



LEAD CYBERSECURITY

PROFESSIONAL CERTIFICATION



LCSPC™ Versión 062024

Lead Cybersecurity Professional Certification LCSPC

Syllabus V062024

Introducción	3
Objetivos de aprendizaje	3
Requisitos Previos	4
Formación	4
Elegibilidad para certificación	4
Contenido	5

Introducción

CertiProf® ofrece la certificación profesional en Ciberseguridad, Lead Cybersecurity Professional Certification LCSPC, donde aprenderás la importancia de la ciberseguridad en el entorno digital actual. El contenido del material abarca desde los fundamentos del ciberespacio y la ciberseguridad, hasta la relación entre diferentes dominios de seguridad como la seguridad en Internet, la seguridad web y la seguridad de la red. Se profundiza en la gestión de riesgos en Internet, incluyendo amenazas como virus, gusanos y troyanos, así como vectores de ataque y vulnerabilidades. También se discuten los roles y responsabilidades de diversas partes interesadas en el ciberespacio, como usuarios, coordinadores, autoridades gubernamentales y proveedores de servicios de Internet, y se enfatiza la importancia de una colaboración internacional y multisectorial para abordar estos desafíos.

El material también ofrece directrices específicas para la implementación de controles de seguridad basados en normas ISO, incluyendo políticas de seguridad en Internet, control de acceso, educación y concientización, gestión de incidentes y gestión de activos. Estas directrices están diseñadas para ayudar a las organizaciones a mitigar riesgos y proteger sus activos digitales mediante estrategias de seguridad efectivas y actualizadas.

Objetivos de aprendizaje

1. Conceptos Fundamentales de Ciberseguridad

- Comprender los principios básicos de la ciberseguridad y su importancia en la protección de la información.
- Estudiar las amenazas comunes y las mejores prácticas para mitigarlas.

2. ISO / IEC 27032

- Familiarizarse con las directrices internacionales para la seguridad en internet, detalladas en la norma ISO/IEC 27032.
- Aprender a aplicar estas directrices en entornos empresariales y organizacionales.

3. Introducción al Marco de Ciberseguridad

- Conocer el marco de ciberseguridad y sus componentes esenciales.
- Evaluar y aplicar el marco para fortalecer la postura de ciberseguridad de una organización.

4. Gestión de Riesgos y el Marco de Ciberseguridad

- Identificar, evaluar y gestionar riesgos de ciberseguridad dentro del marco establecido.
- Desarrollar habilidades para implementar estrategias efectivas de gestión de riesgos.

5. Implementación del Marco de Ciberseguridad

- Adquirir conocimientos prácticos sobre cómo implementar el marco de ciberseguridad en una organización.
- Mejorar la infraestructura de ciberseguridad mediante la adopción de medidas basadas en el marco.

6. Establecer o Mejorar la Ciberseguridad Comunicativa

- Desarrollar estrategias de comunicación eficaces para informar sobre riesgos y medidas de ciberseguridad a las partes interesadas.
- Fomentar una cultura de ciberseguridad dentro de la organización.

7. Metodología para Proteger la Privacidad y las Libertades Civiles

- Aplicar metodologías específicas para salvaguardar la privacidad y las libertades civiles en el entorno digital.
- Asegurar el cumplimiento de las regulaciones y normas de privacidad.

8. Autoevaluación de Riesgos de Ciberseguridad con el Marco

- Realizar autoevaluaciones periódicas de los riesgos de ciberseguridad utilizando el marco.
- Identificar áreas de mejora y desarrollar planes de acción para mitigar riesgos.

Requisitos Previos

- No hay requisitos previos formales para esta certificación.

Formación

- Tipo de curso: Profesional
- Código de certificación: LCSPC™
- Vencimiento: 3 años

Elegibilidad para certificación

- Conocer la importancia de la Ciberseguridad y aprender cómo evitar todo tipo de amenazas que pongan en riesgo la información que está siendo procesada, transportada o almacenada en cualquier dispositivo.

Contenido

Fundamentos del Ciberespacio y la Ciberseguridad

Explicación básica del ciberespacio y los principios de la ciberseguridad.

Relaciones entre la Seguridad en Internet, Seguridad en la Web, Seguridad de Red y la Ciberseguridad

Descripción de cómo se interrelacionan estos dominios de seguridad.

Visión General de la Seguridad en Internet

Partes Interesadas (Roles)

Coordinación y Estandarización

Autoridades de Gobierno

Leyes y agencias de regulación

Proveedores de Servicio de Internet

Evaluación y Tratamiento de los Riesgos para la Seguridad en Internet

Amenazas

Identificación de posibles amenazas a la seguridad en Internet.

Vulnerabilidades

Análisis de puntos débiles que pueden ser explotados.

Vectores de Ataque

Métodos y rutas a través de los cuales pueden realizarse los ataques.

Cybersecurity – Guidelines for Internet Security ISO 27032:2023

Descripción de las directrices de la ISO 27032 para la seguridad en Internet.

Directrices de Seguridad para Internet

Generalidades (Estrategias)

Estrategias generales para implementar la seguridad en Internet.

Controles de Seguridad en Internet

Políticas de Seguridad en Internet

Control de Acceso

Educación, Concientización y Entrenamiento

Gestión de Incidentes de Seguridad

Gestión de Activos

Gestión de Proveedores

Continuidad del Negocio en Internet

Protección de la Privacidad

Gestión de Vulnerabilidades

Gestión de Redes

Control de Cambios

Protección Antimalware

Identificación de Legislación y Requisitos de Cumplimiento Aplicables

Uso de Criptografía

Seguridad de las Aplicaciones Orientadas a Internet

Gestión de Dispositivos de Usuario Final

Control de Acceso

Gestión de Incidentes

Gestión de Proveedores

Referencias Cruzadas entre ISO 27032 e ISO 27002

Comparación y alineación de controles entre ambas normas.

Evaluación y Tratamiento de los Riesgos para la Seguridad en Internet ISO 27032

Detalles sobre la gestión de riesgos específicos según las directrices de la ISO 27032.