FORMACIÓN E-LEARNING

Curso Online de

Fundamentos de Ciberseguridad y manejo seguro de datos para empresas

Estrategias efectivas para identificar amenazas y gestionar datos de forma segura.

Iniciativas Empresariales
estrategias de formación

MANAGER BUSINESS SCHOOL

Tel. 900 670 400 - attcliente@iniciativasempresariales.edu.es
america.iniciativasempresariales.com
Sede Central: BARCELONA - MADRID

Llamada Whatsapp
(34) 601615098

Fundamentos de Ciberseguridad y manejo seguro de datos para empresas

Presentación

¡Descubra el curso que transformará su visión sobre la seguridad empresarial!
En un mundo donde la presencia digital define el éxito, proteger la información de su empresa no es una opción, es una necesidad. Este curso está diseñado para que entienda y adopte prácticas clave que blinden los activos digitales de su organización.

Con un enfoque práctico y adaptado a las necesidades actuales, aprenderá a identificar amenazas como el phishing, gestionar contraseñas de manera segura, proteger dispositivos y redes, y mucho más. Además, incluye ejemplos reales y estrategias probadas para que pueda aplicar los conocimientos adquiridos desde el primer día.
En la actualidad, las empresas que lideran el mercado no solo innovan, también priorizan la confianza de sus clientes al garantizar la protección de sus datos. No deje que su negocio quede atrás. ¡Únase y construya una cultura de seguridad que impulse su competitividad en esta era digital!

Descubra más sobre este curso y cómo puede transformar su empresa. ¡El momento de actuar es ahora!

La Formación E-learning

Los cursos online se han consolidado como un método educativo de éxito en la empresa ya que aportan flexibilidad al proceso de aprendizaje, permitiendo al alumno escoger los momentos más adecuados para su formación.
Con más de 35 años de experiencia en la formación de directivos y profesionales, Iniciativas Empresariales y la Manager Business School presentan sus cursos e-learning. Diseñados por profesionales en activo, expertos en las materias impartidas, son cursos de corta duración y eminentemente prácticos, orientados a ofrecer herramientas de análisis y ejecución de aplicación inmediata en el puesto de trabajo.

Nuestros cursos e-learning dan respuesta a las necesidades formativas de la empresa permitiendo:

1. La posibilidad de *escoger* el momento y lugar más adecuado para su formación.
2. *Interactuar* con otros estudiantes enriqueciendo la diversidad de visiones y opiniones y su aplicación en situaciones reales.
3. *Aumentar sus capacidades* y competencias en el puesto de trabajo en base al estudio de los casos reales planteados en el curso.
4. *Trabajar* con los recursos que ofrece el entorno on-line.

Tel. 900 670 400 - attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Fundamentos de Ciberseguridad y manejo seguro de datos para empresas

Objetivos del curso:

- Proporcionar los principios clave para proteger los datos y sistemas de su organización frente a amenazas cibernéticas y dominar así los fundamentos de la ciberseguridad empresarial.
- Explorar qué es la ciberseguridad, destacando su rol en la protección de sistemas, redes y datos frente a accesos no autorizados o ataques malintencionados.
- Identificar las principales amenazas y riesgos a los que se enfrentan las organizaciones, incluyendo malware, phishing y brechas de seguridad.
- Desarrollar habilidades esenciales para la protección de activos digitales: aprender a identificar riesgos, implementar estrategias seguras y fortalecer la infraestructura tecnológica de la empresa.
- Descubrir cómo empoderar a cada miembro de la organización para convertirse en un defensor activo de la información y de los activos digitales, fomentando una cultura de seguridad dentro de nuestro equipo.
- Conocer las mejores prácticas y herramientas para proteger dispositivos móviles y datos sensibles en el día a día de las operaciones empresariales, así como para configurar redes seguras con VPNs y firewalls.
- Abordar estrategias clave para seleccionar proveedores confiables, evaluar riesgos y aplicar planes de contingencia para mantener la operatividad ante imprevistos.
- Detallar las principales normas y marcos de referencia que establecen buenas prácticas para la gestión de la seguridad, su aplicación y la importancia de su cumplimiento a través de ejemplos prácticos.
- Prepararle para los desafíos de la era digital aprendiendo a implementar estrategias que no solo protejan a su empresa, sino que también la posicionen como un líder confiable en el mercado actual, donde la seguridad es sinónimo de éxito.

> “Un curso práctico para proteger contraseñas, detectar amenazas y asegurar sus dispositivos y redes”

Dirigido a:

Cualquier empresa que quiera construir una cultura de seguridad digital desde dentro, capacitando a sus equipos para reconocer riesgos, actuar con criterio y proteger sus activos con herramientas simples pero efectivas.

Tel. 900 670 400 - attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Fundamentos de Ciberseguridad y manejo seguro de datos para empresas

Estructura y Contenido del curso

El curso tiene una duración de 30 horas lectivas 100% online que se realizan a través de la plataforma e-learning de Iniciativas Empresariales que permite el acceso de forma rápida y fácil a todo el contenido:

Manual de Estudio
7 módulos de formación que contienen el temario que forma parte del curso y que ha sido elaborado por profesionales en activo expertos en la materia.

