Denominación: Ciberseguridad: La Ingeniería Social. Protégete y Protege a los Tuyos Frente a las Nuevas Amenazas.

Horas:	05:00		
Clave:	HU26PF-PHP5	**Año:**	2026
Órgano gestor:	SERVICIO DE ADMINISTRACIÓN PÚBLICA DE LA D.T. DE HUELVA	**Cod. Sirhus**	L5232
Programa:	Perfeccionamiento Horizontal	**Plazas:**	50
Modalidad:	PRESENCIAL	**Evaluación:**	No
Personas destinatarias:	Personal de la Administración General de la Junta de Andalucía, independientemente del puesto que ejerza, con especial atención a quienes manejen información sensible o que tenga especial valor para la Junta de Andalucía.		

Datos de Celebración

Lugar de celebración:	DELEGACIÓN DEL GOBIERNO, SALÓN DE ACTOS (PRIMERA PLANTA), C/ Sanlúcar de Barrameda, 3, 21001 Huelva.		
Provincia:	HUELVA	**Fecha inicio:**	17/03/2026
Horario:	17/03/2026 9:00 - 14:00	**Fecha fin:**	17/03/2026

IMPORTANTE: UNA VEZ RECIBIDO EL CORREO DE ADMISIÓN AL CURSO, LAS PERSONAS SELECCIONADAS DEBEN CONFIRMAR SU ASISTENCIA (O, EN SU CASO, LA RENUNCIA JUSTIFICADA AL MISMO) LO ANTES POSIBLE, MEDIANTE UN CORREO ELECTRÓNICO DIRIGIDO A: formacion.dthuelva.cjalfp@juntadeandalucia.es

1.- Cuando una persona seleccionada para una acción formativa NO PUEDA ASISTIR, deberá comunicarlo por escrito, acompañando justificación, lo más pronto posible, antes del inicio del curso o en el momento en que sobrevenga la causa, a fin de cubrir su vacante con otras solicitudes. En caso contrario, no será seleccionada en la siguiente convocatoria, salvo que acredite una causa justificada de renuncia y la comunique debidamente.

2.- CERTIFICACIÓN DE ASISTENCIA: las personas admitidas al curso deben asistir al menos al 80 % de las horas presenciales y realizar las actividades que proponga el equipo docente durante la impartición. CERTIFICACIÓN DE APROVECHAMIENTO: además de cumplir lo anterior, tendrá que superar la prueba de evaluación correspondiente.

3.- Finalizado el curso recibirás un correo electrónico con la ENCUESTA DE VALORACIÓN de la acción formativa, teniendo 7 DÍAS para contestarla. Os rogamos vuestra colaboración, ya que vuestras respuestas permiten al IAAP evaluar la calidad de la acción formativa con el objetivo de lograr la excelencia que queremos para vuestra formación.

Equipo Docente: Eduardo Antón Santa María. Gestión de Servicios Tecnológicos. Agencia Digital de Andalucía (Consejería de Industria, Energía y Minas)

Objetivos:

Como objetivo general: Incrementar el nivel de concienciación, sensibilización y capacitación en relación a la Ciberseguridad en las personas participantes.

Como objetivo más específico: Preparar al personal asistente para hacer frente a los intentos de manipulación que utilizan los ciberdelincuentes en sus ataques.

La práctica totalidad de los ataques incluyen, en sus primeras fases, el intento de engañar a personas para que sean las propias víctimas quienes realicen acciones como permitir que el atacante acceda a sus equipos, proporcionar contraseñas a terceros o instalar programas maliciosos.

Para evitar poner en riesgo nuestra información, nuestros servicios y nuestros recursos es necesario conocer estos ataques y por qué funcionan, así como prestarles la atención que merecen, otorgarles la importancia que tienen y saber cómo hacerles frente.

Contenido:

UD 1. El riesgo.
¿ Concepto de riesgo y su relación con la ciberseguridad.
¿ Problemas que impiden una adecuada evaluación del riesgo que corremos.
UD 2. Técnicas utilizadas por los atacantes.
¿ Condiciones del ser humano que son aprovechadas por los atacantes.
¿ Las fases de un ataque.
¿ Ejemplos de ataques comunes.
¿ Canales a través de los que se realizan los ataques: correos, SMS, telefonía, etc.
UD 3. El PHISHING.
¿ Técnicas para reconocer direcciones de Internet fraudulentas.
¿ Uso de HTTPS frente a HTTP.
¿ Estructura de una URL.
¿ Formas en las que se generan URLs fraudulentas cómo reconocerlas.
¿ Recomendaciones para el uso de URLs proporcionadas por terceros.
UD 4. La Ingeniería Social en el mundo físico.
¿ Condiciones y situaciones que hacen posible que tengan éxito los intentos de manipulación presenciales.
¿ Técnicas comunes usadas por los atacantes en la interacción física.
UD 5. Tendencias de la Ingeniería Social.
¿ El timo del CEO.
¿ Uso de la IA para generar imágenes, video y audio que pueden ser usados para fines fraudulentos.
¿ Los deep fakes
Cómo defendernos de la Ingeniería Social.
¿ Detección de intentos de engaño, fraude y manipulación.
¿ Control de la información que se hace pública.
¿ Establecer normas de funcionamiento. Y seguirlas.
¿ Comprobaciones a realizar ante comunicaciones sospechosas.
¿ Forma de actuar ante una comunicación sospechosa.
¿ Actitudes a practicar.
¿ Medidas técnicas.
¿ Comunicación y reporte.