Junta de Andalucía

Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa
Instituto de Emergencias y Seguridad Pública de Andalucía (IESPA)

CURSO CONCIENCIACIÓN SOBRE CIBERSEGURIDAD

GUÍA DIDÁCTICA

Carretera Isla Mayor, km 3'5, 41849 Aznalcázar (Sevilla)
iespa.cpidssa@juntadeandalucia.es
formacion.iespa.cpidssa@juntadeandalucia.es

C U R S O: "CONCIENCIACIÓN SOBRE CIBERSEGURIDAD"

C O N T E N I D O

I. FINALIDAD DEL CURSO

II. OBJETIVOS

III. ALUMNADO

IV. ESTRUCTURA. METODOLOGÍA.TEMPORALIZACIÓN

V. CONTENIDOS CURRICULARES

VI. EVALUACIÓN

VII. PROFESORADO

I.- FINALIDAD DEL CURSO

Adquirir conocimientos acerca de la ciberseguridad y presentarla como el conjunto de medidas que debe poner en práctica el usuario de tecnologías de la información para proteger sus datos, intimidad y equipos, frente a ataques maliciosos, fraudes o uso delictivo de redes sociales.

La ciberseguridad debe estar presente en todos los ámbitos de la vida y su aplicación es fundamental para la protección del ciudadano frente a amenazas como la pornografía infantil, estafas, injurias y ataques a la disponibilidad de la información que se realizan por medio del uso de dispositivos informáticos y redes sociales.

II.- OBJETIVOS

- Aclarar conceptos y terminología de uso común en la ciberseguridad, como la amenaza, el riesgo, la vulnerabilidad, antivirus, firewall, etc.

- Describir las buenas prácticas que deben contemplarse a la hora de usar herramientas informáticas y de comunicación, ya sea en el puesto de trabajo o en domicilio particular.

- Conocer un conjunto de acciones delictivas que no están basadas en la presencia de vulnerabilidades en los dispositivos, sino en el uso de las redes sociales con fines delictivos (*ciberbullying*, *grooming*, *sexting*, *doxing* o el delito de injurias y odio), además del panorama de ciberamenazas que está por venir.

- Entender la metodología a seguir a la hora de conservar la evidencia en el caso de ser víctimas de un ataque o delito informático para que éstas adquieran valor legal como pruebas en un procedimiento judicial.

III.- ALUMNADO

Personal de los Cuerpos de la Policía Local de Andalucía, del colectivo de Vigilantes Municipales, de la Unidad del Cuerpo Nacional de Policía Adscrita a la Comunidad Autónoma de Andalucía, de Prevención y Extinción de Incendios y Salvamento, del personal de Protección Civil, así como el voluntario-a de las Agrupaciones Locales del Voluntariado de Protección Civil.

IV.- ESTRUCTURA. METODOLOGÍA.TEMPORALIZACIÓN

Curso de Formación en Semipresencial, a celebrar entre el 16 de mayo y el 6 de junio de 2023, con una duración de 25 horas lectivas.

La jornada presencial se impartirá en la sede del Instituto de Emergencias y Seguridad Pública de Andalucía (IESPA) , sita en Ctra. Isla Mayor, Km. 3.5 , Aznalcázar (Sevilla). La formación en red se desarrollará en la Plataforma de Teleformación del IESPA.

Formación presencial: 5 horas lectivas el día 16 de mayo.

Formación en red: 20 horas lectivas.

V.- CONTENIDOS CURRICULARES

Las materias a impartir en la formación presencial se dividirá como sigue:

Módulo I: Conceptos y terminología de ciberseguridad.

i. El delito informático y la ciberseguridad.
ii. Amenaza y riesgo.
iii. Ataque a un sistema informático o dispositivo que presenta vulnerabilidades.
iv. El antivirus.
v. El firewall o cortafuegos.
vi. Demostración práctica de un ataque que hace uso de una vulnerabilidad.

Módulo II: Las buenas (y malas) prácticas.

i. Cómo usar un navegador de forma segura.
ii. Medios de pago seguros. Tarjetas virtuales, PayPal, etc.
iii. Por qué es peligroso un correo electrónico con un archivo adjunto.
iv. Por qué es peligroso un correo electrónico que contiene un enlace de Internet.
v. El riesgo de compartir la información por medio de enlaces.

vi. ¿Qué es el Malware? Virus, troyanos, gusanos.

vii. Ataque a la disponibilidad de la información: Denegaciones de servicio y ransomware.

viii. Cómo elegir e instalar un antivirus.

Módulo III: Uso de redes sociales con fines delictivos.

i. La red social y su finalidad.

ii. El ciberacoso (*ciberbullying*)

iii. El acoso sexual por redes sociales (*Grooming*)

iv. Compartir contenido erótico o sexual en redes sociales (*Sexting*)

v. Publicación en redes sociales de información personal (*Doxing*)

vi. Publicaciones en redes sociales relativas al delito de odio e injurias.

vii. El control del contenido en redes sociales.

viii. Las aplicaciones de control parental.

ix. Demostración práctica del control de contenidos en redes sociales.

x. Demostración práctica del uso de una aplicación de control parental para proteger a los menores.