Material Complementario
En cada uno de los módulos que le ayudará en la comprensión de los temas tratados.

Ejercicios de aprendizaje y pruebas de autoevaluación
para la comprobación práctica de los conocimientos adquiridos.

Bibliografía y enlaces de lectura recomendados para completar la formación.

Metodología 100% E-learning

Aula Virtual *

Permite el acceso a los contenidos del curso desde cualquier dispositivo las 24 horas del día los 7 días de la semana.
En todos nuestros cursos es el alumno quien marca su ritmo de trabajo y estudio en función de sus necesidades y tiempo disponible.

Soporte Docente Personalizado

El alumno tendrá acceso a nuestro equipo docente que le dará soporte a lo largo de todo el curso resolviendo todas las dudas, tanto a nivel de contenidos como cuestiones técnicas y de seguimiento que se le puedan plantear.

* El alumno podrá descargarse la APP Moodle Mobile (disponible gratuitamente en Google Play para Android y la Apple Store para iOS) que le permitirá acceder a la plataforma desde cualquier dispositivo móvil y realizar el curso desde cualquier lugar y en cualquier momento.

Tel. 900 670 400 - attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Fundamentos de Ciberseguridad y manejo seguro de datos para empresas

Contenido del Curso

MÓDULO 1. Fundamentos de ciberseguridad

6 horas

La ciberseguridad es el conjunto de medidas y prácticas destinadas a proteger sistemas informáticos, redes y datos contra accesos no autorizados, ataques maliciosos y daños. En un mundo cada vez más digital, es esencial para salvaguardar la información personal y empresarial, mantener la confianza en los sistemas digitales y garantizar la continuidad de las operaciones.

1.1. ¿Qué es la ciberseguridad?

1.2. Riesgos y amenazas en el entorno de la oficina:
1.2.1. Principales amenazas cibernéticas en la oficina.
1.2.2. Buenas prácticas para mitigar riesgos en la oficina.

1.3. Buenas prácticas en ciberseguridad.

1.4. Revisión de conceptos.

MÓDULO 2. Protección básica de la información

4 horas

La información es un activo valioso tanto para los individuos como para las empresas. Con el crecimiento del uso de Internet, los riesgos de robo de datos y fraudes han aumentado considerablemente por lo que es fundamental conocer medidas básicas de seguridad para evitar ataques cibernéticos y proteger nuestra privacidad en el entorno digital. El uso de contraseñas fuertes, de la autenticación multifactorial y de gestores de contraseñas contribuye de forma significativa a la seguridad digital.

2.1. Contraseñas: las llaves de tu información.

2.2. Defensa contra malware:
2.2.1. Tipos de malware y sus características.
2.2.2. Estrategias de defensa contra malware.

2.3. Alerta contra el phishing:
2.3.1. Claves para protegerse del phishing.

2.4. Copias de seguridad: tu salvavidas digital
2.4.1. Regla 3-2-1 para copias de seguridad.
2.4.2. Estrategias adicionales para mejorar la seguridad de los backups.
2.4.3. Buenas prácticas para mantener copias de seguridad seguras.

2.5. Revisión de conceptos.

Tel. 900 670 400 - attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Fundamentos de Ciberseguridad y manejo seguro de datos para empresas

MÓDULO 3. Gestión y clasificación de la información

4 horas

La información es un activo valioso para cualquier organización. Su correcta gestión y clasificación es un pilar fundamental para garantizar la seguridad de los datos y el cumplimiento normativo dentro de una empresa. Implementar un sistema eficiente de clasificación de datos permite establecer controles de acceso adecuados, mitigar riesgos y asegurar la integridad de la información de la organización.

3.1. Clasificación de datos:
3.1.1. Clasificación de datos según sensibilidad.
3.1.2. Buenas prácticas para la gestión de datos.

3.2. Control de acceso:
3.2.1. Buenas prácticas para un control de acceso eficiente.

3.3. Capacitación y concienciación del personal:
3.3.1. Estrategias de capacitación.

3.4. Revisión de conceptos.

MÓDULO 4. Protección de dispositivos y redes

4 horas

La protección de dispositivos y redes es un aspecto crítico para salvaguardar la información y garantizar la continuidad operativa de las organizaciones. Con el crecimiento exponencial del uso de la tecnología y la digitalización de los procesos, los riesgos cibernéticos han aumentado significativamente, por lo que la protección de dispositivos y redes es un desafío continuo que requiere la combinación de medidas tecnológicas, procesos claros y capacitación constante.

4.1. Protección de dispositivos móviles:
4.1.1. Principales riesgos de seguridad en dispositivos móviles.
4.1.2. Medidas de protección y ejemplos de implementación.

