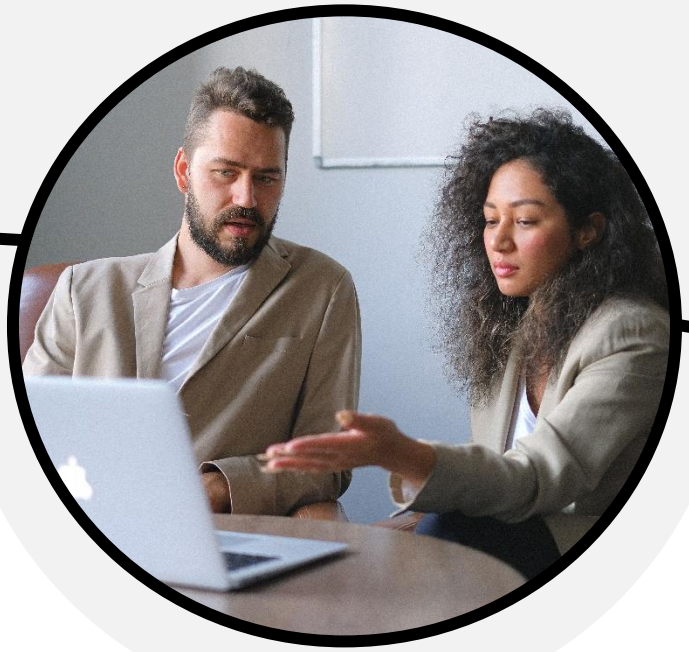
vuela | Junta de Andalucía

Conceptos de ciberseguridad que debes tener en cuenta en tu pyme



Curso MOOC	Nivel Intermedio	20h	25/09 al 03/11	Mínimo de 100 plazas

¿QUÉ VAS A APRENDER?

A través de este MOOC de ciberseguridad, el participante comprenderá las amenazas informáticas y cómo proteger sus datos en línea. Por medio de los distintos vídeos, lecturas y ejercicios prácticos, los participantes pueden adquirir habilidades de prevención del malware, asegurar sus dispositivos y evaluar los principales riesgos cibernéticos.

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

OBJETIVOS:

Conocer los conceptos básicos de seguridad digital: Esta competencia implica que los estudiantes comprendan los términos y conceptos clave de la seguridad digital, tales como: tipos de ataques cibernéticos, virus, gusanos, troyanos, phishing, spam, entre otros. Además, deberán comprender las implicaciones y consecuencias de la falta de seguridad digital, y cómo puede afectar tanto a los individuos como a las organizaciones.

CONTENIDOS:

Módulo 1: Conceptos básicos de Seguridad Digital (4 horas)

1. ¿Qué conozco sobre Ciberseguridad? Conceptos básicos
2. La actualización de los sistemas y los empleados, dos puntos débiles de mi organización
3. ¿Guardo mi información en lugar seguro?
4. Conclusiones

Recursos del módulo:

- Infografía
- Glosario de Términos

Actividad → Corrección entre pares. Se planteará un escenario ficticio de una pyme que describirá los procesos de negocio más importantes y cómo se almacena la información asociada a ellos. El alumno deberá detectar las debilidades del planteamiento y proponer soluciones que mejoren la postura de seguridad.

OBJETIVOS:

Identificar y resolver problemas de malware e ingeniería social: Esta competencia implica que los estudiantes sepan cómo identificar, prevenir y solucionar problemas relacionados con el malware y la ingeniería social. Los estudiantes deberán saber cómo detectar posibles ataques de malware y cómo tomar medidas para proteger sus dispositivos y redes. Además, deberán comprender cómo los atacantes utilizan la ingeniería social para engañar a los usuarios y cómo pueden protegerse contra este tipo de ataques.

CONTENIDOS:

Módulo 2: ¿Qué hacer si tengo malware? ¿Qué es la ingeniería social? (6 horas)

1. Conceptos y términos básicos sobre el malware
2. Herramientas de protección: Antivirus, cortafuegos e inspección del tráfico
3. ¿Qué es la ingeniería social? ¿Dónde se encuentra el punto débil en la seguridad de tu empresa?
4. ¿Qué es el Phishing? ¿Comprendo mi barra de direcciones?
5. Conclusiones

Recursos del módulo:

- Infografía
- Glosario de Términos

Actividad → Corrección entre pares. Se plantearán escenarios que simulan la actividad que un empleado realiza en su día a día relativa al uso de herramientas de comunicación. El alumno deberá identificar correctamente aquellos que se correspondan con ataques de Ingeniería Social.

