaje:** experiencia en el uso de metodologías participativas (análisis de casos, 'Capture The Flag' (CTF) simulados, laboratorios prácticos) que promuevan la transferencia de conocimientos. **Capacidad de resolución de consultas técnicas:** habilidad para responder y orientar sobre problemáticas reales en seguridad computacional.
Requisitos relativos a la experiencia	Experiencia mínima de 5 años en la implementación y/o supervisión de sistemas de seguridad (ej. trabajo en un SOC), auditorías de seguridad, respuesta a incidentes o consultoría en ciberseguridad. Experiencia previa como facilitador en programas de capacitación en temáticas de TI o seguridad. Experiencia en la creación o adaptación de materiales educativos prácticos y casos aplicados.

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
VISUALIZACIÓN DE DATOS APLICADA A LA CIBERSEGURIDAD	50	1	64	Online asincrónica con sesión sincrónica

Identificación
Código SENCE:
Código Curso Duoc UC:

Unidad Académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Informática y Telecomunicaciones	Oscar Araya	17-12-2025

Especialista disciplinar	Analista instruccional
Claudio González P.	Diego Acosta

Aporte de valor del curso (no SENCE)
En Chile, la ciberseguridad enfrenta un volumen de datos sin precedentes, generando millones de alertas y registros (logs) diariamente. La creciente sofisticación de los ciberataques exige que las organizaciones cuenten con profesionales capaces de interpretar rápidamente esta información para detectar, analizar y responder a incidentes. La visualización de datos se ha convertido en un factor determinante para la viabilidad de las operaciones de seguridad, permitiendo transformar datos crudos en inteligencia accionable. El curso Visualización de Datos Aplicada a la Ciberseguridad entrega a las y los participantes herramientas prácticas para interpretar grandes volúmenes de datos de seguridad, construir dashboards efectivos y analizar patrones de ataque. Además, fortalece las competencias para implementar estrategias de Threat Hunting visual y gestionar informes técnicos de alto estándar. Con estas habilidades, los participantes estarán preparados para optimizar la detección de amenazas, reducir los tiempos de respuesta (MTTR) y contribuir de forma efectiva a la postura de seguridad y resiliencia de sus organizaciones.

Caracterización del participante
Profesionales y técnicos que se desempeñan como **Analistas de SOC (Nivel 1 y 2)**, analistas de ciberinteligencia, ingenieros de seguridad, administradores de plataformas SIEM (como Splunk o ELK), coordinadores de respuesta a incidentes, gestores de riesgos tecnológicos, asesores de proyectos con componentes de ciberseguridad y personal de TI o consultoras que participan en el monitoreo, control y mejora del desempeño de la seguridad de organizaciones y proyectos.

Requisitos de ingreso
Ideal conocimientos básicos en ciberseguridad (Modelo OSI, tipos de amenazas, fundamentos de redes) o experiencia en áreas de TI.

Requisitos técnicos
Sistema Operativo Windows 10 o superior; iOS 11 o posterior Memoria RAM: mínimo 8 GB, recomendado 16 GB o más Procesador: 4 Cores y velocidad de 2 GHz o superior mínimo, ideal 8 Cores y 2 GHz o superior Tarjeta de sonido Resolución de monitor: 1024 x 768 o superior. Navegadores Recomendados: Google Chrome (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
Aplicar técnicas de visualización de datos en iniciativas de análisis, detección y respuesta a incidentes de ciberseguridad.

Unidad de aprendizaje	Resultados de aprendizaje	Contenidos	Horas	
			T	P
Unidad 1: Fundamentos de la Visualización en Ciberseguridad	Identificar los fundamentos de la visualización de datos aplicada a la ciberseguridad.	• Definición de visualización de datos de seguridad. • El pipeline de datos: de logs a inteligencia accionable. • Fuentes de datos (Logs, Netflow, Alertas SIEM, EDR). • Principios de percepción visual y diseño (Gestalt).	4	6
Unidad 2: Diseño de Dashboards y Elección de Gráficos	Reconocer buenas prácticas de diseño de dashboards en contextos de ciberseguridad.	• Principios de diseño de dashboards (para SOC vs. Gerencia). • Tipos de gráficos y su aplicación (Histogramas, Heatmaps, Sankey, Grafos). • Errores comunes en la visualización de datos. • Contextualización: Mapeo visual con frameworks (MITRE ATT&CK).	4	6
Unidad 3: Herramientas SIEM – Wazuh y Elastic	Reconocer diferencias de uso entre herramientas de visualización y análisis de logs, destacando Wazuh como plataforma SIEM principal.	• Panorama de los principales SIEM del mercado • Arquitectura de Wazuh • Ingesta y normalización de datos • Lenguaje de consulta y análisis • Visualización y monitoreo	4	6

