CERTIFICACIÓN INTERNACIONAL

FUNDAMENTOS DE CIBERSEGURIDAD

24 Horas | Online

Descubre estrategias para minimizar riesgos, fortalecer la ciberseguridad y garantizar la protección de datos en la empresa.

Programa de Capacitación.
Certificación Internacional en Fundamentos de Ciberseguridad y su Cumplimiento Legal.

Información del programa.

Modalidad: Online - Abierto
Horario: 1:00 pm a 5:00 pm
Fecha de inicio: 05 de junio 2025
Calendario de sesiones:

Junio 2025

Lun	Mar	Mié	Jue	Vie	Sáb	Dom
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

Inversión.

Precio de lista	**$675.00***
Precio preventa válido del 10 al 23 de mayo	**$350.00***
Apoyo Immersion válido hasta el 09 de mayo	**$275.00***

Condiciones.

*Precios no incluyen IVA.
*Consulta por beneficios exclusivos en inversión al inscribir grupos de 3 o más participantes.

Para mayor información contactar:
+503 7840-2073 info@inmersiongroup.com

Immersion International Business School

Descripción.

La Certificación Internacional en Fundamentos de Ciberseguridad está diseñada para proporcionar una comprensión integral de los principios esenciales de la ciberseguridad. Su objetivo es dotar a los participantes de los conocimientos básicos necesarios para identificar amenazas comunes, aplicar controles fundamentales que protejan la información en entornos organizacionales y comprender los riesgos digitales. A través de una metodología práctica e introductoria, se fomenta el desarrollo de una cultura de seguridad desde la base, alineada con buenas prácticas y estándares internacionales.

Conocimientos a adquirir.

- Comprender los conceptos esenciales de la ciberseguridad, identificando los principales tipos de amenazas y vulnerabilidades en entornos digitales.
- Conocer los principios fundamentales de la protección de la información, como la confidencialidad, integridad y disponibilidad.
- Conocer los marcos de referencia y normativas básicas que rigen la seguridad de la información a nivel nacional y global.

Perfil del participante.

- Profesionales de recursos humanos, operaciones, proyectos y áreas administrativas que participan en la implementación de políticas y procesos organizacionales relacionados con la ciberseguridad.
- Profesionales de TI, ciberseguridad y gestión de riesgos, gerentes, directores y responsables de seguridad de la información, interesados en implementar estrategias efectivas de prevención y respuesta ante incidentes y fortalecer sus conocimientos en la protección de activos digitales.
- Abogados, asesores legales y responsables de cumplimiento normativo, que requieren comprender las leyes internacionales y nacionales sobre ciberseguridad y protección de datos.
- Directivos, gerentes generales y miembros de juntas directivas, que toman decisiones estratégicas relacionadas con la protección de la información y el cumplimiento legal.
- Consultores y auditores de ciberseguridad y cumplimiento, encargados de evaluar, diseñar e implementar controles y políticas de protección de datos.

Contenido del programa.

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?
- ¿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

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

- ¿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

Módulo 3: Ley y Regulación

- 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

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

- Definiendo la Privacidad
- 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

Módulo 6: Malware y Tecnologías de Ataque

- 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

Módulo 7: Comportamiento Adverso

- 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

- ¿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

Facilitadora.

Karla Alas de Duarte

Especialista en Derecho y Ciberseguridad

Experiencia.

Karla Alas de Duarte es una abogada especialista en derecho informático y ciberseguridad con más de 20 años de experiencia en el ámbito jurídico y tecnológico. Ha asesorado a empresas del sector telecomunicaciones y despachos en temas de protección de datos, delitos informáticos, propiedad intelectual digital y comercio electrónico. Su trayectoria incluye el liderazgo en la creación de normativas clave para El Salvador, como participación en la redacción de la Ley de Delitos Informáticos y Conexos.

En el campo de la ciberseguridad, ha ocupado cargos estratégicos en firmas como ECIJA Centroamérica y el Grupo Claro El Salvador, donde diseñó y ejecutó estrategias legales para afrontar procesos regulatorios complejos ante instituciones como la Defensoría del Consumidor, SIGET, y ha brindado consultorías para proyectos internacionales como USAID-Nathan Inc. Su experiencia combina la defensa legal en procesos administrativos con la construcción de políticas internas y gestión de crisis legales en entornos digitales.

Además de su labor como asesora, Karla ha desempeñado un papel activo en la formación de profesionales en temas como piratería marcaria, derecho aduanal y telecomunicaciones. Es miembro de organizaciones como Internet Society y Legal Hackers El Salvador. Su formación en Ciencias Jurídicas y Sociales por la Universidad José Matías Delgado, y su dominio del inglés legal, respaldan su capacidad para abordar con precisión los desafíos legales del entorno digital contemporáneo.

Formación.

• Licenciatura en Ciencias Jurídicas y Sociales.

Especialización.

• Derecho Informático.
• Ciberseguridad.
• Protección de Datos.
• Delitos Informáticos.
• Comercio Electrónico.
• Litigios Regulatorios y Administrativos.
• Propiedad Intelectual Digital.