creasys
conocimiento y capacitación

Nuestro curso provee las herramientas teóricas y prácticas para conocer y aplicar técnicas de ciberseguridad utilizando medidas de seguridad y recomendaciones para detectar, evitar y/o mitigar amenazas y ataques a la información de su organización.

DIRIGIDO A

- Mienbros de una organizacióin pública o privada
- Usuarios de sistemas informáticos

CRITERIOS DE APROBACIÓN

- Se requiere el 75% de asistencia
- Nota sobre 4, en una escala del 1 al 7, en la evaluación del curso

DURACIÓN

12 horas

VALOR POR ASISTENTE

$ 134.100

CÓDIGO SENCE

1238015285

METODOLOGÍA

Para la parte teórica del curso se utilizará una metodología expositiva en la cual se dará a conocer la importancia de la ciberseguridad; las amenazas, riesgos y vulnerabilidades, a nivel informático, a las cuales están expuestas hoy en día las compañías; y se mostrarán los patrones de ataque a los activos de información.
En su parte práctica se asignarán ejercicios grupales que permitan identificar los tipos de ataque, aplicar medidas de seguridad informática y emplear lineamientos para crear políticas y un manual de seguridad de la información en la organización.

EVALUACIONES

Prueba escrita que medirá la aplicación de conocimientos.

creasys
conocimiento y capacitación

CONTENIDOS

Unidad 1: Aspectos generales de la seguridad de la información y ciberseguridad, utilizando los contenidos relacionados con las amenazas, riesgos y vulnerabilidad a los que se ven enfrentadas las organizaciones.

- Conociendo la ciberseguridad
  - Importancia de la ciberseguridad
  - Contexto actual
  - Seguridad de la información
  - Principios y pilares de la ciberseguridad

- Amenaza, riesgo y vulnerabilidad
  - Definiciones
  - Ciclo de una amenaza
  - Importancia del factor humano
  - Eventos, ataques e incidentes de seguridad
  - Tipos de atacantes y anatomía de un ataque hacker

Unidad 2: Tipos de amenazas y patrones de ataque a los activos de información, aplicando las características y descripciones de los Malwares y ATPs, así como los tipos de ataque que afectan la red, sistemas y /o aplicaciones.

- Ataques Malware y ATP
  - Introducción
  - Tipos de malware
  - Propagación y replicación
  - Mecanismos de defensa del malware
  - Concepto ATP
  - Fases de una ATP

- Ataques a red / sistemas / aplicación
  - Patrones de ataque
  - Envenenamientos
  - Suplantación
  - Man in the middle
  - Secuestros de sesión
  - Denegaciones de servicio
  - Desbordamientos
  - Inyecciones de código

creasys
conocimiento y capacitación

CONTENIDOS

Unidad 3: Medidas de seguridad a nivel red / servicios / aplicación mediante el uso de diversas contramedidas que permiten detectar y evitar ataques y malwares.

- Contramedidas nivel red
  - Sistemas criptográficos
  - Firma digital y certificados
  - Mecanismos de autenticación
  - Seguridad perimetral
  - Segmentación de redes
  - Detección de intrusos
  - Comunicación segura
  - Redes virtuales (VPN)

- Contramedidas nivel servicios / aplicación
  - Sistemas operativos de confianza
  - Antivirus
  - Codificación segura

Unidad 4: Recomendaciones de seguridad, utilizando las normas y prohibiciones de las actividades de mayor riesgo en una organización.

- Recomendaciones seguridad digital
  - Uso de equipos electrónicos
  - Uso del correo electrónico y redes
  - Uso de passwords

- Descripción y recomendaciones
  - Incidentes de seguridad digital

Unidad 5: Lineamientos para crear políticas y un manual de seguridad de la información, mediante el uso de contenidos y definiciones relacionados con la norma ISO27002 y estructura de un manual.

- Normativa, políticas y manual
  - Norma ISO27002
  - Principios y valores de seguridad
  - Dominios de la certificación (seguridad organizativa, lógica, legal y física)
  - Política de seguridad de la información o sistema de gestión de seguridad

- Oficial de seguridad de la información y comité de seguridad de la información
  - Análisis de riesgos TI
  - Creación de políticas y manual
  - Definiciones y marco de aplicación
  - Propósito
  - Políticas de seguridad (descripción, objetivo, alcance, normas y prohibiciones)
  - Cumplimiento
  - Glosario