4.2. Seguridad física de equipos.

4.3. Redes seguras:
4.3.1. Conceptos claves en seguridad de redes.
4.3.2. Principales medidas de seguridad en redes.

4.4. Revisión de conceptos.

Tel. 900 670 400 - attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Fundamentos de Ciberseguridad y manejo seguro de datos para empresas

MÓDULO 5. Gestión de proveedores y continuidad del negocio

4 horas

La gestión efectiva de proveedores y la continuidad del negocio (Business Continuity Planning - BCP) son elementos fundamentales para garantizar la operatividad y resiliencia de las organizaciones. Las interrupciones en la cadena de suministro o fallos en la infraestructura pueden tener consecuencias devastadoras si no se gestionan adecuadamente.

5.1. Selección y auditoría de proveedores:
5.1.1. Evaluación de seguridad de proveedores.
5.1.2. Cláusulas de seguridad en contratos.
5.1.3. Monitoreo y control de proveedores.

5.2. Plan de Continuidad del Negocio (BCP):
5.2.1. Creación y definición de protocolos.
5.2.2. Simulaciones y validaciones.
5.2.3. Estrategias de recuperación.

5.3. Iniciativas importantes para una gestión integral:
5.3.1. Estrategias para la gestión de riesgos de proveedores.
5.3.2. Integración tecnológica en la gestión de proveedores y continuidad del negocio.

5.4. Resumen y buenas prácticas.

5.5. Revisión de conceptos.

MÓDULO 6. Normas y estándares de seguridad

4 horas

La seguridad de la información es un pilar fundamental en el mundo digital. No se trata solo de proteger datos, sino también de garantizar la continuidad del negocio, la confianza de los clientes y el cumplimiento normativo. Existen diversas normas y marcos de referencia que establecen buenas prácticas para la gestión de la seguridad. Entre las más destacadas se encuentran la ISO/IEC 27001, NIST SP 800-53 y COBIT 2019.

6.1. Normas de seguridad:
6.1.1. ISO/IEC 27001.
6.1.2. COBIT 2019.
6.1.3. NIST SP 800-53.

6.2. Metodologías de control:
6.2.1. Principales metodologías de control de seguridad en la información.
6.2.2. Requisitos para implementar metodologías de control.

Tel. 900 670 400 - attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

6.3. ISO 27001.

6.4. COBIT 2019.

6.5. Comparación entre ISO 27001 y COBIT 2019.

6.6. Beneficios y desafíos.

6.7. Revisión de conceptos.

MÓDULO 7. Mejora continua y evaluación de resultados

4 horas

La seguridad de la información no es un proceso estático, debe actualizarse constantemente para adaptarse a nuevas amenazas y garantizar la protección de los datos. La mejora continua permite a las empresas anticiparse a riesgos, cumplir con todas las normativas y optimizar sus estrategias de ciberseguridad.

7.1. Auditorías de seguridad:
7.1.1. Definición y objetivos de las auditorías de seguridad.
7.1.2. Tipos de auditorías de seguridad.
7.1.3. El papel de la cultura organizacional en la mejora continua de seguridad.
7.1.4. Herramientas de auditoría de seguridad.

7.2. Actualización de políticas:
7.2.1. Metodologías para actualizar políticas.
7.2.2. Metodologías para la mejora continua y evaluación de resultados.

7.3. Capacitación y concienciación.

7.4. Casos reales.

7.5. Fomentar una cultura de seguridad proactiva:
7.5.1. Estrategias clave para una cultura de seguridad proactiva.
7.5.2. Evaluación de resultados en seguridad.

7.6. Medición del impacto de las estrategias de seguridad y productividad:
7.6.1. Metodologías para medir el impacto.
7.6.2. Análisis de productividad.
7.6.3. Inteligencia Artificial e Inteligencia de Negocios (BI) en la seguridad laboral.

7.7. Revisión de conceptos.

Fundamentos de Ciberseguridad y manejo seguro de datos para empresas

Autor

José Antonio Peña
Consultor en Tecnología de la Información e Inteligencia de Negocios con amplia experiencia transformando procesos empresariales mediante estrategias basadas en datos. Con una sólida formación académica, que incluye múltiples maestrías en Administración, Sistemas de Información y Business Intelligence, complementadas con certificaciones internacionales en COBIT, ISO 9001 y redes CISCO, ha liderado proyectos de reingeniería de procesos, de implementación de soluciones tecnológicas innovadoras, así como en el desarrollo de herramientas de análisis avanzado para diversas industrias, destacándose por su enfoque en la mejora continua y la toma de decisiones fundamentadas.

Titulación

Una vez finalizado el curso el alumno recibirá el diploma que acreditará el haber superado de forma satisfactoria todas las pruebas propuestas en el mismo.

MANAGER BUSINESS SCHOOL

DIPLOMA

Iniciativas Empresariales y la Manager Business School certifican que D. / Dña.

XXXXX XXXXXX XXXXXXXXXX

Ha superado satisfactoriamente el curso

FUNDAMENTOS DE CIBERSEGURIDAD Y MANEJO SEGURO DE DATOS PARA EMPRESAS

Habiendo demostrado el dominio de las materias impartidas mediante la superación de las pruebas de evaluación de las que consta el curso.

MANAGER BUSINESS SCHOOL