Certified in Cybersecurity Certification (CC)

Código: ISC2-001

Propuesta de Valor: ISC2

Duración: 14 Horas

A medida que las amenazas cibernéticas continúan interrumpiendo los negocios a diario, la necesidad de expertos en seguridad está en su punto más alto. Sin embargo, el talento es escaso. La investigación muestra que la fuerza laboral de seguridad cibernética necesita crecer en un 65 por ciento para satisfacer la demanda global. La nueva Certificación de ciberseguridad de nivel de entrada ayuda a organizaciones como la suya a llenar ese vacío y construir una línea de defensa más sólida.

(ISC)2 lanzó esta nueva certificación de experiencia cero para permitir que los candidatos, incluidos estudiantes, posibles empleados, profesionales principiantes y personas que cambian de carrera, comiencen su camino hacia el liderazgo en seguridad cibernética con los conceptos fundamentales clave en seguridad de la información, determinados por expertos cibernéticos. y profesionales que trabajan en el campo.

Más información: AQUÍ

Reserve su plaza: AQUÍ

AUDIENCIA

Estudiantes, posibles empleados, profesionales de nivel inicial y cambios de carrera que deseen iniciar su camino hacia el liderazgo en ciberseguridad realizando el examen de ciberseguridad de nivel inicial de (ISC)². Roles de trabajo de ciberseguridad de nivel de entrada:

- Analista de seguridad
- Analista de Controles Industriales
- Analista de Riesgos
- Respondedor de incidentes
- Especialista/analista forense
- Ingeniero de seguridad

PRE REQUISITOS

- No hay requisitos previos específicos. Se recomienda que los candidatos tengan conocimientos básicos de tecnología de la información (TI).
- No se requiere experiencia laboral en seguridad cibernética.

OBJETIVOS

- Evaluar las opciones de gestión de riesgos y el uso de controles de acceso para proteger los activos.
- Examinar el campo de la criptografía para asegurar la información y la comunicación.
- Cree una postura de seguridad asegurando el software, los datos y los terminales.
- Aplicar seguridad de redes y comunicaciones para establecer un entorno de red seguro.
- Evaluar la seguridad inalámbrica y en la nube.
- Prepárese para la detección y respuesta de incidentes.
- Implementar medidas adecuadas que contribuyan a la maduración de la gestión de riesgos.

CERTIFICACIÓN DISPONIBLE

- Este curso lo prepara para el examen: **Certified in Cybersecurity Certification**.
- Puntuación de 70% o más en la evaluación final.
- Certificación oficial de **ISC2**.

CONTENIDO

1. PRINCIPIOS DE SEGURIDAD

1.1. COMPRENDER LOS CONCEPTOS DE SEGURIDAD DEL ASEGURAMIENTO DE LA INFORMACIÓN
1.2. COMPRENDER LOS CONCEPTOS DE GESTIÓN DE RIESGOS
1.3. COMPRENDER LOS CONTROLES DE SEGURIDAD
1.4. COMPRENDER LOS PROCESOS DE GOBERNANZA
1.5. ENTENDER (ISC)² CÓDIGO DE ÉTICA

2. CONCEPTOS DE CONTINUIDAD DEL NEGOCIO (BC), RECUPERACIÓN DE DESASTRES (DR) Y RESPUESTA A INCIDENTES

2.1. COMPRENDER LA RESPUESTA A INCIDENTES
2.2. COMPRENDER LA CONTINUIDAD DEL NEGOCIO (BC)
2.3. COMPRENDER LA RECUPERACIÓN ANTE DESASTRES (DR)

3. CONCEPTOS DE CONTROLES DE ACCESO

3.1. COMPRENDER LOS CONCEPTOS DE CONTROL DE ACCESO
3.2. COMPRENDER LOS CONTROLES DE ACCESO FÍSICO
3.3. COMPRENDER LOS CONTROLES DE ACCESO LÓGICO

4. SEGURIDAD DE LA RED

4.1. COMPRENDER LAS REDES INFORMÁTICAS
4.2. COMPRENDER LAS AMENAZAS Y LOS ATAQUES A LA RED
4.3. COMPRENDER LA INFRAESTRUCTURA DE SEGURIDAD DE LA RED

5. OPERACIONES DE SEGURIDAD

5.1. COMPRENDER LA SEGURIDAD DE LOS DATOS

5.3. COMPRENDER LAS POLÍTICAS DE SEGURIDAD DE MEJORES PRÁCTICAS

5.4. COMPRENDER LA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE SEGURIDAD

BENEFICIOS

- Al finalizar el curso, los participantes podrán brindar mayor confianza en las estrategias y prácticas de seguridad.