Educación Continua

TECNOLÓGICO DE MONTERREY

Diplomado

Gestión de la Seguridad de la Información (Virtual)

Duración 124 horas

Objetivo general:
Proveer las bases teóricas y prácticas de la gestión de la seguridad de la información, con el objetivo de contar con todos los elementos necesarios para diseñar e implementar una estrategia de seguridad dentro de una organización. Esto involucra identificar los diferentes servicios y metodologías necesarios para construir un sistema informático operacional seguro que este alineado con los objetivos de la organización

Beneficio:
Conocerá todas las áreas relacionadas con la gestión de la seguridad de la información.
Contará con los elementos suficientes para definir la estrategia del programa de gestión de la seguridad de la información en todas las áreas de la organización.

Dirigido a:
Personal que labora en el área de sistemas con toma de decisiones, de instituciones privadas como públicas.
Personal de auditoría interna y de contraloría interna de las organizaciones.
Personal que labore en empresas consultoras/auditoras en el área de seguridad de la información.

Requisito:
No requiere contar con un título profesional.
No requiere de experiencia laboral.

Contenido:

Módulo 1 Introducción a la Seguridad de la Información

Al final de este módulo el participante:
? Describirá los conceptos básicos de seguridad de la información.
? Contará con las bases suficientes para implementar un programa de awareness dentro de una organización.
? Diferenciará las principales certificaciones que existen en el área de seguridad de la Información.
? Identificará los diferentes modelos, técnicas y amenazas relacionadas con control de acceso.

Temario

1. Antecedentes y conceptos de seguridad informática.
2. Estándares de Ciberseguridad
3. Fundamentos seguridad de la información
4. Awareness: Marketing o Cambio Organizacional
5. Metodología de Awareness
6. Tips para la implementación de una metodología de awareness
7. Certificación de individuos
8. Certificación de organizaciones

9. Certificación de productos
10. Conceptos base de control de acceso.
11. El proceso del control de acceso.
12. Modelos de control de acceso
13. Técnicas y tecnologías de acceso
14. Amenazas al entorno del acceso
15. Ejercicios prácticos

Duración del módulo: 12 horas

Módulo 2 Políticas de Seguridad

Conocer las diferentes tecnologías existentes necesarias para implementar una estrategia de seguridad de la información.

Temario

1. Conceptos básicos de criptología
2. Dispositivos de seguridad perimetral
3. Seguridad en redes inalámbricas
4. IDS e IPS
5. Computo forense
6. Software malicioso
7. Seguridad en aplicaciones web
8. Seguridad en bases de datos
9. Seguridad en aplicaciones
10. Pruebas de penetración
11. Hardening de sistemas operativos

Duración del módulo: 8 horas

Módulo 3 El rol del Oficial de Seguridad de la Información

Conocer los aspectos relacionados con los requerimientos de la Función de Seguridad así como la interrelación de sus componentes, la visión y skills del CISO actual.

Temario

1. Ubicación de la Función de Seguridad en el Organigrama
2. Estructura Organizacional
3. Propósito, Visión, Objetivos, Metas y Planes de la Función de Seguridad
4. Componentes de la Función de Seguridad y su Interrelación
5. La Seguridad como Función de Negocio
6. Cómo Vender la Seguridad
7. El presupuesto de la Seguridad
8. Visión y Skills del CISO Actual

Duración del módulo: 4 horas

Módulo 4 Respuesta a Incidentes y Manejo de Crisis de TI

Proveer una guía de los pasos a seguir para establecer una Arquitectura de Seguridad de forma ordenada, y que ofrezca un panorama general del establecimiento de la misma en una organización. Identificar los conceptos y principios claves y críticos para asegurar la infraestructura. Conocer los principales frameworks de arquitecturas de seguridad.

Temario

1. Introducción a la Arquitectura de Seguridad (AS)
2. Elementos
3. Arquitectura del sistema
4. Arquitectura del Sistema de Seguridad
5. Análisis de Riesgos
6. Política de Seguridad
7. Requerimientos de la AS
8. Modelos de Seguridad
9. Operación de los Modos de Seguridad
10. Confianza y Aseguramiento
11. Frameworks Arquitectura de Seguridad
12. Sistemas abiertos y cerrados

Duración del módulo: 4 horas

Módulo 5 Auditoría de Seguridad de la InformaciónPolíticas de Seguridad

Entender y aplicar los conceptos teóricos de políticas de seguridad de la información en sistemas de cómputo institucionales y empresariales. Comprender los modelos y políticas de seguridad de la información para entender y establecer el marco de referencia y normas o criterios que debe cumplir un sistema computacional seguro.