Unidad 4: Herramientas: SIEM - sp	Reconocer procedimientos de visualización en Splunk en acciones de análisis de seguridad.	• Introducción a la arquitectura Splunk. • Lenguaje de consulta SPL (Search Processing Language). • Modelo de Información Común (CIM). • Creación de dashboards, reportes y alertas en Splunk.	4	6
Unidad 5: Caso de Uso: Detección y Threat Hunting	Reconocer técnicas de interpretación de información visualizada en acciones de detección de amenazas y Threat Hunting.	• Visualización de tráfico de red (Netflow) para detección de anomalías. • Análisis visual de logs de autenticación (Windows, Linux). • Detección de movimiento lateral y exfiltración de datos. • Visualización de patrones de malware. • Uso de filtros en la CLI de Linux y Powershell, además de expresiones regulares.	4	6
Unidad 6: Caso de Uso: Respuesta a Incidentes y Reporting	Aplicar estrategias de visualización en la respuesta a incidentes y generación de reportes.	• Creación de líneas de tiempo visuales de un incidente. • Visualización de la cadena de ataque (Kill Chain). • Diseño de reportes ejecutivos (KPIs, Métricas de Riesgo). • Diseño de reportes técnicos post-incidente.	4	6
Unidad 7: Seminario	Aplicar técnicas de visualización de datos en un escenario de ciberseguridad simulado.	Evaluación final (Proyecto). Las y los participantes deberán enfrentar un **escenario simulado de ciberseguridad**, que consiste en un conjunto de datos reales o ficticios (logs de red, alertas SIEM, registros de eventos) correspondientes a un incidente potencial. A partir de esta base de datos, deberán: 1. **Construir un dashboard simple** que permita visualizar patrones relevantes y detectar anomalías. 2. **Aplicar técnicas de visualización** para identificar posibles vectores de ataque, origen del incidente y zonas afectadas. 3. **Proponer una estrategia de respuesta**, basada en la visualización y alineada con prácticas de Threat Hunting. 4. **Elaborar un informe técnico breve**, incluyendo capturas del dashboard,		4

		interpretación de datos y recomendaciones.		
		Subtotal	24	40
		Horas totales	64	

Estrategias metodológicas
El curso se desarrollará en modalidad e-learning asincrónica a través del Ambiente Virtual de Aprendizaje (AVA) de eClass. Para esta modalidad, el proceso formativo se desarrollará mediante recursos educativos auto instruccionales tales como: videos interactivos, guías interactivas, podcast, video tutoriales, infografías, PDF u otros; a través of los cuales se presentarán los contenidos de forma contextualizada y representativa según la realidad laboral de los participantes. Los recursos educativos estarán disponibles en versión audiovisual y/o descargable. Además, se desarrollarán evaluaciones formativas enfocadas a la aplicación práctica de los contenidos. Para ello, se utilizarán estrategias metodológicas de enseñanza aprendizaje como: resolución de problemas, análisis de casos, simulaciones, aprendizaje basado en problemas, juegos de roles, entre otras. **Descripción de unidades:** • **Unidad 1: Fundamentos de la Visualización en Ciberseguridad** Esta unidad ofrece una introducción a por qué la visualización es crucial en ciberseguridad. Se revisan las fuentes de datos (logs, redes, endpoints) y cómo la percepción humana procesa la información visual, sentando las bases para un diseño efectivo. • **Unidad 2: Diseño de Dashboards y Elección de Gráficos** En esta unidad, los estudiantes aprenderán los principios de diseño para crear dashboards útiles. Se cubrirá qué tipo de gráfico usar para cada tipo de dato (tráfico de red, logs de autenticación, etc.) y cómo alinear las visualizaciones con frameworks como MITRE ATT&CK. • **Unidad 3: Herramientas: ELK Stack (Kibana)** Esta unidad se enfoca en la herramienta open-source líder, el Stack ELK. Los estudiantes aprenderán a ingestar datos y a construir sus primeros dashboards en Kibana, utilizando consultas KQL para filtrar y analizar logs. • **Unidad 4: Herramientas: Splunk** En esta unidad, se explora la plataforma SIEM líder del mercado, Splunk. Los estudiantes aprenderán el potente lenguaje SPL y cómo usar el Modelo de Información Común (CIM) para crear visualizaciones y alertas estandarizadas. • **Unidad 5: Caso de Uso: Detección y Threat Hunting** Esta unidad se centra en aplicar las técnicas aprendidas a casos de uso ofensivos. Se revisarán métodos visuales para cazar amenazas (*Threat Hunting*), como la detección de anomalías en el tráfico de red o la identificación de patrones de autenticación fallida. • **Unidad 6: Caso de Uso: Respuesta a Incidentes y Reporting** En esta unidad se abordarán los casos de uso defensivos y de comunicación. Los estudiantes aprenderán a construir líneas de tiempo de incidentes y a diseñar reportes efectivos, tanto para equipos técnicos como para la alta gerencia.

