FUNDACIÓN INSTITUTO PROFESIONAL DUOC UC
VICERRECTORÍA ACADÉMICA
RESOLUCIÓN Nº38/2024

APRUEBA DIPLOMADO EN CIBERSEGURIDAD CORPORATIVA

VISTOS:

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

RESUELVO:

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

Comuníquese, publíquese y regístrese.

Santiago, septiembre 5 de 2024.

Alejandra Silva Lafourcade
Firmado digitalmente por Alejandra Silva Lafourcade
Fecha: 2024.09.05 10:15:01 -04'00'

ALEJANDRA SILVA LAFOURCADE
DIRECTORA GENERAL DE DESARROLLO ESTUDIANTIL Y EDUCACIÓN CONTÍNUA

Kiyoshi Fukushi
Firmado digitalmente por Kiyoshi Fukushi
Fecha: 2024.09.06 14:34:24 -04'00'

KIYOSHI FUKUSHI MANDIOLA
VICERRECTOR ACADÉMICO

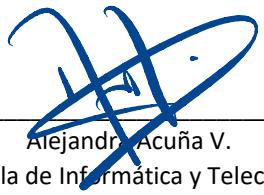
KFM/ASL/JMD/MCS

PRESENTACIÓN DE DIPLOMADO

Señor:
Kiyoshi Fukushi M.
Vicerrector Académico
Duoc UC

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

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



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

DIPLOMADO EN CIBERSEGURIDAD CORPORATIVA

RESUMEN:

Diplomado de oferta abierta desarrollado por la Escuela de Informática y Telecomunicaciones. En la actualidad, donde las amenazas digitales evolucionan de manera constante y el entorno normativo se vuelve cada vez más complejo, la necesidad de contar con profesionales altamente capacitados en el ámbito de ciberseguridad es más crítica que nunca. La ciberseguridad se ha convertido en un componente esencial para la protección de infraestructuras digitales, y las organizaciones deben estar preparadas para enfrentar y mitigar una amplia variedad de riesgos cibernéticos.

El Diplomado en Ciberseguridad Corporativa está diseñado para responder a esta necesidad imperante, proporcionando a los estudiantes una formación integral en ciberseguridad. Este programa educativo destaca por su enfoque práctico y teórico, preparando a los estudiantes para liderar la protección efectiva de los sistemas de información en un entorno laboral cada vez más desafiante, a través del fortalecimiento de su comprensión sobre las amenazas cibernéticas y cómo abordarlas, y de la entrega de habilidades prácticas y estratégicas que les servirán para promover una cultura de seguridad informática en el ámbito empresarial y personal. Más allá de entender las regulaciones que protegen la privacidad en línea, los estudiantes aprenderán a aplicar activamente estos conocimientos en su día a día, garantizando que sus acciones estén siempre alineadas con las normativas vigentes.

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

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

Nombre Módulos	Horas	% de la nota final de diplomado
Estrategias de Seguridad de la Información para las TICs	30	25%
Cumplimiento, Normativas y Aspectos Legales de Ciberseguridad	30	25%
Gestión de Proyectos en Ciberseguridad	30	25%
Estrategias de Gobernanza y Gestión de Riesgo	30	25%
TOTAL DE HORAS	**120**	**100%**

Destinado a profesionales de TI o técnicos que realicen labores como administradores de sistemas, analistas de seguridad y desarrolladores. Jefes de proyectos y/o líderes de equipo que gestionen recursos tecnológicos. Auditores y consultores que buscan comprender prácticas avanzadas de seguridad. Profesionales de derecho y gestión empresarial enfocados en cumplimiento normativo y gobernanza de TI.

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

FICHA ÚNICA DE CREACIÓN DE DIPLOMADOS
PNCT

1. NOMBRE DEL DIPLOMADO

Diplomado en Ciberseguridad Corporativa

2. TOTAL DE HORAS

120

3. POBLACIÓN OBJETIVO

Profesionales de TI o técnicos que realicen labores como administradores de sistemas, analistas de seguridad y desarrolladores. Jefes de proyectos y/o líderes de equipo que gestionen recursos tecnológicos. Auditores y consultores que buscan comprender prácticas avanzadas de seguridad. Profesionales de derecho y gestión empresarial enfocados en cumplimiento normativo y gobernanza de TI.

4. REQUISITOS DE INGRESO

Experiencia en TI o roles relacionados con seguridad de datos. Conocimiento básico de sistemas operativos y redes. Comprensión de principios de gestión de riesgos y prácticas de seguridad informática.

5. JUSTIFICACIÓN DE CREACIÓN

En la actualidad, donde las amenazas digitales evolucionan de manera constante y el entorno normativo se vuelve cada vez más complejo, la necesidad de contar con profesionales altamente capacitados en el ámbito de ciberseguridad es más crítica que nunca. La ciberseguridad se ha convertido en un componente esencial para la protección de infraestructuras digitales, y las organizaciones deben estar preparadas para enfrentar y mitigar una amplia variedad de riesgos cibernéticos.

El Diplomado en Ciberseguridad Corporativa está diseñado para responder a esta necesidad imperante, proporcionando a los estudiantes una formación integral en ciberseguridad. Este programa educativo destaca por su enfoque práctico y teórico, preparando a los estudiantes para liderar la protección efectiva de los sistemas de información en un entorno laboral cada vez más desafiante, a través del fortalecimiento de su comprensión sobre las amenazas cibernéticas y cómo abordarlas, y de la entrega de habilidades prácticas y estratégicas que les servirán para promover una cultura de seguridad informática en el ámbito empresarial y personal. Más allá de entender las regulaciones que protegen la privacidad en línea, los estudiantes aprenderán a aplicar activamente estos conocimientos en su día a día, garantizando que sus acciones estén siempre alineadas con las normativas vigentes.

6. OBJETIVO GENERAL/ IDENTIFICACIÓN PERFIL DE SALIDA

Evaluar riesgos en ciberseguridad considerando metodologías de gestión de proyectos, regulaciones normativas y políticas de seguridad informática efectivas.

7. UNIDAD ACADÉMICA

ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES

8. FECHA

24-6-2024

9. REQUISITOS DE OBTENCIÓN

9.1 - Haber aprobado todos los Cursos del Diplomado

Aprobar los cuatro cursos que componen el Diplomado.