Temario

1. Introducción.
2. Definición e Historia.
3. Beneficios.
4. Aspectos de las Mediciones en la Seguridad.
5. Tipos de Métricas
6. Consideraciones organizacionales
7. Manejabilidad (consideraciones en la administración)
8. Factores de éxito (Correctness & Effectiveness)
9. Indicadores líderes contra rezagados
10. Propiedades cuantitativas y cualitativas (Mediciones pequeñas vs largas)
11. Posibles áreas de aplicación
12. Modelos formales de Mediciones y Métricas de Seguridad
13. Recolección y análisis histórico de datos
14. Técnicas de evaluación con Inteligencia Artificial
15. Métodos de Medición concretos y prácticos
16. Componentes intrínsecamente medibles

Duración del módulo: 8 horas

Módulo 6 Métricas de Seguridad

Proveer una guía para el desarrollo específico, selección e implementación de métricas para ser usadas en la medición del rendimiento de la información de las técnicas y controles de seguridad.

Temario

1. El NIST y Seguridad Información
2. Utilidad de las métricas
3. Definición y características de las métricas

4. Audiencias
5. KPIs y KRIs
6. Características de una buena métrica
7. Categorización de métricas
8. Términos relacionados con métricas
9. Definición de métricas
10. Programas de métricas
11. Frameworks de métricas

Duración del módulo: 4 horas

Módulo 7 Compliance

Entender y aplicar los conceptos teóricos de políticas de seguridad de la información en sistemas de cómputo institucionales y empresariales. Comprender los modelos y políticas de seguridad de la información para entender y establecer el marco de referencia y normas o criterios que debe cumplir un sistema computacional seguro.

Temario

1. Introducción al compliance.
2. Función de compliance vs otras funciones de control.
3. Compliance vs Seguridad Informática.
4. Compliance vs Risk Management.
5. Relación entre compliance y gobierno corporativo.
6. Estructura de compliance: Políticas, estándares, programas.
7. Principales estándares, leyes, regulaciones y mejores prácticas relacionadas con Seguridad Informática.

Duración del módulo: 4 horas

Módulo 8 Outsourcing de Servicios de Seguridad

Proporcionar los principios y controles básicos necesarios para mantener un sistema de información continuamente protegido conforme el nivel requerido por la organización. Reflexionar sobre los controles que deben incorporarse en la organización durante su operación diaria para no sobre-controlar ni sub-controlar. Describir formas de evaluar la seguridad informática desde el punto de vista teórico y práctico.

Temario

1. Introducción
2. Principios Due Care/Due Diligence
3. Proceso de implantación de seguridad informática
4. Controles de seguridad en la organización
5. Familia de estándares ISO 27000
6. Controles Administrativos
7. Tipos de Evaluación

Duración del módulo: 8 horas

Módulo 9 Tecnologías aplicadas a la Seguridad Informática

Revisar los conceptos utilizados en el DRP/BCP (Disaster Recovery Planning / Business Continuity Planning) y presentar una metodología para el desarrollo e implementación de un Plan de Continuidad del Negocio en casos de desastre.

Temario

1. Introducción al DRP/BCP.
2. Metodología para desarrollar el DRP/BCP.
3. Planeación y organización del Proyecto de DRP/BCP.
4. Análisis de riesgos para prevenir desastres.
5. Análisis de impacto al negocio (BIA).
6. Requerimientos de recuperación de TI y de áreas usuarias.
7. El Esquema de respaldos.
8. Costos del DRP/BCP.
9. Estrategias de respaldo y recuperación.
10. Manejo de la emergencia.
11. El documento del DRP/BCP.
12. Prueba y mantenimiento del DRP/BCP.
13. Otros aspectos del DRP/BCP.

Duración del módulo: 8 horas

Módulo 10 Seguridad Física

Conocer los fundamentos de diseño y tecnologías relacionadas con la seguridad física de un centro de datos.

Temario

1. El rol de la seguridad física en la seguridad informática
2. Identificación de los activos a proteger
3. Control de Acceso
4. CCTV

Duración del módulo: 4 horas

Módulo 11 BCP & DRP

Conocer todos los conceptos éticos y legales relacionados con la seguridad de la información.

Temario

1. Ética y seguridad de la información
2. Código de ética de ISC2
3. RFC 1087
4. Privacidad y Datos personales
5. Protección Jurídica del Software
6. Definición de delito informático
7. Acceso ilícito a sistemas y equipos de informática
8. Programas de cómputo
9. Pornografía Infantil
10. Delitos financieros

Duración del módulo: 8 horas

Módulo 12 Seguridad en las Operaciones

Conocer los aspectos relacionados con la Auditoría de Seguridad, así como los enfoques, paradigmas, guías, herramientas y técnicas necesarias para realizar una auditoría.