Estrategias evaluativas		
Indicadores de logro	**Instrumentos de evaluación**	**Normas de aprobación**
Unidad 1		

Identifica las principales fuentes de datos (logs, netflow, EDR) necesarias en el análisis de ciberseguridad. Reconoce los principios de percepción visual aplicados al análisis de datos. Reconoce el pipeline de datos (ingesta, procesamiento, visualización) en un contexto de seguridad.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 2		
Identifica las buenas prácticas de diseño de dashboards (para SOC vs. Gerencia) utilizadas en ciberseguridad. Reconoce los tipos de gráficos adecuados (histogramas, heatmaps, grafos) usados en datos de seguridad. Reconoce el procedimiento de mapeo de visualizaciones con el framework MITRE ATT&CK.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 3		
Identifica los principales SIEM del mercado y explica diferencias clave entre Wazuh, Elastic y Splunk. Configura agentes Wazuh para la ingesta de logs y demuestra comprensión de decodificadores/reglas. Reconoce técnicas de filtro y análisis de eventos de seguridad en Kibana mediante consultas en KQL.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia.

Reconoce técnicas de diseño de dashboards en Kibana que integren métricas de seguridad relevantes. Reconoce alertas generadas por Wazuh y relaciona hallazgos con incidentes simulados.		**Estas evaluaciones representan el 6% de la calificación final.**
Unidad 4		
Reconoce la arquitectura de Splunk y sus componentes en un análisis de seguridad. Reconoce el procedimiento de elaboración de dashboards y reportes en Splunk en estrategias de análisis de seguridad. Reconoce el uso de métodos de consulta SPL (Search Processing Language) en actividades de análisis de datos. Reconoce la función del Modelo de Información Común (CIM) como medio de normalización de datos. Reconoce dashboards y reportes en Splunk, comparando su funcionalidad con Kibana/Wazuh.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 5		
Reconoce técnicas de organización de datos visuales como medio de identificación de patrones de Threat Hunting. Reconoce técnicas de visualización en acciones de análisis de tráfico de red (Netflow). Reconoce estrategias de visualización en el análisis de logs de autenticación (detección de fuerza bruta).	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**

Unidad 6		
Selecciona KPIs y métricas clave en la elaboración de reportes ejecutivos y técnicos. Aplica estrategias de visualización en la construcción de líneas de tiempo de un incidente. Utiliza la cadena de ataque (Kill Chain) mediante herramientas visuales.	La evaluación tiene una finalidad sumativa a través de autoevaluación. Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán con lista de cotejo.	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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 10% de la calificación final.**
Evaluación Final		
Identifica patrones de ataque y anomalías en los datos provistos. Aplica técnicas de análisis de un conjunto de datos (logs) dentro de un incidente de seguridad. Aplica herramientas de visualización (Kibana o Splunk) como herramienta de investigación del incidente. Utiliza estrategias de visualización como medio de comunicación de los hallazgos del incidente. Aplica técnicas de *storytelling* con datos en la construcción de un reporte o dashboard final.	La evaluación tiene una finalidad sumativa a través de **heteroevaluación**. Para ello, los participantes deberán desarrollar una **prueba de preguntas abiertas** de manera individual, debiendo completar una serie de ítems que se evaluarán con **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. Se corregirá el desarrollo aplicando un 50% de exigencia. **Esta evaluación representa el 60% de la calificación final.**

Requisito de aprobación	
Modalidad asincrónica	Nota mínima de aprobación 4.0

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

N/A	N/A	1 1	Plataforma LMS Computador	1 1 1 6 6 6	El curso estará disponible en http://cursos.eclass.com/ . Seleccionar la opción RUT en TIPO DE DOCUMENTO. La guía de uso de la plataforma se encuentra en Http://cursos.eclass.com, en la pestaña Información correspondiente al curso. Inducción tecnológica/metodológica, estará disponible en http://cursos.eclass.com Unidades publicadas en el sitio Http://cursos.eclass.com/ Están escritas en lenguaje claro y contienen gráfica para facilitar la comprensión por parte de los alumnos. Actividades de aplicación publicadas en el sitio http://cursos.eclass.com/ Resumen y glosario de contenido publicados en el sitio Http://Cursos.Eclass.Com/

Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Unidad Académica)
Máximo tres años

Diplomado	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
	Aspectos legales de ciberseguridad y protección de datos

DIPLOMADO EN CIBERSEGURIDAD	Seguridad computacional en la organización
	Visualización de datos aplicada
	Tendencias y Futuro de la Ciberseguridad

Convalidación		
Diplomado	**Curso**	**Código**
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A

Articulación		
Programa	**Escuela**	**Código**
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A