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

Nombre Curso	Horas	% de la nota final de Diplomado
Estrategias de seguridad de la información para las TICs	30	25%
Cumplimiento, normativas y aspectos legales de ciberseguridad	30	25%
Gestión de proyectos en ciberseguridad	30	25%

Estrategias de gobernanza y gestión de riesgo	30	25%
	120	**100%**

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

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

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

10. MODALIDAD DE IMPARTICIÓN

	Modalidad
Presencial	
Semipresencial	
E-learning (asincrónico)	x

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso:	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
Estrategias de Seguridad de la Información para las TICs	50	1	30	Asincrónica

Identificación
Código SENCE
Código curso DuocUC

Unidad académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Escuela de Informática y Telecomunicaciones	Oscar Araya	10/05/2024

Especialista disciplinar	Diseñador(a) curricular	Diseñador(a) instruccional	Analista instruccional
Miguel Ortiz Vera	Miguel Velasco	Ámbar Núñez	Cristian Domínguez

Aporte de valor del programa (no SENCE)
En un mundo interconectado donde los datos representan el núcleo de las organizaciones modernas, la seguridad de la información se convierte en el baluarte esencial que protege contra las amenazas digitales. No es solo una cuestión de establecer barreras y protocolos; es sobre forjar una cultura de seguridad consciente y preparada que pueda adaptarse y reaccionar a un panorama de amenazas en constante evolución. Desde una perspectiva tanto teórica como aplicada, este programa se dedica a inculcar prácticas de seguridad de la información robustas y estratégicas. Se focaliza en tres pilares cruciales: salvaguardar la confidencialidad, integridad y disponibilidad de los datos (CIA); instaurar una gestión de riesgos proactiva que no solo previene, sino que también planifica respuestas ágiles ante incidentes; y promover un cumplimiento normativo que alínea a las empresas con estándares internacionales y legislaciones pertinentes. Este programa surge para responder a la necesidad imperativa de proteger los activos más valiosos en el terreno digital, equipando a los profesionales con el conocimiento, las herramientas y las competencias para edificar una infraestructura TIC resiliente y confiable, y para asegurar que, en la interfaz de la tecnología y el negocio, la seguridad sea una constante prioridad y una ventaja competitiva tangible.

Caracterización del participante
Profesionales y técnicos que hayan cursado una carrera, de a lo menos 6 semestres, idealmente del área TI y que realicen labores como administradores de sistemas, analistas de seguridad y desarrolladores. Jefes de proyectos y/o líderes de equipo que gestionen recursos tecnológicos. Auditores y consultores que buscan comprender prácticas avanzadas de seguridad. Profesionales de derecho y gestión empresarial enfocados en cumplimiento normativo y gobernanza de TI.

Requisitos de ingreso del participante
Experiencia en TI o roles relacionados con seguridad de datos. Conocimiento básico de sistemas operativos y redes. Comprensión de principios de gestión de riesgos y prácticas de seguridad informática.

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

Objetivo general
Aplicar estrategias de seguridad informática de acuerdo con las políticas de seguridad de la empresa.

Unidades	Objetivo específico	Contenidos	Horas	
			T	P
Unidad 1: Fundamentos y Gestión de la Seguridad de la Información	Aplicar técnicas de protección de información de acuerdo con estrategia de gestión de riesgos y políticas de seguridad de la empresa	**1. Introducción a la seguridad de la información:** 1.1 Definición y principios clave (CIA). 1.2 Amenazas y vulnerabilidades. 1.3 Medidas de seguridad: Firewalls, VPNs y sistemas de detección de intrusiones (IDS/IPS). **2. Medidas de seguridad:** 2.1 Técnicas de protección de datos. 2.2 Estrategias de defensa. **3. Introducción a la Gestión de la seguridad de la información:** 3.1 Gestión de riesgos y evaluación de amenazas y vulnerabilidades. 3.2 Planificación y ejecución de políticas de seguridad.	6	9
Unidad 2 Seguridad Técnica en TICs y Seguridad en la Nube	Analizar la seguridad (de la infraestructura) en redes y aplicaciones de acuerdo con criterios de vulnerabilidad de la información	**1. Seguridad en redes y aplicaciones:** 1.1. Implementación de protocolos de seguridad en redes. 1.2. Técnicas de desarrollo y pruebas de seguridad en aplicaciones web. **2. Protección de datos y privacidad:** 2.1 Métodos de encriptación y gestión de claves. 2.2 Estrategias de control de acceso y protección de datos.	5	10

		3. Seguridad de la infraestructura en la nube: 3.1. Exploración de modelos de servicio en la nube (SaaS, PaaS, IaaS). 3.2. Evaluación de seguridad en la infraestructura de proveedores de nube. **4. Tecnologías emergentes y su impacto en la seguridad:** 4.1. Inteligencia Artificial y Seguridad. 4.2. Blockchain y Seguridad. 4.3. Protección de la información en Internet de las Cosas (IoT).		
			Subtotal	11	19
			Horas totales	30	

Estrategias metodológicas
La estrategia metodológica corresponde a la auto instrucción, considerando el diseño del curso una modalidad 100% online donde el proceso de enseñanza/aprendizaje se desarrollará a través de diversos recursos, los cuales estarán dispuestos de forma ordenada en el Ambiente Virtual de Aprendizaje establecido por Duoc UC, según el programa formativo con el fin de que los y las participantes adquieran el conocimiento de manera significativa y dinámica. Los recursos educativos como videos interactivos, guías de aprendizaje, infografías, entre otros; se trabajarán de forma contextualizada y representativa de la realidad laboral de los y las participantes, quienes tendrán a disposición el material para su proceso de aprendizaje, tanto en formato audiovisual como en formato descargable. El trabajo académico privilegia la autorregulación, la colaboración, la responsabilidad y el compromiso, entre otras habilidades, para lograr aprendizajes significativos, utilizando, para ello, herramientas digitales que promueven la retroalimentación y la interacción mediante actividades y recursos que tendrán como propósito la activación de conocimientos previos que se vincularán posteriormente con ideas nuevas, la demostración del contenido en un contexto objetivo y real; la aplicación de lo aprendido mediante el desarrollo de actividades formativas y sumativas y, finalmente, la integración de los aprendizajes. El curso tiene una duración total de 30 horas distribuidas en seis semanas, considerando una dedicación semanal de máximo cinco horas. Además, se realizará una sesión sincrónica (opcional) de dos horas, que permitirá a los y las participantes resolver dudas, profundizar en temas de interés y compartir experiencias con los y las demás participantes. **Descripción de las unidades:** **Unidad 1:** Introduce a los participantes en los fundamentos de la seguridad de la información, enfatizando la importancia de la confidencialidad, integridad y disponibilidad (CIA). Se abordan las distintas amenazas y vulnerabilidades a las que están expuestas las TICs, así como las medidas defensivas correspondientes como firewalls y sistemas de prevención de intrusiones. Además, se explora la gestión de riesgos y la implementación de políticas de seguridad, equipando a los estudiantes con conocimientos teóricos y habilidades prácticas esenciales para proteger los recursos de información. Se utilizará la metodología de análisis de casos para abordar la temática de esta primera unidad.

Unidad 2: Se centra en la seguridad operacional y técnica dentro de las TICs, cubriendo aspectos críticos de la seguridad en redes y aplicaciones. Se investiga la implementación de protocolos de seguridad robustos, prácticas de encriptación y control de acceso, esenciales para la protección de datos. La seguridad en entornos de nube se examina a través de la evaluación de modelos de servicio y la seguridad de infraestructuras proporcionadas por terceros, preparando a los estudiantes para navegar en el creciente ecosistema de la nube. El análisis y desarrollo de casos será la base para que los aprendizajes, tanto teóricos como prácticos, permitiendo el logro de los objetivos de manera efectiva, característica propia de este diplomado.

