Módulo de "Ciberseguridad"

Docente: Doña Pilar Vila Avendaño

Cofundadora de Forensic & Security S.L.

FORENSIC & SECURITY

Peritos Informáticos Forenses & Auditores de Seguridad

Colegiada 311 del CPEIG, perteneciente al cuerpo oficial de Peritos de Galicia. Acreditación profesional 123 de la Asociación Nacional de Ciberseguridad y Pericia Tecnológica.

Ingeniera Informática por la Universidad de A Coruña. Más de 15 años de experiencia laboral en el ámbito de las TIC con un amplio bagaje en peritajes de distinta naturaleza. Amplios conocimientos de desarrollo de aplicaciones, informática forense, redes y seguridad. Docente de Informática Forense en distintos másteres de Seguridad Informática para la UNIR (Universidad Internacional de la Rioja), UNEX (Universidad de Extremadura), UCLM (Universidad de Castilla La Mancha), Armada Española (escuela de especialidades Antonio de Escaño de Ferrol) y Universidad La Salle de Barcelona. Colaboradora de CyberSOC Academy (Centro global de formación de Deloitte). Docente en Jornada de seguridad informática y LOPD dentro del Plan Director para la Guardia Civil y Policía Nacional de Galicia.

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

CONTENIDOS:

El temario está orientado a que sea eminentemente útil en la práctica diaria de los asistentes al mismo.

Módulo de "Delitos telemáticos", 4 horas de duración:

El temario estará dividido en **dos grandes secciones** donde estarán comprendidos lo siguientes aspectos:

1. Obtención y aseguramiento de la prueba tecnológica.

    - Derechos afectados en las investigaciones tecnológicas.
    - Límites a las investigaciones del proceso penal.
    - Medidas cautelares.
    - Obtención de la prueba tecnológica.
    - Aseguramiento, custodia y análisis de la prueba tecnológica.
    - Cadena de custodia en la prueba tecnológica.
    - Agente encubierto.
    - Registro remoto sobre equipos informáticos.

2. Delitos telemáticos.

    - Estafa.
    - Defraudación.
    - Daños informáticos.
    - Espionaje informático.
    - Falsedades.
    - Blanqueo.
    - Pornografía infantil.
    - Child grooming.
    - Acoso.
    - Descubrimiento y revelación de secretos.
    - Calumnias e injurias.
    - Amenazas.
    - Coacciones y extorsiones.
    - Suplantación y robo de personalidad.
    - Ciberterrorismo.

Módulo de "Ciberseguridad", 4 horas de duración:

1.- Como actuar ante amenazas en redes sociales, WhatsApp... cadena de custodia.

2.- Garantizar contenidos de webs, Twitter, correos electrónicos en una fecha concreta: eGarante y archive.org.

3.-Archivos temporales que pueden quedar en el móvil.

4.- Antivirus y software de protección. Herramientas en la página de Incibe muy recomendables. VirusTotal.

5.- Aplicaciones maliciosas en el móvil. Algunos de los peligros que nos podemos encontrar: chat en juegos online, redes wifi abiertas, enlaces fraudulentos.

5.1.- Términos y licencias de lo que instalamos: ¿Qué estamos aceptando?

6.- Correos electrónicos, ver cabeceras y entenderlas

7.- Buscar metadatos en imágenes (inspeccionar elemento, La Foca), documentos, etc

8.- Buscar por imágenes

9.- Búsqueda de información para identificar personas y datos en internet. OSINT

10.- Medidas de prevención que podemos aplicar:

a.- Control de nuestras cuentas: controles de actividad de Google.

b.- Consejos con respecto a nuestras cuentas en internet.

c.- Verificación en dos pasos de las cuentas que lo permitan.

d.- Google Authentcator.

e.- Configuración de Facebook.

f.- Latch, app móvil para proteger cuentas.

g.- Aplicaciones para la gestión de contraseñas.

h.- ¿Nuestras contraseñas han sido robadas?, consultando https://haveibeenpwned.com/

i.- Contraseñas seguras: https//www.howsecureismypassword.net

j.- Soluciones de cifrado y particionado por el móvil.

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

11.- Configuración del router de manera segura.

12- Hacking con Google dorks. ¿vulnerabilidades?, ¿podemos ver documentos?

13- Scam, sexting, etc ¿Qué son? ¿Cómo reaccionar y qué pasos se deben seguir?

14.- Plataformas de denuncia en internet, ¿Qué puedo hacer?

15.- Nuestro fingerprinting: what is my user agent?

16- Tor Browser y la Deep web.