Otros cursos relacionados con la temática
N/A
N/A
N/A

Perfil: Especialista disciplinar diseñador(a)	
Requisitos relativos a la educación	Universitario con postítulo
Requisitos relativos a la formación	Formación en Ingeniería en Informática, Ciberseguridad, Ciencia de Datos o carrera afín, con sólida base académica en análisis de datos de seguridad, operaciones de SOC, gestión de logs y plataformas SIEM. Deseable diplomado, magíster o certificaciones de industria (ej: Splunk Core Certified Power User, Elastic Certified Analyst, GCIA).
Requisitos relativos a las habilidades	**Diseño instruccional especializado:** capacidad para estructurar programas formativos integrando el pipeline de datos de seguridad (de log a dashboard), técnicas de análisis visual de amenazas y metodologías de *Threat Hunting* aplicadas. **Análisis y síntesis de datos:** habilidad para interpretar y adaptar fuentes de datos complejas (Netflow, logs de Windows, EDR) y lenguajes de consulta (SPL, KQL), transformándolos en contenidos didácticos aplicables. **Elaboración de materiales educativos:** capacidad en la creación de guías, presentaciones, conjuntos de datos (datasets) para análisis, casos prácticos, laboratorios en plataformas SIEM (Splunk/Kibana) y actividades evaluativas.

	Actualización técnica: capacidad para integrar en los contenidos cambios en técnicas de ataque (TTPs), nuevas herramientas de visualización y buenas prácticas en operaciones de SOC.
Requisitos relativos a la experiencia	Experiencia mínima de 5 años en el diseño de programas o cursos de análisis de datos de seguridad y visualización, incluyendo plataformas SIEM (Splunk, ELK), operaciones de SOC, análisis de logs y Threat Hunting visual. Experiencia en desarrollo de contenidos educativos con enfoque aplicado y contextualizado a incidentes de seguridad o escenarios de ciberataque reales.

Perfil: Especialista disciplinar facilitador(a)	
Requisitos relativos a la educación	Universitario con postítulo.
Requisitos relativos a la formación	Formación en Ingeniería en Informática, Ciberseguridad, Ciencia de Datos o carrera afín, con conocimientos actualizados en análisis de datos de seguridad, operaciones de SOC, gestión de logs, respuesta a incidentes y plataformas SIEM (Splunk/ELK). Deseable diplomado, magíster o cursos de especialización en ciberseguridad, análisis de datos, ciberinteligencia o certificaciones de herramientas/industria (por ejemplo: Splunk Core Certified Power User, Elastic Certified Analyst, GCIH, GCIA).
Requisitos relativos a las habilidades	**Dominio integral de la temática:** manejo sólido y actualizado de **plataformas SIEM (Splunk, ELK)**, **lenguajes de consulta (SPL, KQL)**, **análisis de logs (red, endpoint, autenticación)**, metodologías de **Threat Hunting visual** y estrategias de **respuesta a incidentes**. **Habilidades comunicacionales:** capacidad para explicar contenidos técnicos complejos de forma clara, adaptándolos a diferentes perfiles laborales (Analistas SOC, personal de TI, etc.). **Facilitación del aprendizaje:** experiencia en el uso de metodologías participativas (análisis de **casos de incidentes reales**, **ejercicios prácticos en SIEM**, **simulaciones de Threat Hunting**) que promuevan la transferencia de conocimientos al entorno laboral. **Capacidad de resolución de consultas técnicas:** habilidad para responder y orientar sobre problemáticas reales en **análisis de datos de seguridad y detección de amenazas**.
Requisitos relativos a la experiencia	Experiencia mínima de 5 años en la **implementación y/o operación en roles de ciberseguridad (Analista SOC, Respuesta a Incidentes, Ciberinteligencia)**, **administración de plataformas SIEM**, **análisis de logs** y **Threat Hunting** en proyectos u operaciones reales.

	Experiencia previa como facilitador en programas de capacitación en **temáticas de ciberseguridad** o análisis de datos. Experiencia en la creación o adaptación de materiales educativos prácticos y **casos de estudio (datasets, escenarios de ataque)** aplicados.

Nombre del curso	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
TENDENCIAS Y FUTURO DE LA CIBERSEGURIDAD	50	1	64	Online asincrónica con sesión sincrónica

Identificación
Código SENCE:
Código Curso Duoc UC:

Unidad Académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Informática y Telecomunicaciones	Oscar Araya	17-12-2025

Especialista disciplinar	Analista instruccional
Claudio González P.	Diego Acosta

Aporte de valor del curso (no SENCE)
El panorama de amenazas digitales evoluciona a una velocidad exponencial. La adopción masiva de la nube, la proliferación de dispositivos IoT y la irrupción de la Inteligencia Artificial Generativa han creado nuevas superficies de ataque que las estrategias de seguridad tradicionales ya no pueden cubrir. Las organizaciones enfrentan ciberataques más sofisticados, como el ransomware operado por IA, los ataques a la cadena de suministro y las amenazas cuánticas emergentes. Este curso entrega a las y los participantes las competencias necesarias para **anticipar, identificar y gestionar las amenazas de ciberseguridad del futuro**. Al finalizar, los participantes podrán evaluar riesgos en entornos cloud e híbridos, diseñar arquitecturas de Confianza Cero (Zero Trust), comprender el impacto de la IA en la ciberdefensa y el ciberataque, y prepararse para la era de la computación cuántica, fortaleciendo la resiliencia y la postura de seguridad de sus organizaciones.

