BTechC
BUSINESS, TECHNOLOGY
& CYBERSECURITY

TALLER DE SEGURIDAD INFORMÁTICA

PRESENTACIÓN

Agradecemos que considere a Business Technology & Cybersecurity (BTechC) para fortalecer sus objetivos de capacitación.

Los cursos impartidos por el Centro de Capacitación BTechC permiten una formación integral en el ámbito técnico-jurídico relacionado con los temas de la Seguridad de la Información, la Ciberseguridad y la Protección de Datos Personales, utilizando nuestra experiencia y know-how en la implementación de estándares y tecnologías aplicando una metodología didáctica.

En BTechC impartimos cursos que enriquecen el conocimiento y le brindan una forma ágil de aprender, desarrollar sus habilidades y apoyarle, de ser necesario en el proceso de certificación.

INTRODUCCIÓN

En la era digital actual, compenetrarnos en la Ciberseguridad es fundamental para el éxito y la sostenibilidad de cualquier organización.

Este Taller está diseñado específicamente para todo aquel que maneje información sensible en una organización, proporcionándoles una comprensión clara y práctica de un entorno seguro.

A través de un lenguaje sencillo y claro, los participantes adquirirán los conocimientos necesarios para aplicar una cultura de Protección en toda la organización.

BENEFICIOS

1 **Comprensión: Los participantes fortalecerán su conocimiento sobre la importancia de la Ciberseguridad.**

2 **Identificación de Riesgos: Aprenderán a identificar y evaluar los riesgos más comunes, incluyendo amenazas internas y externas.**

3 **Toma de Decisiones Informadas: Estarán mejor preparados ante un delito informático a la hora de interactuar en correos electrónicos, aplicaciones, herramientas de mensajería, etc.**

4 **Liderazgo en Seguridad: Desarrollarán habilidades hacia una cultura de protección en toda la organización, promoviendo la conciencia y la responsabilidad en todos los niveles.**

5 **Protección de Activos: Conocerán las mejores prácticas para mitigar los riesgos de los activos más valiosos de la empresa.**

OBJETIVO GENERAL

Al finalizar este taller, los participantes podrán:

Incorporar a través de un lenguaje claro y necesario la importancia de la Ciberseguridad, para contribuir a mitigar los riesgos y disminuir el impacto reputacional, económico y legal.

TEMARIO

Módulo 1: Introducción a la Ciberseguridad (2 horas)

Objetivo: El participante será capaz de comprender los fundamentos de la ciberseguridad, incluyendo su definición, alcance, conceptos clave y marco legal, para identificar y contextualizar las amenazas y riesgos en el entorno digital.

- **Definición y alcance de la ciberseguridad.**
- **Conceptos clave: confidencialidad, integridad, disponibilidad (CIA).**
- **Riesgos, Amenazas, Agente Amenaza, Impacto, Vulnerabilidad, Incidente.**
- **Tipos de amenazas y ataques cibernéticos.**
- **Marco legal y normativas de ciberseguridad.**
- **Tendencias actuales y futuras en ciberseguridad.**

Módulo 2: Amenazas y Vulnerabilidades (3 horas)

Objetivo: El participante será capaz de identificar y clasificar las diferentes amenazas y vulnerabilidades cibernéticas, comprendiendo su impacto potencial en los sistemas y datos de la organización.

- **Malware: virus, gusanos, troyanos, bots, spam, ransomware.**
- **Phishing, Pharming.**
- **Ingeniería social.**
- **Ataques de denegación de servicio.**
- **Vulnerabilidades de software y hardware.**
- **Amenazas internas y externas.**

TEMARIO

Módulo 3: Defensa Cibernética (3 horas)

Objetivo: El participante será capaz de aplicar medidas de protección básicas en sistemas y redes, incluyendo la gestión de contraseñas, la configuración de firewalls y la implementación de VPNs, para mitigar los riesgos de ataques cibernéticos.

- **Contraseñas.**
- **Tipos de cuentas de usuarios.**
- **Fundamentos de redes y protocolos (TCP/IP).**
- **Firewalls y sistemas de detección de intrusiones (IDS/IPS).**
- **Redes privadas virtuales (VPN).**
- **Zero Trust.**
- **Seguridad Wi-Fi.**
- **Segmentación de redes.**

Módulo 4: Seguridad de Sistemas y Datos (3 horas)

Objetivo: El participante será capaz implementar medidas de seguridad para proteger los sistemas y datos de la organización, incluyendo la gestión de identidades y accesos, el cifrado de datos y la realización de copias de seguridad.

- **Sistemas operativos seguros.**
- **Mínimo Privilegio.**
- **Gestión de identidades y accesos (IAM).**

TEMARIO

- **Cifrado de dato en tránsito y en reposo.**
- **Certificados digitales.**
- **Copias de seguridad y recuperación de desastres.**
- **Seguridad de bases de datos.**
- **Seguridad de datos no estructurados.**

Módulo 5: Seguridad en Aplicaciones Web (2 horas)

Objetivo: El participante será capaz de identificar y mitigar las vulnerabilidades comunes en aplicaciones web, aplicando medidas de seguridad en el desarrollo de software y realizando pruebas de seguridad básicas.

- **Vulnerabilidades comunes en aplicaciones web (OWASP Top 10).**
- **Ataques de inyección SQL y cross-site scripting (XSS).**
- **Autenticación y autorización seguras.**
- **Seguridad en el desarrollo de software (SDLC).**
- **Pruebas mínimas de seguridad de aplicaciones web.**

Módulo 6: Marcos de Referencia de Ciberseguridad (3 horas)

Objetivo: El participante será capaz de comprender y aplicar los marcos de referencia de ciberseguridad más relevantes (ISO 27001, NIST, ISO 31000, ISO 22301) para establecer y mejorar el sistema de gestión de seguridad de la información de la organización.

TEMARIO

- **ISO 27001.**
- **NIST.**
- **ISO 31000**
- **ISO 22301.**

Módulo 7: Mejores Prácticas y Políticas de Seguridad (2 horas)

Objetivo: El participante será capaz de aplicar las mejores prácticas y políticas de seguridad cibernética, incluyendo la concientización y capacitación de usuarios, la realización de auditorías y la gestión de vulnerabilidades, para fortalecer la cultura de seguridad de la organización.

- **Políticas de seguridad.**
- **Concientización y capacitación en seguridad.**
- **Auditorías de ciberseguridad.**
- **Pentesting vs Análisis de Vulnerabilidades.**
- **Seguridad mínima para usuarios.**

¿A QUIÉN VA DIRIGIDO?

Este curso está dirigido a todo el personal que maneje datos sensibles en una organización.

DURACIÓN

18 horas
7 **módulos**

METODOLOGÍA

El curso se impartirá de forma presencial y/o en línea de forma interactiva. Se utilizará un lenguaje claro y preciso para los interesados.

ENTREGABLES

MATERIAL DE APOYO

- Presentaciones en formato digital.
- Resumen de los puntos clave de cada módulo.
- Estudios de caso y ejemplos prácticos.
- Guía de recursos adicionales sobre cada uno de los temas

INSTRUCTORES

- Expertos en Protección de Datos Personales y Ciberseguridad, con experiencia en la gestión de riesgos.
- Reconocimiento de la Secretaría del Trabajo

DC-3

BTechC

BUSINESS, TECHNOLOGY & CYBERSECURITY

CONTACTO