Temario CertiProf.

Certificación Internacional

Cybersecurity Awareness Professional Certification - CAPC™



Esta certificación te brindará los conocimientos esenciales de ciberseguridad para proteger su información personal y profesional, a la vez que fomenta una cultura de seguridad en el entorno laboral.

Información del programa.

Objetivos del programa.

- Identificarás amenazas comunes como virus, ransomware, phishing, smishing y otros tipos de ingeniería social.
- Aprenderás prácticas esenciales para proteger la seguridad de contraseñas, cuentas y dispositivos personales.
- Entenderás los conceptos fundamentales de ciberseguridad y su relevancia.
- Comprenderás los requisitos legales, informes y documentación, y su importancia en la protección de información sensible.

Perfil del participante.

- Administradores de redes, administradores de sistemas y personal de soporte de TI que necesiten mejorar sus conocimientos.
- Altos directivos, gestores de proyectos y jefes responsables de supervisar las políticas y estrategias de ciberseguridad.
- Profesionales encargados de garantizar que sus organizaciones cumplen las normas y las mejores prácticas de ciberseguridad.
- Personas que deseen entrar en el campo de la ciberseguridad o mejorar sus conocimientos.

Para mayor información contactar:

+503 7840-2073 info@inmersiongroup.com

Immersion
International Business School

Módulo 1: Introducción a la ciberseguridad.

1.1 Bienvenida y objetivos del curso.

- Presentación del instructor.
- Objetivos y expectativas del curso.

1.2 Conceptos básicos de ciberseguridad.

- ¿Qué es la ciberseguridad?
- Importancia de la ciberseguridad en el entorno actual.
- Diferencias entre ciberseguridad y seguridad de la información.

1.3 Principios de ciberseguridad.

- Confidencialidad, integridad y disponibilidad (CIA).
- Principios de defensa en profundidad.
- Buenas prácticas en seguridad de la información.

Módulo 2: Amenazas y vulnerabilidades comunes.

2.1 Tipos de amenazas.

- Malware: virus, gusanos, troyanos, ransomware.
- Phishing y ataques de ingeniería social.
- Ataques de denegación de servicio (DoS y DDoS).

2.2 Vulnerabilidades comunes.

- Vulnerabilidades de software y hardware.
- Problemas de configuración.
- Errores humanos y su impacto en la seguridad.

Módulo 3: Medidas de protección y buenas prácticas.

3.1 Protección de dispositivos y redes.

- Uso de antivirus y software de seguridad.
- Configuración segura de redes Wi-Fi.
- Importancia de las actualizaciones y los parches de seguridad.

3.2 Seguridad de la información personal y profesional.

- Creación y gestión de contraseñas seguras.
- Uso de la autenticación multifactor (AMF).

- Correo electrónico seguro y gestión de archivos adjuntos.

3.3 Navegación segura por Internet.

- Identificación de sitios web seguros.
- Prevención del fraude en línea.
- Uso de VPN y otras herramientas de privacidad.

Módulo 4: Respuesta a incidentes y buenas prácticas.

4.1 Detección y respuesta a incidentes.

- Qué hacer en caso de incidente de seguridad.
- Protocolos de respuesta y recuperación.
- Importancia de la documentación y la notificación de incidentes.

4.2 Sensibilización y formación continuas.

- Crear una cultura de seguridad dentro de la organización.
- Programas continuos de sensibilización y formación.
- Recursos adicionales y próximos pasos.

Módulo 5: Políticas y cumplimiento.

5.1 Políticas de seguridad.

- Elaboración y aplicación de políticas de seguridad.
- Políticas de uso aceptable.
- Políticas de acceso a la información.

5.2 Cumplimiento de la normativa.

- Introducción a las leyes y normativas sobre ciberseguridad.
- Cumplimiento de normas como GDPR, HIPAA, etc.
- Auditorías y controles de seguridad.

Módulo 6: Ciberseguridad en el entorno empresarial.

6.1 Seguridad en el trabajo a distancia.

- Buenas prácticas para un trabajo a distancia seguro.
- Uso de dispositivos personales y BYOD.
- Garantizar la seguridad de la comunicación y la colaboración en línea.

6.2 Ciberseguridad para ejecutivos y dirigentes.

- Responsabilidades de los líderes en ciberseguridad.
- Integración de la ciberseguridad en la estrategia empresarial.
- Evaluación de riesgos y toma de decisiones con conocimiento de causa.

6.3 Introducción a la gestión de identidades y accesos (IAM).

- Conceptos básicos de IAM.
- Herramientas y tecnologías IAM.
- Mejores prácticas para la gestión de identidades y accesos.

Conoce más sobre nosotros.

Somos tu aliado para transformar el aprendizaje en éxito profesional.

Somos **Immersion International Business School.** Ofrecemos soluciones integrales y trabajamos para potenciar el talento humano y fortalecer a las empresas, ayudándolas a transformar desafíos en oportunidades.

Elige tu modalidad

Programas abiertos.

Accesibles a diferentes empresas con objetivos de aprendizaje en común.

Programas cerrados.

Se adaptan y enfocan a los objetivos y necesidades de cada empresa.

Tenemos presencia en



Nuestros servicios

Capacitaciones

Diseñadas para impulsarte.

Certificaciones

Avaladas internacionalmente.

Consultorías

Personalizadas para tu caso.

Somos #CertiProfPartner

En la actualidad, somos Training v Autorizado de CertiProf, un líder dedicado formar profesionales, potenciando sus habilidades en el ámbito laboral.

Hemos sido aprobados para brindar un servicio de calidad y ayudarte a alcanzar tus objetivos profesionales.

certiprof®
Certified Partner For Learning Solutions

Para mayor información contactar:

+503 7840-2073 info@inmersiongroup.com

Immersion
International Business School