Caracterización del participante
Profesionales y técnicos del área de Tecnologías de la Información, tales como: • Jefes y supervisores de TI y Ciberseguridad. • Analistas de seguridad (SOC). • Ingenieros de redes y sistemas. • Arquitectos de soluciones (Cloud y On-premise). • Oficiales de Seguridad de la Información (CISO) o personal de cumplimiento. • Desarrolladores de software (DevSecOps). • Auditores internos y consultores de TI que busquen actualizar sus conocimientos sobre amenazas emergentes.

Requisitos de ingreso
Ideal conocimientos básicos o experiencia laboral en redes de datos, sistemas operativos y fundamentos de seguridad informática (firewalls, antivirus, gestión de identidades).

Requisitos técnicos
Sistema Operativo Windows 10 o superior; iOS 11 o posterior Memoria RAM: mínimo 8 GB, recomendado 16 GB o más Procesador: 4 Cores y velocidad de 2 GHz o superior Tarjeta de sonido Resolución de monitor: 1024 x 768 o superior. Navegadores Recomendados: Google Chrome (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
Aplicar estrategias de ciberseguridad proactiva considerando las nuevas tendencias en inteligencia artificial, arquitecturas de Confianza Cero y criptografía post-cuántica.

Unidad de aprendizaje	Resultados de aprendizaje	Contenidos	Horas	
			T	P
Unidad 1: el panorama de amenazas modernas	Identificar las tácticas, técnicas y procedimientos (TTPs) de los ciberataques actuales.	• 1. Evolución del Ransomware (RaaS) y doble extorsión. • 2. Ataques a la cadena de suministro (Supply Chain). • 3. Ingeniería social avanzada (Deepfakes, vishing, smishing). • 4. El mercado de la Dark Web y el cibercrimen como servicio (CaaS).	4	6
Unidad 2: IA y Machine Learning en ciberseguridad	Reconocer el uso de la Inteligencia Artificial tanto en situaciones de ciberdefensa como de ciberataque.	• 1. IA en la ofensiva: Automatización de ataques, phishing generativo. • 2. IA en la defensa: Detección de anomalías (UEBA), orquestación y respuesta (SOAR). • 3. Plataformas de protección extendida (XDR) y su integración con IA. • 4. Desafíos éticos y "Adversarial AI".	4	6
Unidad 3: Arquitectura de Confianza Cero (Zero Trust)	Reconocer los pilares de una estrategia de Confianza Cero (ZTA) en entornos corporativos.	• 1. Principios de Zero Trust: "Nunca confiar, siempre verificar". • 2. Pilares de ZTA: Identidad, dispositivo, red, aplicación y datos.	4	6

		• 3. Micro-segmentación y perímetros definidos por software (SDP). • 4. Gestión de Acceso e Identidad (IAM) como núcleo de la estrategia.		
Unidad 4: Seguridad en Entornos Cloud e Híbridos	Reconocer las características de los riesgos específicos en las infraestructuras cloud (IaaS, PaaS, SaaS) y multi-cloud.	• 1. El modelo de responsabilidad compartida. • 2. Gestión de Postura de Seguridad en la Nube (CSPM). • 3. Seguridad de contenedores y Kubernetes. • 4. Seguridad de APIs y entornos "serverless".	4	6
Unidad 5: El futuro: amenaza cuántica y criptografía	Reconocer el riesgo de la computación cuántica hacia la criptografía actual.	• 1. ¿Qué es la computación y la amenaza cuánticas? • 2. El impacto en la criptografía actual (RSA, ECC). • 3. Criptografía Post-Cuántica (PQC): Estándares NIST. • 4. Agilidad criptográfica y preparación para la migración. • 5. Blockchain y la amenaza cuántica.	4	6
Unidad 6: El Factor Humano y la Regulación	Aplicar estrategias de resiliencia y cultura de ciberseguridad en contextos organizacionales.	• 1. Cultura de seguridad: Más allá del phishing (Security Champions). • 2. El rol del "Insider Threat" (amenaza interna). • 3. Panorama regulatorio: Leyes de privacidad y notificación de brechas. • 4. Resiliencia cibernética y planes de respuesta a incidentes.	4	6
Unidad 7: Seminario: Hoja de Ruta de Ciberseguridad	Aplicar técnicas de construcción de una hoja de ruta estratégica con base en metodologías y herramientas de gestión de riesgos.	1. Evaluación final: Desarrollo de caso práctico. Las y los participantes deberán **diseñar y presentar una hoja de ruta estratégica de ciberseguridad**, aplicando **metodologías de gestión de riesgos** en un **escenario simulado o realista**, que integre los riesgos emergentes abordados en las distintas unidades del curso. Para ello, deberán: 1. **Identificar riesgos cibernéticos actuales y emergentes** asociados a: o ataques avanzados (ransomware, ingeniería social, CaaS),		4

