Temario CertiProf.

Certificación Internacional

Cybersecurity Foundation Professional Certification - CSFPC™

La certificación proporciona una comprensión de los principios de la ciberseguridad. Su objetivo es dotar de los conocimientos para identificar amenazas, aplicar controles que protejan la información en entornos organizacionales.



Información del programa.

Objetivos del programa.

- Comprenderás los conceptos clave de la ciberseguridad, identificando los principales tipos de amenazas en entornos digitales.
- Conocer los marcos de referencia y las normativas básicas que rigen la seguridad de la información a nivel nacional y global.
- Comprenderás los conceptos relacionados con los aspectos humanos, organizativos y normativos.
- Comprenderás los conceptos relacionados con Ataques y Defensas.

Perfil del participante.

- Gerentes de Recursos Humanos, Líderes de gestión del talento y Cultura organizacional. Profesionales de TI, ciberseguridad y gestión de riesgos, gerentes, directores y responsables de seguridad de la información.
- Consultores y auditores de ciberseguridad y cumplimiento, encargados de implementar, diseñar y evaluar controles y políticas de protección de datos.

Para mayor información contactar:

+503 7840-2073 info@inmersiongroup.com

Immersion
International Business School

Módulo 0: NIST – Ciberseguridad para Negocios Pequeños.

- Ciberseguridad para Pequeños Negocios.
- La Complejidad de un Pequeño Negocio Moderno.
- Objetivos de Ciberseguridad.
- Confidencialidad.
- Integridad.
- Disponibilidad.
- Pequeño Negocio, Alto Impacto.
- Recursos Básicos de Ciberseguridad.
- Amenazas a la Ciberseguridad.
- Ataques de Phishing (Suplantación de Identidad).
- Ransomware.
- Hacking.
- Estafas Realizadas por Impostores.
- Amenazas Naturales.
- Elementos de Riesgo.
- Impacto de un Incidente.
- ¿Qué está protegiendo?
- 1. Identifique los Activos de su Negocio.
- 2. Identifique los Valores de los Activos.
- 3. Documente el Impacto en su Negocio por la Pérdida/Daño a los Activos.
- 4. Identifique la Probabilidad de Pérdida o Daño al Activo.
- 5. Identifique Prioridades y Soluciones Potenciales.
- Marco de Trabajo de la Ciberseguridad NIST.

Funciones del Marco de Trabajo de la Ciberseguridad.

- Objetivos de Aprendizaje.
- El Núcleo del Marco de Trabajo.
- Un Extracto del Núcleo del Marco de Trabajo.
- Identificar.
- Muestra de Actividades de Identificación.

- Proteger.
- Muestra de Actividades de Protección.
- Detectar.
- Muestras de Actividades de Detección.
- Responder.
- Muestra de Actividades de Respuesta.
- Recuperar.
- Muestra de Actividades de Recuperación.
- Marco de Trabajo.
- Tips Cotidianos.
- Recursos.

Módulo 1: CyBOK – Fundamentos de Ciberseguridad.

- Definición de Ciberseguridad.
- Áreas de Conocimiento CyBOK.
- Cómo Desplegar Conocimiento CyBOK para Resolver Problemas de Protección (Security).
- Funciones Dentro de un Sistema de Gestión de Protección (Security).
- Principios.
- Tema Interdisciplinario.
- Ciberespacio.

Módulo 2: Gestión de Riesgos.

- Temas a Tratar en esta Lección.
- ¿Qué es el riesgo?
- ¿Por qué la evaluación y la gestión del riesgo son importantes?
- ¿Qué es la evaluación y gestión del riesgo cibernético?
- Gobernanza de Riesgo.
- El Factor Humano y Comunicación del Riesgo.
- Cultura de Seguridad y Conciencia.
- Promulgación de la Política de Seguridad.
- Principios de Evaluación y Gestión de Riesgos.

- Elementos de Riesgo.
- Métodos de Evaluación y Gestión de Riesgos.
- Marcos de Gestión de Riesgos Cibernéticos Basados en Componentes.
- Métodos de Gestión de Riesgos Cibernéticos Impulsados por el Sistema.
- Evaluación y Gestión de Riesgos en Sistemas Ciberfísicos y Tecnología Operativa.
- Métricas de Seguridad.
- ¿Qué constituye las métricas buenas y malas?
- Continuidad del Negocio.
- ISO/IEC 27035-1:2016.
- NCSC- ISO/IEC 27035.
- Directrices para Mapear el Problema de Gestión de Riesgo.
- Conclusión.

Módulo 3: Ley y Regulación.

- Introducción.
- Desafíos.
- Respuesta.
- Fuera del Alcance.
- Principios Introductorios de la Ley e Investigación Legal.
- “Para Probar” Algo.
- “Niveles” de Pruebas.
- Aplicando el Derecho al Ciberespacio y las Tecnologías de la Información.
- Distinguiendo el Derecho Penal y Civil.
- Jurisdicción.
- Una Taxonomía de Jurisdicción.
- Jurisdicción Legislativa (Prescriptiva).
- Jurisdicción de Ejecución.
- El Problema de la Soberanía de los Datos.
- Leyes de Privacidad en General e Interceptación Electrónica.
- Interceptación Estatal (Acceso Legal).
- Interceptación No Estatal.

