FORMACIÓN E-LEARNING

Curso Online de

Ciberseguridad práctica para Pymes con Inteligencia Artificial

Prompts, plantillas y checklists para proteger su negocio de amenazas.

CURSO BONIFICABLE

Iniciativas Empresariales
estrategias de formación

MANAGER BUSINESS SCHOOL

Tel. 900 670 400 - attcliente@iniciativasempresariales.com
www.iniciativasempresariales.com

BARCELONA - BILBAO - MADRID - SEVILLA - VALENCIA - ZARAGOZA

Ciberseguridad práctica para Pymes con Inteligencia Artificial

Presentación

Usar la Inteligencia Artificial (IA) de forma responsable refuerza la seguridad de su negocio. En este curso aprenderá a detectar amenazas a tiempo, dejar reglas claras y tomar mejores decisiones del día a día sin tecnicismos ni complejidad.

Está pensado para pymes y equipos no técnicos, con un enfoque paso a paso para aplicar desde mañana y reducir riesgos operativos:

- Fundamentos prácticos (CIA) para proteger lo valioso.
- Hábitos esenciales: MFA, actualizaciones y gestión de vulnerabilidades.
- Señales de ataques comunes y cómo responder.
- IA como acelerador: prioriza alertas y crea borradores de políticas que luego se revisan con criterio humano.
- Material listo para usar: ejemplos ficticios, plantillas y checklists.

Resultados: herramientas concretas, más confianza y opciones claras para proteger su negocio.

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.com - www.iniciativasempresariales.com

Ciberseguridad práctica para Pymes con Inteligencia Artificial

Objetivos del curso:

- Detectar amenazas a tiempo y reducir el riesgo operativo con un enfoque práctico para PYMES.
- Conocer y aplicar principios básicos de ciberseguridad apoyados en herramientas de Inteligencia Artificial (IA), utilizando un lenguaje claro, ejemplos cotidianos y actividades prácticas orientadas a pequeñas empresas.
- Comprender conceptos clave de ciberseguridad y cómo la IA puede apoyar en la protección digital.
- Aprender a usar principios básicos de análisis de riesgo y aplicar la IA para identificar amenazas.
- Comprender cómo la Inteligencia Artificial se convierte en una aliada estratégica al filtrar, contextualizar y priorizar CVE´s importantes para cada empresa.
- Mostrar cómo ChatGPT puede priorizar vulnerabilidades, clasificar riesgos y proponer planes de acción claros, así como crear incidentes simulados, redactar mensajes de phishing, construir escenarios de ransomware o simular respuestas de usuarios comprometidos.
- Practicar ejercicios de seguridad simulada y generar políticas internas de seguridad apoyadas por IA.
- Aprender a responder a incidentes usando la IA de forma eficiente y controlada.

> “Aprenda a detectar amenazas a tiempo y a priorizar vulnerabilidades con IA para responder mejor a incidentes de ciberseguridad en PYMES”

Dirigido a:

Pymes y equipos no técnicos que necesitan reducir riesgos operativos y mejorar su capacidad de prevención y respuesta sin depender de un gran equipo de ciberseguridad. Proporciona un enfoque paso a paso con plantillas, checklists y ejemplos para aplicar.
Especialmente útil para:

- Directivos y mandos intermedios que deben tomar decisiones rápidas ante incidentes y priorizar inversiones/acciones.
- Administración, operaciones, comercial, atención al cliente y RRHH donde el phishing y el error humano impactan directamente en el negocio.
- Responsables de IT/TIC con carga operativa alta que buscan priorizar CVE/vulnerabilidades y acelerar el triaje con apoyo de la Inteligencia Artificial.
- Equipos que necesitan simular ataques, evaluar desempeño y redactar/actualizar políticas internas de seguridad.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Ciberseguridad práctica para Pymes con Inteligencia Artificial

Estructura y Contenido del curso

El curso tiene una duración de 60 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
5 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.com - www.iniciativasempresariales.com

Ciberseguridad práctica para Pymes con Inteligencia Artificial

Contenido del Curso

MÓDULO 1. Fundamentos de ciberseguridad e Inteligencia Artificial

6 horas

1.1. ¿Qué es la ciberseguridad?
1.1.1. Conceptos clave: activos, amenazas, vulnerabilidades y riesgos.
1.1.2. Ejemplos cotidianos en pequeñas y medianas empresas.

