CURSOS

Ciberseguridad

para empresas con presupuesto limitado

Desarrollo Profesional ®
y Consultoría
Ecotec

Descripción

Este curso está diseñado para empresas y profesionales interesados en fortalecer la ciberseguridad de su entorno con herramientas gratuitas y prácticas de bajo costo. A través de las sesiones, los participantes aprenderán a aplicar conceptos de seguridad, implementar estrategias de confianza cero y automatizar tareas clave para proteger sus sistemas, redes y datos.

Justificación

La ciberseguridad es un aspecto crítico en cualquier organización, pero los costos de implementación pueden ser un desafío, especialmente para pequeñas y medianas empresas. Este curso ofrece una solución práctica y asequible para implementar una ciberseguridad robusta, enfocándose en métodos de bajo costo que maximizan los recursos existentes.

Objetivo general

Capacitar a los participantes para mejorar la seguridad de sus entornos tecnológicos mediante la aplicación de principios de confianza cero, herramientas de MFA, control de acceso y técnicas de protección sin requerir grandes inversiones.

Contenido

Unidad 1

Fundamentos de Ciberseguridad con Recursos Limitados (2 hrs)

- Introducción a amenazas, vectores de ataque y principios de ciberseguridad.
- Evaluación de los riesgos y amenazas comunes para empresas con poco presupuesto.

Unidad 2

Principios de Confianza Cero (Zero Trust) (2 hrs)

- Fundamentos de Zero Trust y cómo aplicarlo con recursos existentes.
- Implementación de estrategias como el principio de menor privilegio y segmentación de red.

Unidad 3

Políticas de Contraseñas y Control de Acceso (2 hrs)

- Implementación de políticas de contraseñas robustas y control de acceso mínimo.
- Mejores prácticas de control de acceso y autenticación en equipos de trabajo.

Unidad 4

Configuración Básica de MFA sin Costos (2 hrs)

- Introducción a herramientas de MFA gratuitas, como Google Authenticator y Microsoft Authenticator.
- Implementación de MFA en sistemas críticos sin inversión adicional.

Unidad 5

Endurecimiento de Sistemas Operativos (Hardening) (2 hrs)

- Pasos para proteger sistemas Windows y Linux con configuraciones de hardening.
- Uso de herramientas y configuraciones integradas en el sistema para incrementar la seguridad.
- Lista de verificación de hardening y recomendaciones

Unidad 6

Herramientas de Seguridad Gratuitas para Escaneo de Vulnerabilidades (2 hrs)

- Introducción a escáneres de vulnerabilidades gratuitos como OpenVAS y Nmap.
- Configuración básica y uso de estas herramientas para identificar puntos débiles en la red.
- Interpretación de resultados y acciones recomendadas.

Unidad 7

Seguridad en Redes Internas sin Equipos Costoso (2 hrs)

- Segmentación de red y configuración de firewalls para aplicar Zero Trust.
- Implementación de segmentación de red y reglas de firewall usando recursos gratuitos.
- Configuración de firewalls básicos y uso de cortafuegos en routersy switches.
- Creación de reglas de red para proteger datos críticos.

Unidad 8

Protección contra Malware y Phishing (2 hrs)

- Uso de antivirus gratuitos y buenas prácticas para prevenir infecciones de malware.
- Identificación y prevención de ataques de phishing en entornos empresariales.
- Ejercicio de simulación de ataques de phishing para concienciar al personal.

Unidad 9

Copias de Seguridad y Recuperación de Datos (2 hrs)

- Estrategias de respaldo y restauración de datos usando herramientas comunitarias
- Automatización de copias de seguridad práctica de recuperación de datos como parte de un plan de respuesta ante incidentes.

Unidad 10

Monitorización y Registro de Actividades sin Licencias (2 hrs)

- Uso de herramientas de código abierto para monitorización básica de actividades, como Graylog o ELK Stack.
- Configuración de auditorías de seguridad en sistemas críticos.

Docente

Ing. Carlos Montes

Síntesis curricular

- Especialista en tecnología de la información innovador y comprometido con más de 20 años de experiencia diversa que abarca soporte de TI, administración de sistemas y gestión de redes.
- Reconocido por liderar proyectos técnicos que impulsan mejoras de eficiencia y rendimiento, brindar un soporte excepcional al usuario e implementar soluciones de TI sólidas adaptadas a las necesidades de la organización.
- Entusiasmado por utilizar mi amplia experiencia para contribuir de manera significativa a las empresas, asegurando operaciones tecnológicas fluidas en entornos dinámicos.

Metodología a aplicar

El curso es 100% práctico y se desarrolla mediante talleres aplicados a cada tema, con demostraciones en vivo y ejercicios que permiten implementar los conceptos aprendidos en tiempo real. La metodología combina una breve explicación teórica seguida de actividades prácticas. Los participantes recibirán orientación para aplicar estos conocimientos en sus propios entornos empresariales, enfatizando el uso de recursos accesibles y de bajo costo.

Evaluación

La evaluación del curso se basará en la participación activa en los talleres. Se valorará la creatividad, la aplicabilidad en el contexto académico y la capacidad de integrar lo aprendido a lo largo del curso.

Recursos

Hardware: Computadora portátil o de escritorio con acceso a internet y sistema operativo Windows/Linux. **Software:** Herramientas de MFA gratuitas (Google Authenticator, PrivacyIDEA), escáneres de vulnerabilidades (OpenVAS, Nmap), configuraciones de firewall básicas. **Material de Apoyo:** Documentación sobre hardening de sistemas, talleres del curso, máquinas virtuales, entre otros recursos digitales.

Presencial
Modalidad

20 hrs.
Duración

Febrero 2025
Inicio del curso

Viernes de 15:00 a 19:00
Sábados (2 días) de 09 a 13:00 y 14:00 a 18:00 con almuerzo incluido

Conoce más de nosotros

CONTÁCTANOS

+593-979 492 245

PBX: (04) 5150400 OPC. 2

posgrado@ecotec.edu.ec

CAMPUS

GUAYAQUIL
Av. Juan Tanca Marengo Km. 2

uecotec uecotec @UnivEcotec Universidad Ecotec Universidad Ecotec