

CONTROLES DE CIBERSEGURIDAD PARA LAS PYMEs

Este curso está diseñado para proporcionar a los participantes una comprensión profunda y práctica de los controles esenciales necesarios para proteger las organizaciones de amenazas cibernéticas. A lo largo de 12 horas de formación intensiva, divididas en tres días, cubriremos una amplia gama de temas cruciales para la seguridad de la información.

La ciberseguridad es un campo en constante evolución, y las amenazas se vuelven cada vez más sofisticadas. Este curso se enfoca en los Controles de CIS (Center for Internet Security) v8, que son un conjunto de acciones recomendadas para mitigar las amenazas más comunes y mejorar la seguridad general. Al finalizar este curso, los participantes estarán equipados con el conocimiento necesario para implementar y gestionar estos controles en sus propias organizaciones.

Dirigido a:

Este curso es ideal para profesionales de TI, responsables de seguridad y cualquier persona interesada en mejorar la ciberseguridad en micro, pequeña y mediana empresa. Nuestro objetivo es proporcionar herramientas y conocimientos prácticos que se puedan aplicar directamente en el trabajo diario para mejorar la postura de seguridad de cualquier organización.

Inversión

Incluye diploma de participación y 12 CPE

- **Miembros ISACA:** USD \$ 85 + IVA
- **No Miembros:** USD \$ 95 + IVA

Para inscribirte debes enviarnos la ficha de inscripción completa y comprobante de pago, por dudas escríbenos a capitulosansalvador@isaca.org.sv y 6844-5653 (**cupo limitado**)

Fechas y lugar del curso

- **Fechas:** 13, 20 y 27 de septiembre (12 horas)
- **Modalidad:** Virtual
- **Hora:** 8:00 a 12:00 m.d.

Más información

 @chapter_sv_isac

 @ISACAEISalvador

 +503 6844-5653

 @ISACAEISalvador

 capitulosansalvador@isaca.org.sv

 www.isaca.org.sv

Instructores

Héctor Jiménez



Especialista con más de 30 años de trayectoria en seguridad de la información, ciberseguridad, auditoría de TI y continuidad del negocio, con experiencia en sector financiero, telecomunicaciones y retail.

Áreas de Experiencia: Implementación de Sistemas de Gestión de Seguridad de la Información (ISO 27001, NIST CSF, PCI DSS, ISO 22301, CobiT, ITIL), Gestión de riesgos tecnológicos y operativos, Ciberdefensa, monitoreo y respuesta ante incidentes, Auditoría de TI y diagnósticos de seguridad, Planes de continuidad y recuperación ante desastres.

Con certificación en:

- ISO 27001 Lead Implementer
- Certified Penetration Testing Engineer (CPTE)
- Cybersecurity Fundamentals (CSX-F)
- Cloud Fundamentals – ISACA

Manuel Sigüenza



Profesional con más de 12 años de trayectoria en auditoría de tecnología y ciberseguridad, especializado en sectores clave como el bancario, de telecomunicaciones y bursátil. Sólida formación profesional que incluye una Ingeniería en Sistemas Informáticos, una Maestría en Dirección y Gestión de las Tecnologías de la Información (en curso), posgrados en Ciberseguridad, Finanzas Internacionales y Criptomonedas, y certificaciones de prestigio internacional como CISA, CSXF, ISO 27001 y COBITF 2019.

Más información

 @chapter_sv_isac

 @ISACAEISalvador

 +503 6844-5653

 @ISACAEISalvador

 capitulosansalvador@isaca.org.sv

 www.isaca.org.sv

Contenido del curso

Día 1: Introducción y Fundamentos, y Controles Básicos

1. Bienvenida y presentación del curso
2. Introducción a los Controles de CIS
3. Fundamentos de ciberseguridad
4. Estructura y objetivos de los Controles de CIS v8
5. Control 1: Inventario y control de activos
6. Control 2: Gestión de software autorizado y no autorizado
7. Control 3: Gestión continua de vulnerabilidades
8. Control 4: Uso controlado de privilegios administrativos

Día 2: Controles Fundamentales y Organizacionales

1. Control 5: Configuración segura de hardware y software
2. Control 6: Mantenimiento, monitoreo y análisis de registros de auditoría
3. Control 7: Protección de correo electrónico y navegadores web
4. Control 8: Defensa contra malware
5. Control 9: Limitación y control de puertos, protocolos y servicios
6. Control 10: Capacitación y concienciación en seguridad
7. Control 11: Protección de datos
8. Control 12: Respuesta y gestión de incidentes

Día 3: Controles Avanzados y Implementación

1. Control 13: Seguridad en la red
2. Control 14: Seguridad en aplicaciones
3. Control 15: Gestión de accesos y cuentas
4. Control 16: Monitoreo y control de cuentas
5. Control 17: Implementación de controles de seguridad
6. Control 18: Evaluación y auditoría de seguridad
7. Taller práctico: Implementación de controles en un entorno simulado
8. Evaluación final y cierre del curso

 @chapter_sv

Más información

 @chapter_sv_isac

 @ISACAEISalvador

 +503 6844-5653

 @ISACAEISalvador

 capitulosansalvador@isaca.org.sv

 www.isaca.org.sv