Estrategias evaluativas		
Criterios de evaluación:	**Instrumentos de evaluación:**	**Normas de aprobación:**
Evaluación Diagnóstica		
Reconoce los principios fundamentales de la seguridad de la información.	La evaluación diagnóstica consiste en la resolución de preguntas con alternativas de respuesta de selección simple. Esta evaluación estará dispuesta en el AVA y se dará retroalimentación automática.	Esta evaluación no tiene ponderación.
Unidad 1		
Identifica la importancia de los principios de Confidencialidad, Integridad y Disponibilidad en la seguridad de la información y cómo se relacionan con las amenazas y vulnerabilidades actuales. Comprende los riesgos de seguridad de la información mediante la identificación y el análisis de amenazas y vulnerabilidades potenciales. Aplica técnicas de protección de datos y estrategias de defensa, incluido el uso adecuado de firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) en un escenario dado. Aplica políticas de seguridad, evidenciando la comprensión de los componentes críticos de una política efectiva y la ejecución de éstas en un entorno controlado. Utiliza la gestión de la seguridad de la información en estudios de caso, identificando áreas de fortaleza y oportunidades de mejora.	En esta unidad, se evaluará la comprensión y aplicación de los principios fundamentales de la seguridad de la información, a través de un análisis de caso y posterior resolución de preguntas de selección simple. La evaluación será individual y se desarrollará en la plataforma con retroalimentación automática.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 30% de la calificación final del curso.**

Unidad 2		
Determina la efectividad de protocolos de seguridad en redes que protegen contra intrusiones en un escenario de red corporativa. Utiliza algoritmos y técnicas de gestión de claves en un entorno de prueba. Establece controles de acceso que salvaguarden datos en sistemas de información, mostrando su aplicación en un caso de uso empresarial. Analiza configuraciones de seguridad en la nube, comparando diferentes modelos de servicio y sus implicancias en la protección de la infraestructura. Selecciona aplicaciones web para detectar y remediar vulnerabilidades.	En esta unidad, se evaluarán los conocimientos técnicos para analizar la seguridad de redes y aplicaciones, garantizando la seguridad de la infraestructura y las aplicaciones en entornos de nube, a través de un análisis de caso y posterior desarrollo de actividades. La evaluación será individual y se desarrollará en un formato de entrega, donde los/as participantes deberán desarrollar una serie de actividades en los espacios destinados para ello. Se utilizará rúbrica como instrumento de evaluación.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 30% de la calificación final del curso.**
Evaluación Final		
Analiza un escenario de caso dado para identificar riesgos y vulnerabilidades, aplicando conocimientos de encriptación y control de accesos. Aplica mejoras basadas en un análisis crítico de las configuraciones de seguridad existentes en la infraestructura de un proveedor de nube. Propone un plan de gestión de riesgos y políticas de seguridad detallado para un entorno de nube, incluyendo SaaS, PaaS y IaaS. Selecciona un sistema integral de seguridad que aborde tanto la protección de redes como la de aplicaciones, enfocándose en la seguridad técnica y en la nube.	La evaluación final consiste en asegurar la confidencialidad, integridad y disponibilidad de la información en un caso dado, en el cual se debe realizar análisis para reconocer amenazas y vulnerabilidades y se debe aplicar mecanismos de protección de la información. La evaluación será individual y se desarrollará en un formato de entrega, tipo informe, donde cada participante deberá desarrollar una serie de actividades en los espacios destinados para ello. Se utilizará una rúbrica como instrumento de evaluación.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 40% de la calificación de fin de curso**.

Requisito de aprobación	
Modalidad sincrónica - asincrónica	Nota mínima de aprobación 4.0

Recursos para la implementación del curso					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
Características de la infraestructura requerida para la ejecución del curso.	**Dónde se impartirá el curso** ***Anexo ficha de costos**	**Indicar cantidad**	**Tipo de equipo y/o herramienta para la implementación del curso** ***Indicar duración de licencias o equipamientos.**	**Indicar cantidad**	**Indicar el material que se requiere para la implementación del curso**
N/A	N/A	1 (P/P)	Notebook o computador de escritorio con conexión a internet. Ambiente Virtual de Aprendizaje (AVA) DUOC. Blackboard Ultra. Sistema de videoconferencia online integrado a plataforma.	1 (P/P)	Programa, recursos educativos y evaluaciones vinculadas a cada unidad. Link o acceso a recursos audiovisuales utilizados en sesiones (en los casos que corresponda), o su URL. Bibliografía digital.

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

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

Diplomado:	Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)
Diplomado en Ciberseguridad Corporativa	**1. Estrategias de Seguridad de la Información para las TICs**
	2. Cumplimiento, Normativas y Aspectos Legales de Ciberseguridad
	3. Gestión de Proyectos en Ciberseguridad

	4. Estrategias de Gobernanza y gestión de riesgo

Otros cursos relacionados con la temática

Recursos docentes: Perfil desarrollador	
Profesión	Ingeniero Informático o carrera afín, con especialización en ciberseguridad.
Años de experiencia	10 años o más.
Conocimientos y habilidades relevantes	Experiencia docente con experiencia práctica en el área de la seguridad de la información aplicada a la industria. Dominio de los principios fundamentales de confidencialidad, disponibilidad y confidencialidad, además de los riesgos y herramientas para la prevención de incidentes informáticos. Conocimiento sólido en diseño de mecanismos de protección y controles de seguridad, tanto en entornos on-premise como cloud. Habilidad destacada para comunicar conceptos complejos de manera clara, adaptándose a diversos niveles de conocimiento. Versátil y hábil para guiar la creación efectiva de experiencias digitales altamente usables.
Observaciones	

Recursos docentes: Perfil relator	
Profesión	Ingeniero Informático o carrera afín, con especialización en ciberseguridad.
Años de experiencia	3 años o más en el área disciplinar 2 años o más en docencia o relatorías
Conocimientos y habilidades relevantes	Capacidad de comunicar de manera efectiva los principios fundamentales de la seguridad de la información. Con un enfoque claro en la prevención de incidentes de seguridad a través de controles, tanto en entorno on-premise como cloud. Además, se valorará su conocimiento sobre gestión de riesgos, políticas de seguridad, y seguridad en tecnologías emergentes.
Observaciones	

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso:	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
Cumplimiento, Normativas y Aspectos Legales de Ciberseguridad	50	1	30	Asincrónica

Identificación
Código SENCE
Código curso DuocUC

Unidad académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Escuela de Informática y Telecomunicaciones	Oscar Araya	10/05/2024

Especialista disciplinar	Diseñador(a) curricular	Diseñador(a) instruccional	Analista instruccional
Felipe Flores	Miguel Velasco	Ámbar Núñez	Cristian Domínguez

Aporte de valor del programa (no SENCE)
A través de este curso integral de ciberseguridad, los participantes no solo fortalecerán su comprensión sobre las amenazas cibernéticas y cómo abordarlas, sino que también adquirirán habilidades prácticas y estratégicas para promover una cultura de seguridad informática tanto en el ámbito empresarial como en su entorno personal. Más allá de entender las regulaciones que protegen la privacidad en línea, los estudiantes aprenderán a aplicar activamente estos conocimientos en su día a día, garantizando que sus acciones estén siempre alineadas con las normativas vigentes. A lo largo del curso, se explorarán en detalle las leyes y regulaciones relevantes en materia de ciberseguridad, permitiendo a los participantes comprender su alcance y aplicación práctica en diversos contextos organizacionales. Al estar plenamente informados sobre las regulaciones pertinentes, los estudiantes serán capaces de contribuir significativamente a que sus empresas cumplan con todas las leyes relacionadas con la ciberseguridad, lo que no solo refuerza la confianza del público en la empresa, sino que también garantiza la protección integral de los datos confidenciales. Con un enfoque práctico y orientado a resultados, este curso ofrece a los participantes las herramientas y el conocimiento necesario para enfrentar los desafíos emergentes en el panorama digital actual y convertirse en líderes en la promoción de la seguridad cibernética en sus organizaciones y comunidades.