Temario

1. Conceptos generales de la Auditoría
2. Ubicación de la Auditoría de la Seguridad en el Organigrama
3. Diferencias entre la Auditoría de Seguridad y la Auditoría de TI
4. Alcance de la Auditoría de Seguridad
5. Enfoques de la Auditoría de Seguridad
6. Paradigmas de la Auditoría de Seguridad
7. Tipos de Pruebas en la Auditoría de Seguridad
8. Guías, Técnicas y Herramientas de la Auditoría de Seguridad

Duración del módulo: 8 horas

Módulo 13 Aspectos Legales y Éticos

Conocer las características, condiciones para el outsoursing de seguridad informática, así como aspectos para la elaboración de RFP´s y acuerdos de niveles de servicio para la contratación de servicios de outsoursing de seguridad informática.

Temario

1. Antecedentes y origen del outsoursing.
2. Los Managed Security Services Providers (MSSP´s)
3. Características del outsoursing de seguridad Informática.
4. Condiciones para el outsoursing de seguridad informática.
5. RFP Para la contratación de servicios en outsoursing de seguridad Informática
6. Guías de contenido para la elaboración de acuerdos de niveles de servicio para el outsoursing
7. de seguridad informática.
8. Metodología para un convenio de servicios de outsourcing de seguridad informática.
9. Mercado de los MSSP´s.

Duración del módulo: 16 horas

Módulo 14 Tendencias Seguridad Información

El participante comprenderá el ciclo de producción de inteligencia para poder generar productos accionables, que permitan prevenir y detectar amenazas basándose en evidencia.

Temario

1. El ciclo de vida de la Inteligencia sobre Amenazas
1.1. El ciclo de inteligencia
1.2. Las Preguntas Clave de Inteligencia (Key Intelligence Questions)
1.3. Planeación y Dirección
1.4. Acopio / Recolección de información en crudo
1.5. Procesamiento / Clasificación de la información
1.6. Análisis de información y técnicas de análisis estructurado.
1.7. Generación del producto de inteligencia y su diseminación
1.8. Retroalimentación al ciclo

2. Tipos de Productos de Inteligencia sobre Amenazas
2.1 Estratégicos
2.2 Tácticos
2.3 Operacionales

3. Casos de uso de Inteligencia sobre amenazas

3.1 Respuesta a incidentes
3.2 Operaciones de seguridad (SoC)
3,3 Gestión de vulnerabilidades
3.4 Análisis de riesgos
3.5 Prevención de fraudes
3.6 Liderazgo de seguridad

Duración del módulo: 4 horas

Módulo 15 Inteligencia Sobre Amenazas

Que el alumno conozca los diferentes documentos de referencia, procesos y políticas necesarias para poder hacer un plan de respuesta a incidentes.

Temario

Contenido
Temario del módulo 1. Estándares y Guías de Respuesta a Incidentes
2. Equipo de Respuesta a Incidentes
3. Procesos y Procedimientos
4. Listas de Seguimiento
5. Triage
6. Ejercicio práctico

Duración del módulo: 4 horas

Módulo 16 Análisis de Riesgos

Conocer los aspectos básicos del análisis de riesgos, así como las herramientas, metodologías y técnicas usadas en esta área.

Temario

1. Antecedentes.
2. Conceptos de los elementos del riesgo.
3. Análisis de riesgos.
4. Manejo o administración de riesgos.
5. Análisis de riesgos cuantitativos.
6. Análisis de riesgos cualitativos.
7. Drivers del manejo de riesgos.
8. ISO/IEC TR 13335 como guía para la identificación y priorización de riesgos.
9. Metodologías, estándares y herramientas.

Duración del módulo: 8 horas

Módulo 17 Práctica de FRAP

Conocer, analizar y trabajar con la metodología de análisis de riesgos FRAP con un caso práctico donde los participantes tengan la experiencia de realizar un análisis de riesgos, así como el poder utilizar todos los conocimientos obtenidos en el diplomado y así poder trazar una estrategia de seguridad informática basada en el análisis.

Temario

1. Antecedentes.
2. Metodología FRAP.
3. FRAP y otras metodologías.
4. Caso práctico.
5. Estrategia de seguridad basada en el análisis de riesgos.

Duración del módulo: 8 horas

Módulo 18 Arquitectura de Seguridad

Conocer la evolución que ha tenido la seguridad de la información hasta nuestros días, así como las nuevas tecnologías y procesos relacionados con ataques y defensa de sistemas.

Temario

1. Estado actual de la seguridad de la información
2. Evolución de la seguridad de la información
3. La academia y la ciencia de la seguridad
4. Ataques computacionales del futuro
5. Dispositivos y medidas de seguridad del futuro

Duración del módulo: 4 horas