		○ entornos de IA (tanto en la ofensiva como en la defensa), ○ arquitecturas Zero Trust, ○ plataformas cloud y multi-cloud, ○ amenazas cuánticas, ○ factores humanos y normativas vigentes. 2. **Evaluar y priorizar los riesgos** detectados usando herramientas de análisis como matrices de impacto/probabilidad, frameworks NIST, o análisis de superficie de ataque. 3. **Diseñar una hoja de ruta estratégica**, que incluya: ○ acciones de mitigación, ○ responsables, ○ plazos, ○ tecnologías a implementar, ○ indicadores de monitoreo. Esta hoja debe reflejar un enfoque integral y realista, considerando capacidades organizacionales y el contexto regulatorio.		
			Subtotal	24	40
			Horas totales	64	

Estrategias metodológicas
El curso se desarrollará en modalidad **e-learning asincrónica** a través del Ambiente Virtual de Aprendizaje (AVA) de eClass. Para esta modalidad, el proceso formativo se desarrollará mediante recursos educativos auto instruccionales tales como: **videos interactivos, guías interactivas, análisis de reportes de inteligencia de amenazas (threat intelligence reports), video tutoriales, infografías y lecturas de *white papers***; a través de los cuales se presentarán los contenidos de forma contextualizada y representativa según la realidad laboral de los participantes. Los recursos educativos estarán disponibles en versión audiovisual y/o descargable. Además, se desarrollarán evaluaciones formativas enfocadas a la aplicación práctica de los contenidos. Para ello, se utilizarán estrategias metodológicas de enseñanza-aprendizaje como: **resolución de problemas, análisis de casos (basados en ciberataques reales y recientes), simulaciones de respuesta a incidentes y aprendizaje basado en proyectos**.

Descripción de unidades:

- **Unidad 1: El Panorama de Amenazas Modernas** Esta unidad introduce a los participantes en el ecosistema actual del cibercrimen. Se analizarán las tácticas, técnicas y procedimientos (TTPs) más recientes, como el Ransomware como Servicio (RaaS) y los ataques a la cadena de suministro. Los estudiantes comprenderán cómo la ingeniería social ha evolucionado con herramientas como los *deepfakes* y por qué las defensas tradicionales ya no son suficientes.
- **Unidad 2: IA y Machine Learning en Ciberseguridad** En esta unidad, se profundiza en el rol dual de la Inteligencia Artificial. Los estudiantes aprenderán cómo la IA es utilizada por los atacantes para automatizar y optimizar ciberataques, y, a su vez, cómo es empleada por los defensores para la detección avanzada de anomalías (UEBA) y la orquestación de la respuesta (SOAR). Se explorará el concepto de XDR (Detección y Respuesta Extendida) como una evolución clave impulsada por la IA.
- **Unidad 3: Arquitectura de Confianza Cero (Zero Trust)** Esta unidad se enfoca en el cambio de paradigma fundamental de la ciberseguridad: del modelo de "castillo y foso" a la Confianza Cero (Zero Trust). Los estudiantes aprenderán los principios de "nunca confiar, siempre verificar" y cómo implementar sus pilares fundamentales, incluyendo la identidad como perímetro de seguridad, la microsegmentación de redes y la gestión de acceso de mínimo privilegio.
- **Unidad 4: Seguridad en Entornos Cloud e Híbridos** En esta unidad, los estudiantes abordarán los desafíos únicos de seguridad que presentan las infraestructuras en la nube (IaaS, PaaS, SaaS) y los entornos híbridos. Se explorarán conceptos clave como el modelo de responsabilidad compartida, la gestión de la postura de seguridad en la nube (CSPM), y las estrategias específicas para proteger contenedores, Kubernetes y APIs, que son superficies de ataque críticas en aplicaciones modernas.
- **Unidad 5: El Futuro: Amenaza Cuántica y Criptografía** Esta unidad ofrece una visión prospectiva de la amenaza más disruptiva en el horizonte: la computación cuántica. Los estudiantes comprenderán por qué las computadoras cuánticas romperán la criptografía actual (como RSA y ECC) y aprenderán sobre el desarrollo de la Criptografía Post-Cuántica (PQC) y los nuevos estándares NIST, preparando a sus organizaciones para la futura "migración criptográfica".
- **Unidad 6: El Factor Humano y la Regulación** Esta unidad se centra en el eslabón más crítico de la cadena de seguridad: las personas. Los estudiantes aprenderán estrategias para construir una cultura de ciberseguridad robusta que vaya más allá del *phishing*, cómo gestionar el riesgo de la amenaza interna (*insider threat*) y cómo navegar el creciente y complejo panorama de regulaciones y leyes de privacidad de datos.