Caracterización del participante
Profesionales y técnicos que hayan cursado una carrera, de a lo menos 6 semestres, idealmente del área TI y que realicen labores en Equipos de gestión y/o Directivos, Oficiales de Seguridad de la información, Personal de área jurídica y cumplimiento legal.

Requisitos de ingreso del participante
Experiencia en TI o roles relacionados con seguridad de datos, conocimiento básico de sistemas operativos y redes, y/o comprensión de principios de gestión de riesgos y prácticas de seguridad informática.

Requisitos técnicos del participante
Sistema Operativo Windows 10 o superior; iOS 11 o posterior
Memoria RAM: 16 GB o más
Procesador: velocidad de 2 GHz o superior
Tarjeta de sonido
Resolución de monitor: 1024 x 768 o superior.

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

Objetivo general
Analizar las regulaciones normativas de ciberseguridad de acuerdo a normas vigentes a nivel internacional y en Chile

Unidades	**Objetivo específico**	**Contenidos**	**Horas**	
			T	**P**
Unidad 1 Fundamentos Legales y Marco Regulatorio en Ciberseguridad	Comprender las leyes y marcos internacionales de ciberseguridad de acuerdo con sus alcances	**1.** Introducción a la legislación chilena en ciberseguridad 1.1 Panorama general de las leyes y regulaciones relevantes. **2.** Ley N° 19.628 sobre Protección de la Vida Privada 2.1 Principios y disposiciones clave de la ley. 2.2 Obligaciones para las organizaciones en el manejo de datos personales. **3.** Ley N° 21.459 sobre Delitos Informáticos 3.1 Tipos de delitos informáticos y sus sanciones asociadas. 3.2 Procedimientos legales para la investigación y persecución de delitos informáticos en Chile. **4.** Ley marco de ciberseguridad 4.1 Implicancias en el contexto chileno.	6	9
Unidad 2 Implementación Práctica y Cumplimiento Normativo en Ciberseguridad	Aplicar la normativa de ciberseguridad en la gestión de los riesgos informáticos de la empresa.	**1.** Evaluación de riesgos y estrategias de mitigación 1.1 Descripción detallada de la ISO 270001. 1.2 Riesgos cibernéticos específicos para organizaciones en Chile. 1.3 Estrategias de mitigación basadas en la legislación y regulaciones aplicables. **2.** Capacitación y concientización en ciberseguridad 2.1 Capacitación para empleados sobre aspectos legales y normativos en ciberseguridad.	5	10

		2.2 Fomento de una cultura de seguridad cibernética en la organización. **3.** Auditorías de seguridad y cumplimiento normativo 3.1 Auditorías de seguridad cibernética y evaluación de cumplimiento normativo. 3.2 Identificando áreas de mejora y acciones correctivas basadas en la auditoría.		
		Subtotal	11	19
		Horas totales	30	

Estrategias metodológicas
La estrategia metodológica corresponde a la auto instrucción, considerando el diseño del curso una modalidad 100% online donde el proceso de enseñanza/aprendizaje se desarrollará a través de diversos recursos, los cuales estarán dispuestos de forma ordenada, en el Ambiente Virtual de Aprendizaje establecido por Duoc UC, según el programa formativo con el fin de que los y las participantes adquieran el conocimiento de manera significativa y dinámica. Los recursos educativos como videos interactivos, guías de aprendizaje, infografías, entre otros; se trabajarán de forma contextualizada y representativa de la realidad laboral de los y las participantes, quienes tendrán a disposición el material para su proceso de aprendizaje, tanto en formato audiovisual como en formato descargable. El trabajo académico privilegia la autorregulación, la colaboración, la responsabilidad y el compromiso, entre otras habilidades, para lograr aprendizajes significativos, utilizando para ello herramientas digitales que promueven la retroalimentación y la interacción mediante actividades y recursos que tendrán como propósito la activación de conocimientos previos que se vincularán posteriormente con ideas nuevas, la demostración del contenido en un contexto objetivo y real; la aplicación de lo aprendido mediante el desarrollo de actividades formativas y sumativas, y, finalmente, la integración de los aprendizajes. El curso tiene una duración total de 30 horas distribuidas en seis semanas, considerando una dedicación semanal de máximo cinco horas. Además, se realizará una sesión sincrónica (opcional) de dos horas, que permitirá a los y las participantes resolver dudas, profundizar en temas de interés y compartir experiencias con los y las demás participantes. **Descripción de las unidades:** **Unidad 1:** Fundamentos Legales y Marco Regulatorio en Ciberseguridad: Esta primera unidad proporcionará a los estudiantes una comprensión fundamental de la legislación chilena relacionada con la ciberseguridad. A través de un enfoque teórico-práctico, los estudiantes explorarán el panorama general de las leyes y regulaciones relevantes en este campo, con un énfasis en dos leyes clave: la Ley N° 19.628 sobre Protección de la Vida Privada y la Ley N° 20.009 sobre Delitos Informáticos. **Unidad 2:** Implementación Práctica y Cumplimiento Normativo en Ciberseguridad: La unidad 2 proporcionará a los participantes los conocimientos y habilidades necesarios para evaluar, mitigar y gestionar los riesgos cibernéticos en el contexto empresarial chileno. A través de un enfoque práctico y basado en casos de estudio, los participantes adquirirán competencias en la identificación de riesgos, desarrollo de estrategias de mitigación, capacitación y

concientización en ciberseguridad, así como en la realización de auditorías de seguridad y cumplimiento normativo.
El análisis y desarrollo de casos será la base para que los aprendizajes, tanto teóricos como prácticos, permitan lograr de forma efectiva el logro de los objetivos, característica propia de este diplomado.

Estrategias evaluativas		
Criterios de evaluación:	**Instrumentos de evaluación:**	**Normas de aprobación:**
Evaluación Diagnóstica		
Describe las políticas y procedimientos internos de la empresa relacionados con la ciberseguridad y sus responsabilidades legales.	La evaluación diagnóstica consiste en la resolución de cinco preguntas con alternativas de respuesta de selección simple. Esta evaluación estará dispuesta en el AVA y se dará retroalimentación automática.	Esta evaluación no tiene ponderación.
Unidad 1		
Reconoce los tipos de delitos informáticos bajo la legislación chilena. Describe las implicancias legales del nuevo marco normativo en el plano empresarial. Identifica la aplicabilidad del marco normativo actual y futuro. Comprende los fundamentos del marco legislativo en ciberseguridad a nivel nacional e internacional.	En esta unidad se evaluará la comprensión de principios de la legislación relacionada con la ciberseguridad a nivel nacional e internacional, a través de un análisis de caso y posterior resolución de preguntas de selección simple. La evaluación será individual y se desarrollará en la plataforma con retroalimentación automática.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 30% de la calificación final del curso.**
Unidad 2		
Analiza estrategias de evaluación de riesgos en casos prácticos. Describe el procedimiento de auditoría legal aplicado al contexto empresarial. Reconoce los aspectos fundamentales de los planes de concientización de una organización y su impacto.	En esta unidad, se evaluará la aplicación de estrategias relacionadas con la ciberseguridad y cumplimiento normativo, a través de un análisis de caso y posterior desarrollo de preguntas. La evaluación será individual y se desarrollará en un formato de entrega, tipo informe, donde cada participante deberá desarrollar una serie de actividades en los espacios destinados para ello. Se utilizará la rúbrica como instrumento de evaluación.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 30% de la calificación final del**