OBJETIVOS:

Asegurar dispositivos móviles y redes WIFI: Esta competencia implica que los estudiantes sepan cómo proteger sus dispositivos móviles y redes WIFI contra posibles amenazas de seguridad. Deberán comprender cómo asegurar su conexión a Internet, cómo evitar conexiones no autorizadas y cómo proteger sus datos personales.

CONTENIDOS:

Módulo 3: Asegura tus dispositivos móviles y redes WIFI (4 horas)

1. ¿Qué debo saber sobre protocolos de seguridad inalámbrica más comunes?
2. Uso de redes WIFI públicas, riesgos y consecuencias.
3. Aislar el tráfico de mi organización. He perdido mi móvil ¿Qué debo hacer?
4. ¿Debo instalar un antivirus en mi móvil?
5.

Recursos del módulo:

- Infografía
- Glosario de Términos

Actividad → Corrección entre pares. Se plantearán diversos escenarios relativos a los contenidos de la unidad. Para cada uno de ellos, el alumno deberá describir cuál es el problema de seguridad al que se enfrenta y determinar cuál es la mejor práctica.

OBJETIVOS:

Evaluar los principales riesgos en ciberseguridad: Esta competencia implica que los estudiantes sepan cómo evaluar los principales riesgos en ciberseguridad para, aplicando las técnicas, prevenirlos y mitigarlos.

CONTENIDOS:

Módulo 4: Aprender a evaluar los principales riesgos en ciberseguridad (6 horas)

1. ¿Cómo articular la seguridad de la información en la empresa?
2. El Sistema de Gestión de la Seguridad de la Información (SGSI) y sus ventajas
3. Análisis y gestión de riesgos en las organizaciones. Entendiendo activos, amenazas, salvaguardas, impacto y riesgo

Recursos del módulo:

- Infografía
- Glosario de Términos

Actividad → Corrección entre pares. Partiendo de un caso de uso de una pyme modelo, en el que se describen los procesos de negocio y las herramientas informáticas que se emplean, el alumno realizará un análisis de riesgo sobre los activos de información y aportará las medidas recomendadas para que el impacto sobre dichos activos sea aceptable

¿A QUIÉN ESTÁ DIRIGIDO?

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

- Personas que trabajen en pymes o en régimen de autónomo.
- Estricto orden de llegada.

En caso de que no se cubran las plazas mínimas del curso por el público destinatario, Andalucía Vuela dará paso a las inscripciones, por estricto orden de llegada, de otros perfiles (personas desempleadas, trabajadoras en administración pública, grandes empresas, etc).

REQUISITOS DE ACCESO:

Al ser un curso masivo, este apartado no es requerido, basta con que se inscriban y cumplan con el perfil de las personas destinatarias.

- Plazo de apertura de inscripciones: 17/07
- Plazo de cierre: 15/09

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:**
  25/09/2023
- **Fecha fin del curso:**
  10/11/2023.

EVALUACIÓN: (Sólo para acciones formativas en las que sea necesario)

Obligatorio para obtener el certificado:

- [60%] La propia consulta de materiales.
- [15%] Pruebas tipo Test (individual).

No es obligatorio pero sí muy recomendable:

- [15%] Grado de participación. Se evaluará la participación en los foros y colaboración del alumno durante todo el proceso formativo así como la evaluación entre pares. El trabajo cooperativo no sólo consistirá en generar conocimiento colectivo. También se establecerán dentro de las rúbricas, apartados donde tendrán que analizar y evaluar el trabajo entre compañeros.
- [10%] Consulta de recursos adicionales.

CERTIFICADO (Sólo para acciones formativas en las que sea necesario. Cambiar si procede)

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 SEGÚN LA TIPOLOGÍA DE AAFF:

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

- Tiempo de consulta de contenidos y vídeos: 15 horas.
- Tiempo de realización de actividades: 2 horas.
- Tiempo de realización de exámenes: 1,5 horas.
- Tiempo de consulta en foros e interacción con los compañeros: 1,5 horas.

De todas formas y al tratarse de un curso abierto y 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.