Estrategias evaluativas		
Indicadores de logro	**Instrumentos de evaluación**	**Normas de aprobación**
Unidad 1		
Identifica las tácticas, técnicas y procedimientos (TTPs) de amenazas modernas en contextos de ciberseguridad.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de	Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo

Reconoce la evolución de la ingeniería social mediante la identifiación de nuevas alternativas de amenaza. Reconoce los motivos de ineficiencia de las defensas perimetrales tradicionales ante nuevas amenazas.	selección única que se evaluarán con claves.	requerido para la aprobación. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 2		
Reconoce el rol dual de la IA en situaciones defensivas y ofensivas. Reconoce maneras en que la IA potencia la detección avanzada (UEBA) y la orquestación (SOAR) en contextos de ciberseguridad. Identifica el concepto de XDR (Detección y Respuesta Extendida) como una evolución impulsada por la IA.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 3		
Reconoce el contraste entre paradigma "nunca confiar, siempre verificar" y el modelo de "castillo y foso" en situaciones de amenaza. Identifica los pilares fundamentales de una arquitectura Zero Trust (ZTA) en ciberseguridad. Reconoce los conceptos de identidad como perímetro y micro-segmentación en un escenario dado.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 4		

Reconoce diferencias en los desafíos de seguridad específicos de IaaS, PaaS y SaaS. Reconoce correctamente las características del modelo de responsabilidad compartida en un escenario híbrido. Reconoce el uso de estrategias de riesgos clave en contenedores, Kubernetes y APIs como superficies de ataque.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 5		
Reconoce los riesgos de la computación cuántica a la criptografía actual. Reconoce el impacto de algoritmos cuánticos sobre RSA y ECC con base en vulnerabilidades. Reconoce los principales algoritmos de criptografía post-cuántica (Kyber, Dilithium, Falcon) y su estado en NIST. Reconoce estrategias de agilidad criptográfica en la preparación de migración hacia esquemas post-cuánticos. Reconoce el impacto de la amenaza cuántica en Blockchain, según riesgos y posibles soluciones post-cuánticas.	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de selección única que se evaluarán 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. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 6% de la calificación final.**
Unidad 6		
Identifica los requisitos clave de las regulaciones y leyes relevantes respecto a privacidad de datos Aplica estrategias de construcción de una cultura de ciberseguridad	La evaluación tiene una finalidad sumativa a través de heteroevaluación Para ello, los participantes deberán desarrollar una prueba de selección única de manera individual, debiendo completar una serie de ítems de	Las calificaciones derivadas de las evaluaciones sumativas estarán expresadas con notas entre 1.0 y 7.0, siendo 4.0 el mínimo

considerando defensas a ataques más allá del phishing. Aplica métodos de gestión del riesgo de la amenaza interna	selección única que se evaluarán con claves.	requerido para la aprobación. Se corregirá el desarrollo aplicando un 60% de exigencia. **Estas evaluaciones representan el 10% de la calificación final.**
Evaluación Final		
Aplica técnicas de diagnóstico correcto de los riesgos emergentes en un caso de estudio integral. Propone controles modernos (ZTA, IA, PQC) de forma coherente en una estrategia. Aplica técnicas de diseño de una Hoja de Ruta (Roadmap) de ciberseguridad estratégica, priorizada y con planificación deresiliencia a largo plazo.	Entrega de un documento "Hoja de Ruta de Ciberseguridad" basado en el caso de estudio provisto, evaluado mediante una rúbrica detallada.	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. Se corregirá el desarrollo aplicando un 50% de exigencia. **Esta evaluación representa el 60% de la calificación final.**

Requisito de aprobación	
Modalidad asincrónica	Nota mínima de aprobación 4.0

Recursos para la implementación					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
N/A	N/A	1 1	Plataforma LMS (AVA) Computador	1 1	El curso estará disponible en http://cursos.eclass.com/. Seleccionar la opción RUT en TIPO DE DOCUMENTO. La guía de uso de la plataforma se encuentra en Http://cursos.eclass.com, en la pestaña

				1 6 6 6	Información correspondiente al curso. Inducción tecnológica/metodológica, estará disponible en http://cursos.eclass.com Unidades publicadas en el sitio Http://cursos.eclass.com /Están escritas en lenguaje claro y contienen gráfica para facilitar la comprensión por parte de los alumnos. Actividades de aplicación publicadas en el sitio http://cursos.eclass.com / Resumen y glosario de contenido publicados en el sitio Http://Cursos.Eclass.Com/

Próxima actualización sugerida (Debe ser sugerido por Experto Disciplinar designado por la Unidad Académica)
Máximo tres años

Diplomado	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
DIPLOMADO EN CIBERSEGURIDAD	Aspectos legales de ciberseguridad y protección de datos
	Seguridad computacional en la organización
	Visualización de datos aplicada
	Tendencias y Futuro de la Ciberseguridad

Convalidación		
Diplomado	**Curso**	**Código**
N/A	N/A	N/A
N/A	N/A	N/A

N/A	N/A	N/A

Articulación		
Programa	**Escuela**	**Código**
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A