Utiliza estrategias que consideren la evaluación de riesgos y mitigación.		**curso.**
Evaluación Final		
Identifica la situación jurídica actual de la realidad chilena respecto de la ciberseguridad y seguridad de la información. Analiza la evaluación y gestión de riesgos en un contexto aplicado. Identifica los diferentes tipos de delitos informáticos, sus características, consecuencias legales y medidas preventivas asociadas a cada uno de ellos. Describe la aplicabilidad de un correcto plan de concientización dentro de la organización. Aplica políticas y procedimientos que apunten al cumplimiento normativo vigente.	La evaluación final consiste en analizar las políticas y estrategias de ciberseguridad, a través de la revisión de un caso y posterior desarrollo de actividades. La evaluación será individual y se desarrollará en un formato de entrega, tipo informe, donde cada participante deberá desarrollar una serie de actividades en los espacios destinados para ello. Se utilizará la rúbrica como instrumento de evaluación.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 40% de la calificación de fin de curso**.
Requisito de aprobación		
Modalidad sincrónica - asincrónica	Nota mínima de aprobación 4.0	

Recursos para la implementación del curso					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
Características de la infraestructura requerida para la ejecución del curso.	**Dónde se impartirá el curso** ***Anexo ficha de costos**	**Indicar cantidad**	**Tipo de equipo y/o herramienta para la implementación del curso** ***Indicar duración de licencias o equipamientos.**	**Indicar cantidad**	**Indicar el material que se requiere para la implementación del curso**
N/A	N/A	1 P/P	Notebook o computador de escritorio con conexión a internet. Ambiente Virtual de Aprendizaje (AVA) DUOC. Blackboard Ultra. Sistema de videoconferencia online integrado a plataforma.	1 P/P	Programa, recursos educativos y evaluaciones vinculadas a cada unidad. Link o acceso a recursos audiovisuales utilizados en sesiones (en los casos que corresponda), o su URL. Bibliografía digital.

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

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

Diplomado:	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
Diplomado en Ciberseguridad Corporativa	**1. Estrategias de Seguridad de la Información para las TICs**
	2. Cumplimiento, Normativas y Aspectos Legales de Ciberseguridad
	3. Gestión de Proyectos en Ciberseguridad
	4. Estrategias de Gobernanza y gestión de riesgo

Otros cursos relacionados con la temática

Recursos docentes: Perfil desarrollador	
Profesión	Ing. en Telecomunicaciones, Informático o de Redes / Abogado especialista en Ciberseguridad
Años de experiencia	5 años o más.
Conocimientos y habilidades relevantes	Conocimientos en normativa jurídica chilena, Ley Marco de ciberseguridad, Ley 18168, ISO 2700, auditoría informática, Ley 19628. Experiencia en gestión de riesgos, políticas de seguridad, y seguridad en tecnologías emergentes.
Observaciones	

Recursos docentes: Perfil relator	
Profesión	Ing. en Telecomunicaciones, Informático o de Redes / Abogado especialista en Ciberseguridad o carreras afines.
Años de experiencia	3 años o más en el área disciplinar 2 años o más en docencia o relatorías
Conocimientos y habilidades relevantes	Con conocimientos en normativa jurídica chilena, Ley Marco de ciberseguridad, Ley 18168, ISO 2700, auditoría informática, Ley 19628.
Observaciones	

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso:	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
Gestión de Proyectos en Ciberseguridad	50	1	30	Asincrónica

Identificación
Código SENCE
Código curso DuocUC

Unidad académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Escuela de Informática y Telecomunicaciones	Oscar Araya	10/05/2024

Especialista disciplinar	Diseñador(a) curricular	Diseñador(a) instruccional	Analista instruccional
Elisa Molina	Miguel Velasco	Patricia Ojeda	Cristian Domínguez

Aporte de valor del programa (no SENCE)
En la actualidad la ciberseguridad se ha convertido en un componente crítico para la protección de infraestructuras digitales, este curso no solo instruye a los estudiantes en las mejores prácticas y marcos de trabajo para la ciberseguridad, sino que también enfatiza la necesidad de habilidades de liderazgo y gestión de proyectos. Este enfoque dual asegura que no solo comprendan las complejidades técnicas, la asignatura empodera a los estudiantes para que gestionen efectivamente los recursos, tiempos y personal, asegurando la implementación exitosa de las soluciones de seguridad que las organizaciones requieren. Los proyectos de ciberseguridad son fundamentales para proteger los sistemas de información contra amenazas cibernéticas, como el robo y la exfiltración de datos, los malwares y los ataques de ciberdelincuentes como ransomware, entre otros. Al invertir en proyectos de ciberseguridad, las organizaciones pueden salvaguardar la confidencialidad, integridad y disponibilidad de los datos, así como proteger la infraestructura crítica y los activos digitales. Además, el desarrollo de proyectos de ciberseguridad promueve la conciencia y la educación sobre las mejores prácticas de ciberseguridad, tanto a nivel organizacional como individual. Esto contribuye a crear una cultura de seguridad informática, donde los empleados y usuarios están mejor preparados antes estos eventos y desarrollen ciberresiliencia.

Caracterización del participante
Profesionales y técnicos que hayan cursado una carrera, de a lo menos 6 semestres, idealmente del área TI y que realicen labores de TI, como Ingenieros de Proyectos, Ingenieros de Sistemas y/o a líderes o jefes de proyectos que deseen interiorizarse en la gestión de proyectos de ciberseguridad.

Requisitos de ingreso del participante
Los participantes deben contar con conocimientos en tecnologías de la información con una comprensión básica de los principios de gestión de proyectos, junto con habilidades analíticas y una actitud proactiva hacia el aprendizaje continuo.