1.2. Amenazas digitales actuales:
1.2.1. Phishing.
1.2.2. Malware y ransomware.
1.2.3. Ataques a dispositivos IoT.

1.3. El triángulo CIA: confidencialidad, integridad y disponibilidad
1.3.1. Definición de cada componente.
1.3.2. Ejemplos combinados.

1.4. Introducción a la Inteligencia Artificial:
1.4.1. Diferencias entre IA, Machine Learning y ChatGPT.
1.4.2. Analogía visual: reconocer gatos en fotos.

1.5. Cómo la IA fortalece la ciberseguridad:
1.5.1. Detección de anomalías y automatización de alertas.
1.5.2. Limitaciones: errores y sesgos de la IA.

MÓDULO 2. Análisis de riesgos y escenarios con IA

8 horas

Para decidir qué atender primero en seguridad, miramos el negocio con "lentes de riesgo": ¿qué puede salir mal?, ¿qué tan probable es?, ¿cuánto daño causaría? Con esa base, la Inteligencia Artificial nos ayuda a ver patrones entre miles de señales, priorizar lo urgente y convertir hallazgos en acciones concretas.

2.1. Cómo analizar riesgos en ciberseguridad:
2.1.1. Método básico: probabilidad × impacto.
2.1.2. Valoración de activos.

2.2. Amenazas digitales actuales:
2.2.1. Clasificación vs anomalía.
2.2.2. Casos prácticos: phishing y malware.

2.3. Fortalezas y debilidades de la IA en análisis de riesgos:

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

2.3.1. Fortalezas: escalabilidad y velocidad.
2.3.2. Debilidades: falsos positivos/negativos y sesgos.

2.4. Uso de ChatGPT para mejorar la seguridad:
2.4.1. Principios de prompt.
2.4.2. Buenas prácticas.

2.5. Tus primeros prompts de ciberseguridad:
2.5.1. Plantillas básicas.
2.5.2. Personalización por riesgo.

2.6. Tus primeros prompts de ciberseguridad:
2.6.1. Uso guiado.
2.6.2. Ajuste de controles recomendados.

MÓDULO 3. Detección de vulnerabilidades con IA

14 horas

La Inteligencia Artificial (IA) ha comenzado a transformar la manera en que las organizaciones identifican y gestionan vulnerabilidades en sus sistemas. A diferencia de los métodos tradicionales, que se basan en reglas fijas, listas de control o escáneres que requieren interpretación técnica, la IA tiene la capacidad de aprender patrones, analizar grandes volúmenes de datos en tiempo real y detectar señales débiles que pueden indicar riesgos potenciales.

3.1. Descubrimiento y parches de vulnerabilidades:
3.1.1. Métodos para identificar vulnerabilidades.
3.1.2. Aplicación y gestión de parches.

3.2. Escáneres básicos y herramientas abiertas:
3.2.1. Herramientas comunes de escaneo.
3.2.2. Ventajas y limitaciones del escaneo abierto.

3.3. Priorización de CVES con IA:
3.3.1. Evaluación automática de criticidad.
3.3.2. Prompts de ejemplo en ChatGPT.

3.4. Análisis de patrones de explotación:
3.4.1. Identificación de indicadores de compromiso (IoC).
3.4.2. Correlación de eventos con IA.

3.5. Privacidad y divulgación responsable del uso de IA:
3.5.1. Divulgación responsable de vulnerabilidades.
3.5.2. Limitaciones: errores y sesgos de la IA.

3.6. Virus, ransomware y secuestro de datos:

3.6.1. Divulgación responsable de vulnerabilidades.
3.6.2. Funcionamiento del ransomware.

3.7. Firmas vs comportamiento:
3.7.1. Detección basada en firmas.
3.7.2. Detección basada en comportamiento.

3.8. Modelos GPT y detección de software malicioso:
3.8.1. ¿Qué pueden hacer los modelos GPT en este contexto?

3.9. Limitaciones: evasión de modelos, falsos negativos
3.9.1. Evasión de modelos de detección.
3.9.2. Divulgación responsable de vulnerabilidades.