Módulo IV: La ingeniería social o el arte de engañar al usuario.

i. ¿Qué es la Ingeniería Social?

ii. Ataques de Phishing por correo electrónico, SMS, WhatsApp…

iii. Estafas y suplantación de identidad: el Pretexting y su aplicación en el timo del CEO.

iv. Fake News y Scams.

v. Qué hacer con un USB que me he encontrado en el suelo: ataque de tipo Baiting.

vi. Riesgos asociados a la tarjeta SIM: el duplicado de la SIM.

vii. Amenazas y alarmas falsas: scareware.

viii. Acceso físico a las instalaciones mediante ingeniería social: tailgaiting.

ix. Estafas telefónicas o solicitación: vishing.

Módulo V: Las redes WiFi y sus amenazas.

i. ¿Cómo verificar si mi dispositivo se conecta al router usando un protocolo seguro?

ii. El Protocolo WPA-2.

iii. Suplantación del punto de acceso: la técnica del hombre en medio (Man in the Middle).

iv. Riesgos potenciales al conectar a redes WiFi públicas.

v. Por qué el uso de la conexión 4G o 5G es el método preferido frente a WiFis públicas.

vi. Demostración: conocer si se está usando WiFi o 4G en el teléfono y buenas prácticas.

vii. Demostración: aplicar seguridad al router.

Módulo VI: Conservación de la evidencia.

i. ¿Qué es la Informática Forense?

ii. ¿Debo apagar el equipo para que se conserve la evidencia?

iii. Ejemplo práctico: contacta con las autoridades. ¿Cómo proceder si eres víctima de un ciberdelito?

iv. Si eres empresa: delega en el profesional. El rol del perito forense informático como investigador.

Módulo VII: Nuevas amenazas

v. IoT/OT/ICS: internet en todas partes, fábricas conectadas.

vi. Comunicaciones ultrarrápidas y sin latencia: ¿una ventaja?

vii. Drones, vehículos autónomos: ¡esto se mueve!

viii. Actores de amenazas avanzados: el teatro se llena.

ix. Computación cuántica: ya nada es lo que era.

Las materias a impartir en la formación en red se distribuirán en distintas unidades para alcanzar los objetivos específicos del curso:

Unidad 1. Seguridad electrónica

1.1 Clasificación de las medidas de seguridad.

1.2 Confidencialidad, integridad y disponibilidad.

1.3 Ataques: Clasificación.

Unidad 2. La ciberseguridad

2.1 ¿Qué es la ciberseguridad?

2.2 Amenazas, vulnerabilidades y riesgos.

2.3 Clasificación de las amenazas

2.4 Seguridad informática en casa y en la empresa.

Unidad 3. Software dañino

3. 1 Tipología del código malicioso

3.2 Técnicas de ataque que utilizan código malicioso

3.3 Medidas de protección contra el software dañino

Unidad 4. Seguridad en redes Wireless

4.1 Redes inalámbricas de área local

4.2 Redes 1G/2G/3G/4G/5G

4.3 Seguridad: autenticación y contraseñas

Unidad 5. Sistemas de seguridad informática

5.1 Protección del sistema operativo

5.2 Protección frente a código malicioso

IX.- EVALUACIÓN

El Instituto expedirá diploma de asistencia al alumnado que asista a la formación presencial, además de participar en los foros y en las actividades que se planteen en la Plataforma. El alumnado que desee obtener certificado de aprovechamiento deberá superar las pruebas de evaluación del curso, consistente en un examen test al que se exigirá un 65 % de acierto conforme a lo establecido en la Orden de la Consejería de Gobernación de 18 de marzo de 1996, por la que se establecen las normas de evaluación de las actividades docentes de la Escuela de Seguridad Pública de Andalucía. Asimismo, es necesario superar las actividades prácticas establecidas durante el desarrollo del curso.

VII.- PROFESORADO

Adrián Ramírez Correa: Ingeniero Técnico en Informática y Experto en Ciberseguridad y Peritaje Informático Judicial. Desde 2013 ejerce como perito informático forense y dirige la Dolbuck, llevando a cabo tareas de Auditorías de redes y sistemas, Hacking ético y pentesting, así como procesos de respuesta ante incidentes de seguridad. Forma parte de varios cuadros de docentes en diversos Máster en la Universidad Camilo José Cela y Universidad Católica de Murcia.

Eloy Rafael Sanz Tapia: Doctor en Informática. Desde 2004 centrado en la ciberseguridad. Actualmente, en el Servicio de Ciberseguridad de la Agencia Digital de Andalucía, se ocupa de la coordinación de actividades de ciberseguridad en la Junta de Andalucía. En paralelo, entre 1999 y 2019, ha sido profesor asociado en las Universidades de Córdoba y Pablo de Olavide, impartiendo, entre otras, asignaturas de Seguridad y de Informática Forense.