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

Objetivo general
Aplicar estrategias de gestión de proyectos en ciberseguridad de acuerdo a metodologías existentes

Unidades	Objetivo específico	Contenidos	Horas	
			T	P
Unidad 1: Fundamentos de la Gestión de Proyectos en Ciberseguridad	Aplicar metodologías de gestión de proyectos en contextos de ciberseguridad.	**1. Introducción a la Gestión de Proyectos:** 1.1 Principios y prácticas fundamentales. 1.2 Ciclo de vida de un proyecto. **2. Metodologías de Gestión de Proyectos:** 2.1 Revisión de metodologías tradicionales (PMBOK). 2.2 Metodologías ágiles (Scrum) aplicadas a la ciberseguridad. **3. Planificación de Proyectos:** 3.1 Inicio del proyecto 3.2 Desarrollo del proyecto 3.3 Cierre de proyecto	6	9
Unidad 2: Ejecución y Liderazgo de Proyectos en Ciberseguridad	Analizar proyectos de ciberseguridad de acuerdo a metodologías de gestión existentes.	**1. Liderazgo en la Gestión de Proyectos:** 1.1.Diferentes tipos de liderazgo aplicables con los equipos de trabajo. 1.2 Comunicación efectiva y resolución de conflictos. **2. Técnicas de Ejecución y Monitoreo de Proyecto:** 2.1 Implementación de estrategias y planes de proyecto. 2.2 Técnicas de seguimiento y control. **3. Técnicas de cierre de proyectos:** 3.1 Procesos de cierre y evaluación de proyectos.	5	10

		3.2 Documentación y análisis de lecciones aprendidas para mejorar futuros proyectos.		
		Subtotal	11	19
		Horas totales	30	

Estrategias metodológicas
La estrategia metodológica corresponde a la auto instrucción, considerando el diseño del curso una modalidad 100% online donde el proceso de enseñanza/aprendizaje se desarrollará a través de diversos recursos, los cuales estarán dispuestos de forma ordenada, en el Ambiente Virtual de Aprendizaje establecido por Duoc UC, según el programa formativo con el fin de que los y las participantes adquieran el conocimiento de manera significativa y dinámica. Los recursos educativos como videos interactivos, guías de aprendizaje, infografías, entre otros; se trabajarán de forma contextualizada y representativa de la realidad laboral de los y las participantes, quienes tendrán a disposición el material para su proceso de aprendizaje, tanto en formato audiovisual como en formato descargable. El trabajo académico privilegia la autorregulación, la colaboración, la responsabilidad y el compromiso, entre otras habilidades, para lograr aprendizajes significativos, utilizando, para ello, herramientas digitales que promueven la retroalimentación y la interacción mediante actividades y recursos que tendrán como propósito la activación de conocimientos previos que se vincularán posteriormente con ideas nuevas, la demostración del contenido en un contexto objetivo y real; la aplicación de lo aprendido mediante el desarrollo de actividades formativas y sumativas, y, finalmente, la integración de los aprendizajes. El curso tiene una duración total de 30 horas distribuidas en seis semanas, considerando una dedicación semanal de máximo cinco horas. Además, se realizará una sesión sincrónica (opcional), de dos horas, que permitirá a los y las participantes resolver dudas, profundizar en temas de interés y compartir experiencias con los y las demás participantes. **Descripción de las unidades:** **Unidad 1: Fundamentos de la Gestión de Proyectos en Ciberseguridad:** La primera unidad proporciona a los participantes los conocimientos y habilidades necesarios para comprender y aplicar los principios y prácticas fundamentales de gestión de proyectos en el contexto de la ciberseguridad. A lo largo de la unidad, los estudiantes explorarán el ciclo de vida de un proyecto, revisarán diferentes metodologías de gestión de proyectos, desde enfoques tradicionales hasta metodologías ágiles. **Unidad 2: Ejecución y Liderazgo de Proyectos en Ciberseguridad:** A lo largo de la segunda unidad, los estudiantes explorarán el rol del liderazgo en la gestión de proyectos, aprenderán técnicas para desarrollar equipos efectivos, mejorarán sus habilidades de comunicación y resolución de conflictos, y adquirirán las herramientas necesarias para implementar, monitorear y cerrar proyectos de manera efectiva. El análisis y desarrollo de casos será la base para que los aprendizajes, tanto teóricos como prácticos, permitan lograr de forma efectiva el logro de los objetivos, característica propia de este diplomado.

Estrategias evaluativas		
Criterios de evaluación:	**Instrumentos de evaluación:**	**Normas de aprobación:**
Evaluación Diagnóstica		
Reconoce los fundamentos de la Gestión de Proyectos en Ciberseguridad.	La evaluación diagnóstica consiste en la resolución de cinco preguntas con alternativas de respuesta de selección simple. Esta evaluación estará dispuesta en el AVA y se dará retroalimentación automática.	Esta evaluación no tiene ponderación.
Unidad 1		
Identifica correctamente los principios fundamentales de la gestión de proyectos. Comprende metodologías de gestión de proyectos y su aplicabilidad en ciberseguridad. Aplica principios de gestión de proyectos a escenarios hipotéticos relacionados con ciberseguridad. Selecciona los métodos adecuados para diferentes fases del proyecto.	En esta unidad, se evaluará la aplicación de metodologías relacionadas con la organización de proyectos, a través de un análisis de caso y posterior resolución de preguntas de selección simple. La evaluación será individual y se desarrollará en la plataforma con retroalimentación automática.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 30% de la calificación final del curso.**
Unidad 2		
Aplica conocimientos relacionados con la ejecución y liderazgo efectivo de proyectos de ciberseguridad. Identifica prácticas efectivas de liderazgo y gestión de equipos dentro de un proyecto de ciberseguridad. Analiza el progreso del proyecto de acuerdo a los desafíos presentados. Selecciona las estrategias adecuadas para la ejecución efectiva de proyectos, considerando la asignación de recursos y la gestión del tiempo.	En esta unidad, se evaluará el análisis de proyectos de ciberseguridad, a través de un análisis de caso y posterior desarrollo de informe. La evaluación será individual y se utilizará rúbrica como instrumento de evaluación.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 30% de la calificación final del curso.**

Evaluación Final		
Emplea los principios básicos de la gestión de proyectos y las metodologías específicas para ciberseguridad. Aplica principios y metodologías a situaciones complejas y decisiones críticas dentro de escenarios hipotéticos de ciberseguridad. Identifica las habilidades de liderazgo y la capacidad para gestionar la ejecución efectiva de proyectos de ciberseguridad, incluyendo la resolución de conflictos y la toma de decisiones estratégicas. Comprende el progreso de un proyecto de ciberseguridad. Desarrolla técnicas de seguimiento y evaluación de riesgos en gestión de proyectos.	La evaluación final consiste en desarrollar técnicas y principios de gestión en el marco de la gestión de proyectos de ciberseguridad, a través de un análisis de caso y posterior desarrollo de informe. La evaluación será individual y se utilizará la rúbrica como instrumento de evaluación.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 40% de la calificación de fin de curso**.
Requisito de aprobación		
Modalidad sincrónica - asincrónica	Nota mínima de aprobación 4.0	

Recursos para la implementación del curso					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
Características de la infraestructura requerida para la ejecución del curso.	**Dónde se impartirá el curso** ***Anexo ficha de costos**	**Indicar cantidad**	**Tipo de equipo y/o herramienta para la implementación del curso** ***Indicar duración de licencias o equipamientos.**	**Indicar cantidad**	**Indicar el material que se requiere para la implementación del curso**
N/A	N/A	1 P/P	Notebook o computador de escritorio con conexión a internet. Ambiente Virtual de Aprendizaje (AVA) DUOC.	1 P/P	Programa, recursos educativos y evaluaciones vinculadas a cada unidad. Link o acceso a recursos audiovisuales utilizados en sesiones (en los casos que corresponda), o su URL.

			Blackboard Ultra. Sistema de videoconferencia online integrado a plataforma.		Bibliografía digital.