3.10. Casos de phishing avanzado:
3.10.1. ¿Qué es el phishing avanzado?

3.11. IA para clasificación de correos y análisis de URLS:
3.11.1. Clasificación de correos sospechosos con IA.
3.11.2. Análisis de URLS sospechosas con IA.

MÓDULO 4. Simulación de ataques y políticas con IA

16 horas

En el contexto de la ciberseguridad moderna, simular ataques y escenarios de riesgo es una de las estrategias más efectivas para preparar a una organización antes de que ocurra un incidente real. Las simulaciones permiten poner a prueba no solo las tecnologías disponibles, sino también a las personas y los procesos. Para una PYME, realizar simulaciones puede ser la forma más económica y accesible de mejorar su capacidad de respuesta y fortalecer su cultura de seguridad.

4.1. Simulaciones: tipos, diseño y análisis
4.1.1. ¿Por qué simular ataques?
4.1.2. Tipos de simulaciones aplicables a PYMES.
4.1.3. Diseño paso a paso de una simulación.

4.2. Generación automática de escenarios con IA:
4.2.1. ¿Qué significa generar escenarios con IA?

4.3. Evaluación del desempeño de equipos:
4.3.1. ¿Qué es "desempeño" en una simulación de ciberseguridad?

4.4. Políticas de seguridad:
4.4.1. ¿Qué es una política de seguridad y por qué es fundamental?
4.4.2. Cómo la IA (ChatGPT) ayuda a crear políticas personalizadas.

4.5. Recomendaciones automatizadas vía IA:

4.5.1. Ejemplos prácticos de uso en PYMES.

4.6. Virus, ransomware y secuestro de datos:
4.6.1. Riesgos del uso no responsable de IA en ciberseguridad.
4.6.2. Buenas prácticas para un uso responsable.

MÓDULO 5. Respuesta y automatización de seguridad con IA

16 horas

En un entorno digital cada vez más complejo, las empresas enfrentan múltiples amenazas cibernéticas que pueden surgir en cualquier momento. Desde intentos de acceso no autorizados hasta correos maliciosos o actividad anómala en sistemas, la capacidad de responder rápidamente y con precisión se ha convertido en una ventaja competitiva esencial.
Tradicionalmente, esta respuesta ha estado en manos de equipos técnicos, muchas veces sobrecargados, o incluso inexistentes en el caso de pequeñas y medianas empresas. Sin embargo, gracias a la Inteligencia Artificial, es posible automatizar parte de estas tareas, optimizando tiempos, recursos y mejorando la efectividad general ante incidentes.

5.1. Clasificación automática de alertas:
5.1.1. ¿Por qué simular ataques?
5.1.2. Cómo implementar la clasificación automática en una PYME.

5.2. Evaluación de riesgos con semáforo:
5.2.1. Implementación práctica del modelo de semáforo en una PYME.

5.3. Acciones automáticas: bloqueo, notificaciones, reportes
5.3.1. Implementación práctica de acciones automáticas en una PYME.

5.4. Mejora continua: pruebas de prompts, ajustes
5.4.1. Cómo realizar pruebas y ajustes de prompts en una PYME.

5.5. Roles: analista vs gerente
5.5.1. Cómo adaptar prompts según el rol del usuario.

5.6. Diseño de agente digital de seguridad:
5.6.1. Entrenamiento y configuración paso a paso.

Ciberseguridad práctica para Pymes con Inteligencia Artificial

Autor

Christopher Delgado
Ingeniero en Conectividad y Redes con amplia experiencia en Ciberseguridad, Continuidad Operacional, Auditoría TI, Inteligencia Artificial y Gestión de Incidentes. Amplio dominio de entornos híbridos (Cloud & On-Premise), liderazgo en proyectos de seguridad y ejecución de pruebas de hacking ético.

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.