Latam IT Academy
Latin American IT Academy

Curso Ciberseguridad: Fundamentos Transversales

Duración: 60 horas.
Modalidad: Sincrónica.

Súmate a los nuevos empleos

SCI CERTIFICACIONES NCH 2728 Gestión OTEC

Público Objetivo:

Este curso está diseñado para **personas sin experiencia previa o conocimientos técnicos profundos en informática o tecnología de la información (TI)**. Incluye a profesionales de diversas áreas, estudiantes no técnicos, y cualquier individuo interesado en comprender los **conceptos básicos y la importancia de la ciberseguridad en su vida digital personal y profesional**. El curso se enfoca en el **conocimiento transversal** que permite a cualquier persona abordar los riesgos de seguridad en el mundo digital actual.

Objetivos Generales de Aprendizaje:

1. **Comprender la relevancia de la ciberseguridad** en el entorno digital actual y su impacto en la vida cotidiana y las organizaciones.
2. **Identificar las amenazas y riesgos comunes** en el ciberespacio, utilizando un lenguaje accesible y evitando tecnicismos innecesarios.
3. **Conocer las principales partes interesadas** en el ciberespacio y sus roles en la seguridad de la información.
4. **Familiarizarse con las prácticas y directrices esenciales** para proteger la información personal y organizacional en línea.
5. **Desarrollar una conciencia fundamental sobre la importancia de la privacidad de los datos** y las libertades civiles en el entorno digital

Metodología:

Aspectos motivacionales: Al inicio de la actividad el alumno cuenta con una evaluación inicial, lo que permitirá medir los conocimientos prácticos y conceptuales del participante y así, al final del curso poder medir brechas iniciales, resueltas por medio de la capacitación, mediante la comparación de los resultados. Los tipos de evaluación que se utilizarán son tres:

1. Evaluaciones de reforzamiento y estudios de casos estas no son ponderadas, aunque todas las evaluaciones constan de retroalimentaciones por parte del tutor, estas actividades sirven para afianzar el contenido de cada módulo.

2. Evaluaciones sumativas correspondientes a cada módulo, las que miden conocimientos técnicos correspondientes a las unidades respectivas. Estas evaluaciones están diseñadas como pequeños estudios de caso en los cuales el participante es llevado a una situación hipotética y debe tomar las decisiones correctas según el contenido de cada uno de los módulos.

3- control final, el cual corresponde a la evaluación automatizada efectuada por el participante al finalizar las actividades de cada módulo, donde mide los conocimientos completos del curso. Los criterios de evaluación buscan medir los conocimientos conceptuales y prácticos de cada módulo, los cuales tienen como finalidad mejorar las habilidades de cada participante, que se verán reflejadas en el puesto de trabajo, este primer criterio será de forma cualitativa en base a respuestas y opciones seleccionadas por el alumno, las cuales se medirán por medio de la escala LIKET.

Por otra parte, el criterio cuantitativo será la evaluación del 1 al 7, correspondiendo a las normas de evaluación la nota mínima de aprobación a la calificación 4, equivalente a un 75% de las respuestas correctas en cada control.

Contenidos:

MÓDULO 1:

Introducción al Ciberespacio y la Ciberseguridad: Un Mundo Conectado

OBJETIVOS ESPECÍFICOS:

- Definir el concepto de **ciberespacio** como el entorno resultante de la interacción de personas, software y servicios en Internet.
- Explicar la **importancia de la ciberseguridad** para gestionar los riesgos de seguridad de la información digital.
- Establecer la relación entre **Seguridad en Internet**, **Seguridad en la Web**, **Seguridad de Red** y la **Ciberseguridad**, mostrando cómo se interconectan.
- Identificar las **principales partes interesadas** en el ciberespacio, incluyendo usuarios, coordinadores y organizaciones de estandarización, autoridades gubernamentales, organismos encargados de hacer cumplir la ley y proveedores de servicios de Internet.