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

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

Diplomado:	**Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)**
Diplomado en Ciberseguridad Corporativa	**1. Estrategias de Seguridad de la Información para las TICs**
	2. Cumplimiento, Normativas y Aspectos Legales de Ciberseguridad
	3. Gestión de Proyectos en Ciberseguridad
	4. Estrategias de Gobernanza y gestión de riesgo

Otros cursos relacionados con la temática

Recursos docentes: Perfil desarrollador	
Profesión	Ingeniero en Ciberseguridad, Informática o carreras afines.
Años de experiencia	10 años o más.
Conocimientos y habilidades relevantes	Amplia experiencia en el ámbito de la ciberseguridad, habiendo trabajado en la implementación de soluciones de seguridad en diversos entornos tecnológicos. Además, deberá poseer un historial en la gestión de proyectos, con habilidades destacadas en la planificación, ejecución y entrega efectiva de proyectos. Experiencia laboral en roles de ciberseguridad, preferentemente en posiciones de liderazgo como CISO (Chief Information Security Officer), gestor de riesgos TI.
Observaciones	

Recursos docentes: Perfil relator	
Profesión	Ingeniero en Ciberseguridad, Informática o carreras afines.
Años de experiencia	3 años o más en el área disciplinar 2 años o más en docencia o relatorías
Conocimientos y habilidades relevantes	Contar con una sólida trayectoria en ciberseguridad, destacándose en roles técnicos y de liderazgo en la implementación de proyectos de seguridad informática. Además, debe poseer experiencia comprobada en la gestión de proyectos, aplicando diversas metodologías en entornos de TI.
Observaciones	

Ficha Programa No Conducente a Título (PNCT)

Nombre del curso:	Vacantes Educación Continua	Vacantes SENCE	Horas totales	Modalidad factible
Estrategias de Gobernanza y Gestión de Riesgo	50	1	30	Asincrónica

Identificación
Código SENCE
Código curso DuocUC

Unidad académica	Subdirector(a) Unidad Académica	Fecha de elaboración
Escuela de Informática y Telecomunicaciones	Oscar Araya	10/05/2024

Especialista disciplinar	Diseñador(a) curricular	Diseñador(a) instruccional	Analista instruccional
Elisa Molina	Miguel Velasco	Rafael Siverio	Cristian Domínguez

Aporte de valor del programa (no SENCE)
En la actualidad, donde las amenazas digitales evolucionan de manera constante y el entorno normativo se vuelve cada vez más complejo, la necesidad de contar con profesionales altamente capacitados en el ámbito de ciberseguridad es más crítica que nunca. Dentro de este contexto, la asignatura Gobernanza y Gestión de Riesgo, surge como un pilar fundamental para el desarrollo de competencias avanzadas en la gestión de seguridad y la resiliencia organizacional. Este curso es crucial para desarrollar competencias en la creación de políticas de ciberseguridad robustas, manejo de regulaciones y fomento de una cultura preventiva. A través de un enfoque práctico y teórico, prepara a los estudiantes para liderar en la protección efectiva de los sistemas de información en un entorno laboral cada vez más desafiante.

Caracterización del participante
Profesionales y técnicos que hayan cursado una carrera, de a lo menos 6 semestres, idealmente del área TI, como Ingenieros de Sistemas, Analistas de Ciberseguridad, Administradores de Redes, jefes de Riesgo y/o profesionales o técnicos en puestos de toma de decisiones que requieren conocimiento acerca de la gestión de riesgos y gobernanza TI.

Requisitos de ingreso del participante
Base sólida de conceptos TI y una comprensión básica de ciberseguridad, sin ser excluyente. Se requieren habilidades analíticas y críticas para abordar y resolver problemas complejos relacionados con la seguridad de la información.

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

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

Objetivo general
Evaluar estrategias de gobernanza y gestión de riesgos en ciberseguridad de acuerdo a efectividad.

Unidades	**Objetivo específico**	**Contenidos**	**Horas**	
			T	**P**
Unidad 1: Fundamentos de Gobernanza y Gestión de Riesgos	Comprender los principios y marcos de referencia de la gobernanza de TI y la importancia de la gestión de riesgos en el contexto de la Seguridad de la Información.	**1. Fundamentos de Gobernanza:** 1.1 Definición y principios de la gobernanza de TI. 1.2 Roles y responsabilidades clave en la gobernanza de TI. **2. Fundamentos de la Gestión de Riesgos:** 2.1 Identificación, Evaluación y mitigación de riesgos. 2.2 Principales marcos y estándares de gestión de riesgos. 2.3 Relación entre gobernanza TI y gestión de riesgos.	6	9
Unidad 2: Implementación y Operación de la Gobernanza y Gestión de Riesgos	Desarrollar estrategias de gobernanza y gestión de riesgos de la seguridad informática de acuerdo con marcos y estándares de gestión existentes.	**1. Estrategias de Gobernanza:** 1.1 Diseño e implementación de políticas de gobernanza TI. 1.2 Estrategias avanzadas para la evaluación y mitigación de los riesgos. 1.3 Desarrollo de planes de Respuesta y Recuperación ante desastres.	5	10
		Subtotal	11	19
		Horas totales	30	

Estrategias metodológicas
La estrategia metodológica corresponde a la auto instrucción, considerando el diseño del curso que presenta una modalidad 100% online donde el proceso de enseñanza/aprendizaje se desarrollará a través de diversos recursos, los cuales estarán dispuestos de forma ordenada en el Ambiente Virtual de Aprendizaje establecido por Duoc UC, según el programa formativo, con el fin de que los y las participantes adquieran el conocimiento de manera significativa y dinámica. Los recursos educativos como videos interactivos, guías de aprendizaje, infografías, entre otros, se trabajarán de forma contextualizada y representativa de la realidad laboral de los y las participantes, quienes tendrán a disposición el material para su proceso de aprendizaje, tanto en formato audiovisual como en formato descargable.

El trabajo académico privilegia la autorregulación, la colaboración, la responsabilidad y el compromiso, entre otras habilidades, para lograr aprendizajes significativos, utilizando, para ello, herramientas digitales que promueven la retroalimentación y la interacción mediante actividades y recursos que tendrán como propósito la activación de conocimientos previos que se vincularán posteriormente con ideas nuevas, la demostración del contenido en un contexto objetivo y real, la aplicación de lo aprendido mediante el desarrollo de actividades formativas y sumativas y, finalmente, la integración de los aprendizajes.

El curso tiene una duración total de 30 horas distribuidas en seis semanas, considerando una dedicación semanal de Además, se realizará una sesión sincrónica (opcional), de dos horas, que permitirá a los y las participantes resolver dudas, profundizar en temas de interés y compartir experiencias con los y las demás participantes.

Descripción de las unidades:

Unidad 1: Fundamentos de Gobernanza y Gestión de Riesgos: en esta unidad, se revisarán los fundamentos esenciales de la gobernanza de Tecnologías de la Información (TI) y la Gestión de Riesgos, dos áreas críticas para el éxito y la seguridad de las organizaciones en la era digital. Se iniciará analizando en detalle la gobernanza de TI, comprendiendo su definición, principios claves y la importancia de su implementación en el contexto empresarial. Además, se explorarán los roles y responsabilidades fundamentales dentro de la gobernanza de TI, identificando cómo cada uno contribuye al cumplimiento de los objetivos estratégicos y las técnicas fundamentales para la identificación, evaluación y mitigación de los riesgos de seguridad de la información. Se utilizará el estudio de casos como estrategia metodológica.

