
## Objetivo:

Esta certificación busca acreditar los conocimientos en la gestión de la ciberseguridad, así como la identificación adecuada de medidas ante las amenazas, vulnerabilidades y riesgos que con respecto a la ciberseguridad están expuestas las organizaciones.

## Grupo Objetivo:

Cualquier persona cuyo rol asuma responsabilidades de la gestión de la seguridad informática, entre ellos: Administrador de red, Desarrollador de aplicaciones, Oficial de seguridad, Auditor de Seguridad, Gerente de Calidad, Gerente de Operaciones.

## Detalles de la Certificación:

| | |
|---|---|
| • Duración: | 60 minutos. |
| • Cantidad de Preguntas: | 30 (Opción múltiple). |
| • Mínimo aprobatorio: | 65%. |
| • Libro abierto: | No. |
| • Equipo electrónico permitido: | No. |
| • Nivel: | Intermedio. |
| • Idiomas disponibles: | Inglés, Español. |
| • Requisitos: | No. |
| • Tipos de Supervisión disponible: | Live Proctoring, Belive Proctoring. |
| • Segunda oportunidad (gratuita): | Sí. |
| • Mínimo aprobatorio Segunda oportunidad: | 75%. |

# Temario:

### Explorando la ISO 27032:

- Estructura de la norma.
- Naturaleza de la ciberseguridad.
- Partes interesadas en el ciberespacio.
- Activos en el ciberespacio.
- Alcance y enfoque de ciberseguridad.

### Redes TCP/IP:

- Conexiones de nodo y direccionamiento TCP / IP.
- Modelo OSI, Modelo TCP/IP, Protocolos.

### Sistemas de Computación:

- Arquitectura de computadores, sistemas operativos.
- Vulnerabilidades de los sistemas de computación.
- Medidas de seguridad de los sistemas de computación.

### Base de datos y aplicaciones:

- Desarrollo de aplicaciones.
- Bases de datos.
- Problemas de seguridad y contramedidas.

### Criptografía:

- Metodologías y estándares de encriptación.
- Firmas digitales, “Hashing”.
- Infraestructura de clave pública (PKI).
- SSL/TLS, IPSec.

### Gestión de Identidad y Acceso:

- Identificación, autenticación, biometría, inicio de sesión único (SSO), gestión de contraseñas.
- Autorización.

### “Cloud Computing”:

- Características y modelos de despliegue.
- Riesgos.

### Explotando vulnerabilidades:

- Categorías de ataque y tipos de amenazas.
- Herramientas y roles frecuentes.