Otros cursos relacionados con la temática
N/A
N/A
N/A

Perfil: Especialista disciplinar diseñador(a)	
Requisitos relativos a la educación	Universitario con postítulo
Requisitos relativos a la formación	Formación en ingeniería informática, ingeniería en ciberseguridad, ciencias de la computación, telecomunicaciones, derecho digital o carrera afín, con sólida base académica en normativas de seguridad, gestión de riesgos tecnológicos, arquitectura de redes y protección de datos. Deseable diplomado, magíster o cursos de especialización en ciberseguridad, inteligencia artificial aplicada, derecho informático, gestión de incidentes o certificaciones reconocidas (por ejemplo: CISSP, CISM, ISO/IEC 27001, CompTIA Security+).
Requisitos relativos a las habilidades	**Diseño instruccional especializado**: capacidad para estructurar programas formativos integrando normativas de ciberseguridad, arquitecturas defensivas, herramientas de cumplimiento, análisis de amenazas y metodologías de respuesta a incidentes. **Análisis y síntesis técnica y normativa**: habilidad para interpretar y adaptar legislación digital, estándares de seguridad (como NIST, ISO/IEC), y metodologías técnicas (como Zero Trust, XDR, CSPM), transformándolos en contenidos didácticos aplicables a contextos laborales reales. **Elaboración de materiales educativos**: capacidad en la creación de guías interactivas, infografías, análisis de casos reales, simulaciones, actividades evaluativas y recursos multimedia que faciliten la aplicación práctica de los contenidos. **Actualización técnica**: capacidad para integrar en los contenidos cambios tecnológicos, tendencias emergentes (como IA ofensiva/defensiva, amenazas cuánticas), y buenas prácticas internacionales en ciberseguridad, privacidad y resiliencia organizacional.
Requisitos relativos a la experiencia	**Experiencia mínima de 5 años en el diseño de programas o cursos de ciberseguridad**, incluyendo aspectos normativos, arquitecturas defensivas, gestión de riesgos tecnológicos, protección de datos y respuesta a incidentes. **Experiencia en el desarrollo de contenidos educativos con enfoque aplicado y contextualizado**, integrando casos reales de ciberataques, simulaciones de respuesta, análisis de amenazas emergentes y proyectos prácticos alineados

	con entornos laborales actuales (cloud, híbridos, Zero Trust, IA defensiva/ofensiva). Familiaridad con entornos virtuales de aprendizaje (AVA) y metodologías asincrónicas, incluyendo el uso de recursos auto instruccionales como videos interactivos, guías, tutoriales, infografías y análisis de reportes de inteligencia de amenazas. Capacidad demostrada para integrar tendencias disruptivas como la computación cuántica, la Criptografía Post-Cuántica (PQC), y el cumplimiento normativo en privacidad y protección de datos.

Perfil: Especialista disciplinar facilitador(a)	
Requisitos relativos a la educación	Universitario con postítulo.
Requisitos relativos a la formación	Formación en ingeniería informática, ciberseguridad, telecomunicaciones, ciencias de la computación, derecho digital o carrera afín, con conocimientos actualizados en normativas de seguridad, gestión de riesgos tecnológicos, protección de datos y arquitectura de redes. Deseable diplomado, magíster o cursos de especialización en ciberseguridad, inteligencia artificial aplicada, derecho informático, gestión de incidentes o certificaciones reconocidas (por ejemplo: CISSP, CISM, ISO/IEC 27001, CompTIA Security+).
Requisitos relativos a las habilidades	Dominio integral de la temática: manejo sólido y actualizado de normativas de ciberseguridad, implementación de arquitecturas defensivas (Zero Trust, XDR), auditoría de sistemas de seguridad, evaluación de riesgos tecnológicos y estrategias de mitigación en entornos cloud e híbridos. Habilidades comunicacionales: capacidad para explicar contenidos técnicos complejos como IA ofensiva/defensiva, amenazas cuánticas o simulaciones de respuesta, adaptándolos a distintos perfiles laborales. Facilitación del aprendizaje: experiencia en el uso de metodologías participativas como análisis de casos reales de ciberataques, simulaciones de respuesta a incidentes, resolución de problemas y aprendizaje basado en proyectos, que promuevan la transferencia de conocimientos al entorno laboral. Capacidad de resolución de consultas técnicas: habilidad para orientar sobre problemáticas reales en cumplimiento normativo, gestión de amenazas emergentes, implementación de controles modernos y resiliencia organizacional.
Requisitos relativos a la experiencia	Experiencia mínima de 5 años en la implementación y/o supervisión de estrategias de ciberseguridad, cumplimiento normativo, gestión de riesgos tecnológicos y respuesta a incidentes en proyectos u operaciones reales. Experiencia previa como facilitador en programas de capacitación en temáticas de ciberseguridad, privacidad de datos o transformación digital.

	Experiencia en la creación o adaptación de materiales educativos prácticos, simulaciones, análisis de casos y recursos interactivos contextualizados al entorno laboral.