Unidad 2: Implementación y Operación de la Gobernanza y Gestión de Riesgos: en esta segunda unidad, se revisarán las estrategias avanzadas de gobernanza y gestión de riesgos en Tecnologías de la Información (TI), fundamentales para garantizar la seguridad, eficiencia y continuidad operativa en las organizaciones modernas.
Se comenzará analizando el diseño e implementación de políticas de gobernanza TI, comprendiendo su importancia en la definición de roles, responsabilidades y procesos que guían el uso adecuado y responsable de la tecnología en la organización. Explorarán cómo desarrollar políticas efectivas que aborden aspectos claves como la seguridad de la información, el cumplimiento normativo y la gestión de recursos tecnológicos, garantizando la continuidad operativa y la resiliencia organizacional.

El análisis y desarrollo de casos será la base para que los aprendizajes, tanto teóricos como prácticos, permitan lograr de forma efectiva el logro de los objetivos, característica propia de este diplomado.

Estrategias evaluativas		
Criterios de evaluación:	**Instrumentos de evaluación:**	**Normas de aprobación:**
Evaluación Diagnóstica		
Reconoce los principios fundamentales de la Gobernanza y la Gestión de Riesgo.	La evaluación diagnóstica consiste en la resolución de cinco preguntas con alternativas de respuesta de selección simple. Esta evaluación estará dispuesta en el AVA y se dará retroalimentación automática.	Esta evaluación no tiene ponderación.
Unidad 1		
Identifica los principios claves de la gobernanza TI y la Gestión de Riesgos presentados en el caso.	En esta unidad, se evaluará la comprensión de los estudiantes sobre los conceptos básicos de la gobernanza de TI y la gestión de riesgos, a través de un análisis de caso y	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0

Comprende la importancia de la gestión de riesgos en la seguridad de la información y sus implicaciones en las organizaciones. Relaciona los principios de la gobernanza de TI con su aplicación práctica en la toma de decisiones organizacionales. Comprende cómo los principios de gobernanza y gestión de riesgos se aplican en el contexto del caso.	posterior resolución de preguntas de selección simple. La evaluación será individual y se desarrollará en la plataforma con retroalimentación automática.	el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 30% de la calificación final del curso.**
Unidad 2		
Utiliza métodos y técnicas adecuadas para diseñar e implementar un plan de gobernanza en un escenario organizacional. Aplica los conocimientos teóricos adecuados como insumo en la creación de un plan operativo realista y fundamentado. Propone un plan efectivo de respuesta y recuperación ante desastres. Propone un plan efectivo de gobernanza o gestión de riesgos, incluyendo objetivos claros y estrategias efectivas. Justifica la viabilidad y sostenibilidad del plan propuesto.	En esta unidad, se evaluará la habilidad de los estudiantes para aplicar teorías y técnicas aprendidas en la implementación práctica de un plan de gobernanza o gestión de riesgo, a través de un análisis de caso y posterior desarrollo de preguntas. La evaluación será individual y se desarrollará en un formato de entrega, tipo informe, donde cada participante deberá desarrollar una serie de actividades en los espacios destinados para ello. Se utilizará una rúbrica como instrumento de evaluación.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 30% de la calificación final del curso.**
Evaluación Final		
Identifica claramente las problemáticas principales del caso. Comprende conceptos técnicos como normativas legales, tecnología de la información y estrategias corporativas. Aplica los conceptos de gobernanza TI y gestión de riesgos, con el fin de analizar las situaciones presentadas.	Al final del curso se evaluará el desarrollo de estrategias efectivas de gobernanza y gestión de riesgos en ciberseguridad. La evaluación final consiste en un análisis de caso y posterior desarrollo de preguntas. La evaluación será individual y se desarrollará en un formato de entrega, tipo informe, donde cada participante deberá desarrollar una serie de actividades en los espacios destinados para ello. Se utilizará la rúbrica como instrumento de evaluación.	Las calificaciones derivadas de las evaluaciones sumativas del curso estarán expresadas con notas entre 1,0 y 7,0, siendo 4,0 el mínimo requerido para la aprobación del curso. Se corregirán los productos presentados aplicando un 60% de exigencia. **Esta evaluación representa el 40% de la calificación de fin de curso**.

Evalúa la relevancia y las estrategias para abordar los problemas identificados. Desarrolla estrategias de manera clara y ordenada, factibles y viables de llevar a cabo. Demuestra lógica coherente en la secuencia y desarrollo de las estrategias propuestas.		

Requisito de aprobación	
Modalidad sincrónica - asincrónica	Nota mínima de aprobación 4.0

Recursos para la implementación del curso					
Infraestructura	**Indicar sede**	**Equipos y herramientas**		**Material didáctico**	
Características de la infraestructura requerida para la ejecución del curso.	**Dónde se impartirá el curso** ***Anexo ficha de costos**	**Indicar cantidad**	**Tipo de equipo y/o herramienta para la implementación del curso** ***Indicar duración de licencias o equipamientos.**	**Indicar cantidad**	**Indicar el material que se requiere para la implementación del curso**
N/A	N/A	1 P/P	Notebook o computador de escritorio con conexión a internet. Ambiente Virtual de Aprendizaje (AVA) DUOC. Blackboard Ultra. Sistema de videoconferencia online integrado a plataforma.	1 P/P	Programa, recursos educativos y evaluaciones vinculadas a cada unidad. Link o acceso a recursos audiovisuales utilizados en sesiones (en los casos que corresponda), o su URL. Bibliografía digital.

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

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

Diplomado:	Cursos conducentes al diplomado o certificación (identificar cursos base y optativos)
Diplomado en Ciberseguridad Corporativa	**1. Estrategias de Seguridad de la Información para las TICs**
	2. Cumplimiento, Normativas y Aspectos Legales de Ciberseguridad
	3. Gestión de Proyectos en Ciberseguridad
	4. Estrategias de Gobernanza y gestión de riesgo

Otros cursos relacionados con la temática

Recursos docentes: Perfil desarrollador	
Profesión	Ingeniero o Magister en Ciberseguridad
Años de experiencia	10 años o más.
Conocimientos y habilidades relevantes	Experiencia laboral en roles de ciberseguridad, preferentemente en posiciones de liderazgo como CISO (Chief Information Security Officer), gestor de riesgos TI. Experiencia comprobable en diseño y ejecución de estrategias de seguridad y gobernanza de TI en organizaciones.
Observaciones	

Recursos docentes: Perfil relator	
Profesión	Ingeniero en Informática, Telecomunicaciones o carreras afines.
Años de experiencia	3 años o más en el área disciplinar 2 años o más en docencia o relatorías
Conocimientos y habilidades relevantes	Excelentes habilidades para comunicar conceptos complejos de manera clara y comprensible para distintos públicos. Motivación por la enseñanza y la ciberseguridad, con el fin de inspirar e incentivar a los estudiantes. Habilidad para fomentar el pensamiento crítico y la resolución de problemas, guiando a los estudiantes a través de desafíos reales y simulaciones.
Observaciones	