vuela | Junta de Andalucía

La importancia de la concienciación del empleado frente a la ciberdelincuencia

Curso eLearning	Nivel Intermedio	10h	22/05 al 27/06	De 25 a 45 personas

¿QUÉ VAS A APRENDER?

Los empleados son el primer eslabón en la cadena de seguridad y es crucial que estén informados y capacitados para proteger la información de la empresa. Con este curso, se pretende concienciar a las pymes de todos los posibles riesgos y consecuencias que tiene un ciberataque hacia su organización.

Este conocimiento puede aplicarse tanto en el ámbito personal como profesional.

OBJETIVOS:

Identificar los diferentes tipos de ciberdelincuencia: Los participantes deben ser capaces de distinguir los diferentes tipos de ciberdelincuencia, así como de entender cómo los ciberdelincuentes operan y las herramientas que utilizan para llevar a cabo sus ataques. Esto les permitirá estar más alerta y prevenir posibles ataques.

CONTENIDOS:

Módulo 1: ¿Qué es la ciberdelincuencia? (2 horas)

1. ¿Qué es la ciberdelincuencia?
2. Estadísticas y tendencia actuales de la ciberdelincuencia en el sector pyme.
3. Herramientas tecnológicas usadas por los ciberdelincuentes.
4. Impacto de la ciberdelincuencia relativos a la privacidad, reputación y pérdidas económicas.
5. La informática forense. ¿Cómo debes actuar en caso de un ciberataque?

Actividad → Se planteará una serie de escenarios de ataques y se planteará al alumno la forma correcta de preservar evidencias para que puedan ser aceptadas legalmente.

OBJETIVOS:

Comprender los motivos de los ciberdelincuentes: Los participantes deben aprender sobre las motivaciones detrás de la ciberdelincuencia, lo que les permitirá tener una visión más completa de las posibles amenazas. Deben ser capaces de identificar las motivaciones que podrían llevar a un ciberdelincuente a atacar a una empresa o a un individuo, como el dinero, la información confidencial, la notoriedad, entre otros.

CONTENIDOS:

Módulo 2: ¿Qué motiva al ciberdelincuente? (1 hora)

1. ¿Por qué se convierte una persona en un ciberdelincuente?
2. Motivaciones económicas.
3. Motivaciones políticas.
4. Motivaciones sociales.

Actividad → Estudio de una serie de ciberdelitos que han tenido relevancia mediática recientemente con el objetivo de determinar las causas que incitaron a cometerlos.

OBJETIVOS:

Detectar malas prácticas comunes: Los participantes deben ser capaces de identificar y detectar las malas prácticas comunes que podrían poner en peligro la seguridad de su empresa y su información. Estas prácticas pueden incluir el uso de contraseñas débiles, la apertura de correos electrónicos sospechosos, la instalación de software sin autorización, entre otros.

CONTENIDOS:

Módulo 3: Determinación de malas prácticas habituales. (5 horas)

1. No valorar o conocer al antivirus.
2. No actualizar los sistemas.
3. Confiar en todo el mundo.
4. Realizar un uso higiénico de la navegación por Internet.

Actividad → Exponer una serie de actividades realizadas por un usuario y determinar la mala práctica que se está cometiendo.

OBJETIVOS:

Realizar prácticas de concienciación: Los participantes deben ser capaces de aplicar lo aprendido en los módulos anteriores para diseñar e implementar prácticas de concienciación frente a un ataque en una pyme.

CONTENIDOS:

Módulo 4: Realización de prácticas de concienciación (2 horas)

1. Identificación de ataques de ingeniería social.
2. Ataque simulado con mensaje al usuario final.
3. Determinación de debilidades y aplicación de medidas correctivas.

Actividad → El alumno deberá identificar correctamente el tipo de ataque analizando imágenes de ataques cibernéticos reales.

¿A QUIÉN ESTÁ DIRIGIDO?

Personal directivo y trabajadores de las pymes de Andalucía.

REQUISITOS DE ACCESO:

Podrán participar los trabajadores, directivos, socios y administradores de las pymes con sede social, delegación o establecimiento de producción o prestación de servicios en Andalucía.

- Que sea una pyme o autónomo.
- Estricto orden de llegada hasta completar plazas.

CONOCIMIENTOS MÍNIMOS REQUERIDOS:

- Acceso a Internet
- Competencias digitales básicas.

EQUIPO DOCENTE

Antonio Salazar Graván

Ingeniero Técnico Informático por la Universidad de Cádiz, MCT de Microsoft desde 2012.

Especialista en Ciberseguridad e infraestructuras con más de 20 años de experiencia en formación y consultoría

https://www.linkedin.com/in/antonio-salazar-gravan/

.

CALENDARIO:

- **Fecha inicio del curso:** 22/05/2023
- **Fecha fin del curso:** 27/06/2023.

EVALUACIÓN:

Obligatorio para obtener el certificado:

- [60%] La propia consulta de materiales.
- [20%] Pruebas tipo Test (individual).

No es obligatorio pero sí muy recomendable:

- [10%] Grado de participación. Se evaluará la participación en los foros y colaboración del alumno durante todo el proceso formativo así como la realización de actividades.
- [10%] Consulta de recursos adicionales.

CERTIFICADO

Una vez superadas todas las evaluaciones de los módulos del curso y habiendo asistido al número mínimo de clases exigido, podrás obtener la certificación.

El certificado se emitirá digitalmente en formato pdf incluyendo la siguiente información:

- Datos del alumno.
- Datos del curso: título, fecha de impartición, duración, contenidos impartidos.
- Sello y firma digitalizada de la empresa impartidora del curso. El certificado no lleva firma digital ni sello/firma de la Junta de Andalucía

Ten en cuenta que estos cursos no tienen validez académica ni acreditación de créditos universitarios.

OTRAS CUESTIONES DE INTERÉS

Una posible orientación al tiempo dedicado al estudio, lectura y visualización del contenido sería la siguiente:

- Tiempo de consulta de contenidos y vídeos: 7 horas.
- Tiempo de realización de actividades: 1 hora.
- Tiempo de realización de exámenes: 1,5 horas.
- Tiempo de consulta en foros e interacción con los compañeros: 0,5 horas.

De todas formas y al tratarse de un curso en línea, cada alumno podrá seguir su propio ritmo de aprendizaje siempre y cuando cumpla con los criterios mínimos de evaluación para la obtención del certificado de formación.