- Protección de Datos.
- Los “Jugadores”.
- ¿Qué se regula?
- “Datos Personales” vs “PII”
- Puntos Destacados de la Protección de Datos.
- Delitos Informáticos.
- Crímenes en Contra de los Sistemas de Información.
- Desafíos Recurrentes.
- Contrato.
- Contrato como un Medio para Incentivar Conductas de Protección (Security).
- Límites de Influencia.
- Influencia Relacionada con el Contrato Sobre Comportamiento de Protección (Security).
- Incumplimiento de Contrato y Recursos.
- Delito.
- Ejemplos de Delito.
- Negligencia (Responsabilidad Culposa).
- Responsabilidad del Producto (Responsabilidad Rigurosa).
- Cuantía de Pérdida (Q).
- Asignación e Imputación de Responsabilidad.
- Propiedad Intelectual.
- Ingeniería Inversa.
- Blindaje de los Intermediarios de Internet de los Procedimientos de Responsabilidad y Remoción (Bajar el Contenido).
- Desmaterialización de los Documentos y de los Servicios Fiduciarios Electrónicos.
- Emergen Cambios Legales.
- Otras Cuestiones Normativas.
- Ley Pública Internacional.
- Atribución Estatal.
- Operaciones de un Único Lugar.
- Ética.
- Códigos de Conducta.

- Pruebas de Vulnerabilidad y Divulgación.
- Gestión del Riesgo Legal.

Módulo 4: Factores Humanos.

- Introducción.
- Factores Humanos.
- La Protección (Security) Debe Ser Utilizable.
- Adaptar la Tarea al Ser Humano.
- Capacidades y Limitaciones Humanas.
- STM Y One-time password (OTPs).
- Capacidades y Limitaciones Humanas Generales.
- CAPTCHA.
- Metas y Tareas
- Capacidades y Limitaciones del Dispositivo.
- Error Humano.
- Condiciones de Diseño Latentes.
- Conciencia y Educación.
- Sensibilización y Educación.
- ¿Qué problemas de utilización enfrentan los desarrolladores?
- ¡Los Desarrolladores no son el Enemigo! La Necesidad de APIs de Protección (Security) Utilizables.
- La Utilización Huele: Un Análisis de la Lucha de los Desarrolladores con las Bibliotecas Criptográficas.

Módulo 5: Privacidad y Derechos en Línea.

- Introducción.
- Visión General.
- Privacidad como Confidencialidad.
- ¿Cuál es el problema?
- ¿Qué es la privacidad?
- Definiendo la Privacidad.

- Privacidad como…
- Privacidad como Transparencia.
- Privacidad como Control.
- Límites del Control y Transparencia.
- Privacidad como Confidencialidad.
- Panorama de Amenazas a la Privacidad.
- Enfoque Formal para el Control de Inferencia.
- Privacidad como Confidencialidad.
- Confidencialidad de Datos.
- Confidencialidad de Metadatos.
- Privacidad como Control.
- Privacidad como Transparencia.
- Tecnologías de Privacidad.
- Ingeniería de la Privacidad.
- Evaluación de la Privacidad.
- Conclusiones.

Módulo 6: Malware y Tecnologías de Ataque.

- Introducción.
- Malware.
- Taxonomía del Malware.
- Taxonomía del Malware: Dimensiones.
- Taxonomía: Ejemplos.
- Programas Potencialmente No Deseados (PUPs).
- Actividades Maliciosas del Malware.
- El Modelo Cyber Kill Chain.
- Ecosistema Clandestino.
- Objetivos de Acción.
- ¿Por qué analizar el Malware?
- Adquiriendo la Información del Malware.
- Análisis Estático.

- Análisis Dinámico.
- Otras Técnicas de Análisis.
- Entorno de Análisis.
- Entornos Comunes.
- Seguridad y Entornos Vivos.
- Técnicas de Anti-Análisis y Evasión.
- Objetivo de la Detección de Malware.
- Evasión y Contramedidas.
- Detección de Ataque de Malware.
- Análisis de Seguridad Basado en ML.
- Detección de Malware Basada en ML.
- Evasión de la Detección de Malware Basada en ML.
- Deriva Conceptual.
- Respuesta del Malware.
- Interrupción de las Operaciones de Malware.
- Atribución.
- Evasión y Contramedidas.
- Conclusión.

Módulo 7: Comportamiento Adverso.

- Introducción.
- Una Caracterización de Adversarios.
- Agresores Interpersonales.
- Delincuentes Organizados Cibernéticos.
- Hacktivistas.
- Actores Estatales.
- Los Elementos de una Operación Maliciosa.
- Servicios Especializados.
- Servicios Humanos.
- Métodos de Pago.
- Modelos para Entender las Operaciones Maliciosas.

- Árboles de Ataque: Ejemplo de un Ataque.
- Cyber Kill Chain.
- Criminología Ambiental.
- Atribución de Ataque.

Módulo 8 : Operaciones de Seguridad y Gestión de Incidentes.

- Introducción.
- ¿De qué se trata?
- Cronología y Alcance.
- Blucle MAPE-K General.
- Componentes de MAPE-K Supervisar-Analizar-Planificar-Ejecutar.
- Despliegues de las Tecnologías SOIM.
- Principios de Arquitectura - Arquitectura Típica.
- Detección de Intrusos y Sistemas de Prevención.
- MONITOR: Fuentes de Datos.
- Fuentes de Datos de Red: Posibles Detecciones.
- Fuentes de Datos de Aplicación.
- Fuentes de Datos del Sistema.
- Syslog.
- Problemas Frecuentes de Fuentes de Datos.
- Análisis de Rastros.
- Del Evento al Incidente.
- Detección de Uso Indebido.
- Detección de Anomalías.
- Problemas Generales en la Detección de Intrusos.
- Arquitectura Típica Información de Seguridad y Gestión de Eventos.
- Recolección de Datos en SIEM.
- Correlación de Alerta.
- Mitigación y Contramedidas Herramientas y Técnicas.
- Inteligencia y Análisis.
- Ciclo de Vida de la Gestión de Incidentes.

- Conclusión.

Módulo 9: Examen de Certificación.

- Insignia.
- Condiciones del Examen.

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