vuela | Junta de Andalucía

Sistemas de autenticación y medidas de refuerzo

Curso eLearning

Nivel Intermedio

10h

08/06 al 19/07

De 25 a 45 personas

¿QUÉ VAS A APRENDER?

El curso tiene como objetivo proporcionar a los participantes las habilidades necesarias para diseñar y mantener sistemas de autenticación seguros y eficaces en el entorno de una pequeña y mediana empresa. Los participantes aprenderán sobre las últimas tecnologías de autenticación, así como sobre las medidas de refuerzo necesarias para prevenir ataques de seguridad y proteger la información empresarial sensible.

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

OBJETIVOS:

Buenas prácticas sobre el uso de contraseñas: Los participantes deben ser capaces de distinguir entre una contraseña débil y otra fuerte.

Comprenderán por qué no deben utilizar la misma contraseña y los peligros del procedimiento de recuperación cuando se usan preguntas personales.

CONTENIDOS:

Módulo 1: Buenas prácticas sobre el uso de contraseñas (2 horas)

1. La importancia de una contraseña robusta frente al ataque de diccionario.
2. El peligro de la reutilización de la contraseña.
3. Trucos y reglas útiles para crear contraseñas fuertes.
4. Peligros en el procedimiento de recuperación de una contraseña olvidada.

Actividad → El alumno deberá crear un informe que identifique las malas prácticas que comete relacionadas con las contraseñas. Deberá explicar las medidas correctoras que debe aplicar.

OBJETIVOS:

Gestores de contraseña: Los participantes deben entender que usar contraseñas débiles o reutilizarlas en diferentes sitios webs es peligroso. Para ello deberá aprender a usar los gestores de contraseñas.

CONTENIDOS:

Módulo 2: Gestores de contraseña (3 horas)

1. ¿Qué es un gestor de contraseña y por qué me conviene usarlo?
2. Gestor de contraseñas del navegador Edge.
3. Gestor de contraseñas del navegador Chrome.
4. Otros gestores de contraseñas.

Actividad → El alumno describirá los pasos necesarios para habilitar el gestor de contraseñas de un navegado determinado.

OBJETIVOS:

Entender el principio del consentimiento en la autorización: Los participantes deben ser capaces de identificar cuándo una página web le está pidiendo el consentimiento.

También deberá concienciarse sobre el alcance de ese consentimiento: Acceder a información personal, leer el correo, acceder a sus archivos, etc.

CONTENIDOS:

Módulo 3: El consentimiento en la autorización. (3 horas)

1. ¿Cómo funciona la autorización moderna?
2. Usar autorización moderna en sitios como Google, Facebook o Twitter.
3. Cómo podrían engañarte en la autorización moderna.

Actividad → Para los sitios web que se planteen, el alumno deberá identificar si se está usando la autorización moderna o la clásica.

OBJETIVOS:

Factores adicionales de autenticación: Los participantes deben ser capaces de entender que proteger sus activos solo con una contraseña es insuficiente.

Conocerán los factores adicionales a su disposición, en especial los biométricos y su uso en la tríada de autenticación.

CONTENIDOS:

Módulo 4: Factores adicionales de autenticación (2 horas)

1. ¿Qué son los factores de autenticación?
2. Por qué son tan importantes en tu actividad diaria.
3. Cómo habilitar factores adicionales en tu banco, Google, Facebook, etc.

Actividad → Se propondrá al alumno el estudio de los pasos a realizar para activar un factor de autenticación adicional a la contraseña en un sitio web de ejemplo.

¿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:**
  23/06/2023
- **Fecha fin del curso:**
  19/07/2023.

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.

Es obligatoria la entrega de la Declaración Responsable firmada electrónicamente para la obtención del certificado del curso.

OTRAS CUESTIONES DE INTERÉS SEGÚN LA TIPOLOGÍA DE ACCIÓN FORMATIVA:

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