EDUCACIÓN CONTINUA

Obtén la certificación de habilidades profesionales

Introducción a la Ciberseguridad

¿En qué consiste?

validar tus competencias fundamentales de forma rápida y directa, rindiendo un único examen sin necesidad de cursar una formación previa. Esta modalidad está diseñada para ti, que tienes conocimientos básicos en tecnología y deseas demostrar habilidades esenciales en identificación de amenazas, evaluación de riesgos y aplicación de medidas de seguridad en entornos digitales.

Objetivo de la certificación:

Con esta certificación, demostrarás que sabes identificar vulnerabilidades en sistemas informáticos, aplicar controles de acceso, utilizar principios básicos de criptografía, gestionar identidades digitales y diseñar estrategias de seguridad para redes, servidores y dispositivos móviles.

Público Objetivo:

Estudiantes y profesionales del rubro tecnológico, administrativos y operativos que desean certificar habilidades introductorias en ciberseguridad y mejorar su perfil profesional en entornos donde la protección de la información es clave.

Competencias que te certifican:

- Identificación de amenazas y vulnerabilidades en sistemas y redes.
- Evaluación de riesgos y planificación de estrategias de mitigación.
- Aplicación de controles de acceso y autenticación segura.
- Uso de criptografía para proteger información sensible.
- Seguridad en redes, servidores, dispositivos móviles y entornos cloud.

Metodología de evaluación

Rendirás un examen compuesto por 40 preguntas seleccionadas aleatoriamente, cada una con una única respuesta correcta y un valor de 0.5 puntos. La evaluación tendrá una duración de 1 hora, será en un solo intento, y deberás alcanzar una nota mínima de 13 para aprobar.

La prueba combinará diferentes tipos de desafíos para evaluar tus conocimientos de forma integral:

Preguntas objetivas
Opción Múltiple en respuesta directa, completar texto, verdadero/falso.

Análisis de casos y gráficos
Aplicación de conocimientos a escenarios prácticos.

Ejercicios prácticos
Corrección técnica, tareas instruidas y resolución de casos operativos

Requisitos

Para rendir el examen necesitarás:

- DNI a la mano
- Cámara y micrófono encendidos
- Acceso a internet
- Laptop o PC para rendir el examen

Temario de evaluación

Evaluación equivalente a
32 horas sincrónicas de estudio | **20** Preguntas aleatorias

Tema 1
Fundamentos de Seguridad IT
Reconocer conceptos clave de ciberseguridad, amenazas actuales, marcos normativos y políticas d seguridad.

- Entendiendo la Seguridad
- Responsabilidades
- Construyendo un Programa de Seguridad
- Auditoria de la CIA
- Evaluando el Cumplimiento de Riesgo
- Estado de la Seguridad Actual

Tema 2
Gestión de Riesgos
Aplicar metodologías para identificar, evaluar y mitigar riesgos, y responder ante incidentes.

- Gestión de Riesgos - Fundamentos
- Evaluación de Riesgos
- Tipos de Riesgo, Amenazas y Vulnerabilidades
- Mitigación de Riesgos
- Descubriendo Vulnerabilidades y Amenazas
- Respondiendo a Riesgos

Tema 3
Criptografía Básica
Utilizar técnicas de cifrado, hashing y gestión de certificados digitales para proteger datos.

- Entendiendo la Criptografía
- Cifrado Simétrico
- Cifrado Asimétrico
- Hashing
- PKI (Infraestructura de Clave Pública)
- Criptografía en Uso

Tema 4
Gestión de Identidades y Accesos
Controlar accesos mediante autenticación, gestión de sesiones y monitoreo de actividades.

- Gestión de Identidad
- Técnicas de Autenticación
- Sign-On y Session Management
- Sign-On y Session Management

Tema 5
Seguridad de Datos
Clasificar información, aplicar cifrado y cumplir con normativas de protección de datos.

- Defendiendo Datos en Reposo
- Opciones de Cifrado
- Gestión de Datos

Tema 6
Seguridad en Redes
Implementar medidas de protección en redes alámbricas e inalámbricas, firewalls y segmentación.

- Protocolos y Servicios
- Dispositivos de Red y Seguridad
- Diseño de Red
- Redes Inalámbricas

Tema 7
Gestión de Seguridad de Servidores y Hosts
Configurar y endurecer sistemas operativos, garantizar seguridad física y aplicar buenas prácticas en cloud.

- Sistemas Operativos Inalámbricos
- Endurecimiento del Sistema Operativo
- Seguridad Física
- Virtualización y Tecnologías Cloud

Tema 8
Dispositivos Móviles y Seguridad Web
Identificar amenazas móviles, aplicar políticas de BYOD y proteger aplicaciones móviles y APIs.

- ¿Qué Dispositivos Móviles Están en Riesgo?
- ¿Cuál es el Riesgo?
- Endurecimiento de Dispositivos Móviles
- Introducción a la Gestión de Aplicaciones Web

Beneficios

1. Certificate tus competencias enIntroducción a la Ciberseguridad en 1 hora y media
2. Obtén equivalencia académica a 32 horas de formación que se incluirá en tu certificado.
3. Mejora tu empleabilidad con una certificación reconocida.

Con el respaldo de intercorp