APRENDIZAJES ESPERADOS:

- Serán capaces de **describir qué es el ciberespacio** en términos sencillos.
- Comprenderán por qué la **ciberseguridad es fundamental** en la actualidad.
- Podrán **distinguir las áreas básicas de la seguridad digital** (Internet, web, redes) y su conexión con la ciberseguridad.
- Identificarán los **diferentes actores clave** que participan en la seguridad del entorno digital.

MÓDULO 2:

Amenazas y Riesgos Comunes en Internet Relación entre Dominios de Seguridad

OBJETIVOS ESPECÍFICOS:

- Identificar **amenazas comunes** en Internet, como el **malware** (virus, gusanos, troyanos) y sus posibles consecuencias.
- Explicar el concepto de **vulnerabilidades** como debilidades en los sistemas que pueden ser explotadas.
- Reconocer **vectores de ataque** comunes, como el phishing, el spam, los sitios web maliciosos y las descargas no verificadas.
- Comprender los **riesgos asociados con el robo de identidad** y la información personal (IIP) en línea.

APRENDIZAJES ESPERADOS:

- Serán capaces de **nombrar y describir los tipos básicos de malware** y su forma de propagación.
- Entenderán qué significa una **vulnerabilidad** en un sistema informático.
- Podrán **reconocer las formas en que los atacantes intentan acceder a la información** (vectores de ataque).
- Comprenderán los **peligros del robo de identidad** y la exposición de información personal en Internet.

MÓDULO 3:
Directrices Esenciales para la Seguridad en Internet: Prácticas Clave para Usuarios

OBJETIVOS ESPECÍFICOS:

- Conocer las **estrategias generales** para mejorar la seguridad en Internet.
- Comprender la importancia de tener **políticas de seguridad en Internet** (a nivel conceptual).
- Reconocer la necesidad del **control de acceso** básico mediante la autenticación y autorización.
- Valorar la importancia de la **educación, concientización y entrenamiento** para reconocer amenazas.
- Entender la necesidad básica de la **gestión de incidentes de seguridad** y qué pasos seguir ante un problema.
- Comprender la importancia de la **protección de la privacidad** de la información personal en línea.
- Familiarizarse con el concepto de **protección antimalware** como el uso de software para detectar amenazas.
- Reconocer la importancia de **identificar la legislación y requisitos de cumplimiento** relevantes (a nivel de conocimiento general).

APRENDIZAJES ESPERADOS:

- Conocerán **principios básicos para navegar por Internet de forma más segura**.
- Entenderán por qué es importante tener **reglas para el uso de Internet**.
- Comprenderán la necesidad de **proteger el acceso a sus cuentas e información**.
- Serán más conscientes de las **amenazas comunes** y cómo evitarlas.
- Tendrán una idea general de **qué hacer si experimentan un problema de seguridad**.
- Entenderán la **importancia de cuidar su información personal** en línea.
- Conocerán la utilidad de los **programas antivirus**.
- Comprenderán que existen **leyes relacionadas con la seguridad en Internet**.

MÓDULO 4:

Todos Somos Parte de la Ciberseguridad: Roles y Colaboración en el Mundo Digital

OBJETIVOS ESPECÍFICOS:

- Comprender las **responsabilidades de los usuarios** en la seguridad de Internet.
- Reconocer la importancia de la **coordinación y estandarización** a través de organizaciones como ICANN, IETF y W3C.
- Entender el papel de las **autoridades gubernamentales** en la protección de la infraestructura e información y en la coordinación ante incidentes.
- Comprender la función de los **proveedores de servicios de Internet (ISP)** en la prestación de acceso y la posible monitorización de amenazas.
- Valorar la necesidad de la **colaboración internacional y multisectorial** para abordar los desafíos globales de la ciberseguridad.

APRENDIZAJES ESPERADOS:

- Serán conscientes de que **sus acciones en línea afectan la seguridad general**.
- Entenderán que existen **organizaciones que trabajan para establecer normas en Internet**.
- Comprenderán que **los gobiernos tienen un papel importante en la ciberseguridad**.
- Conocerán la **función de las empresas que les dan acceso a Internet**.
- Valorarán la **importancia de trabajar juntos** a nivel mundial para enfrentar los riesgos cibernéticos.


Latam IT
Academ
Latin American IT Academy