CURSO Nº60/2023

FORMACIÓN PARA ARQUITECTURA TÉCNICA

CIBERSEGURIDAD

PONENTE: Miguel Cortés Astilleros

Retransmisión en directo
¡Síguela por internet!

ORGANIZA

APAREJADORES ALBACETE

COLABORA

FORMACIÓN PARA ARQUITECTURA TÉCNICA

Introducción

Se trata de un curso de concienciación sobre el uso seguro de internet que contará con una base teórica dinámica en los que como partícipe aprenderás a detectar situaciones de peligro y categorizar amenazas.

Se proporcionarán enlaces a videos y debatiremos por el foro de la plataforma. Hablaremos sobre los diferentes riesgos existentes actualmente en internet y que pueden afectarnos en nuestro día a día.

En este curso te facilitaremos una serie de contenidos, con los que podrás adquirir conocimientos para aplicarlos en tu trabajo diario y en tu vida privada.

Objetivos

Conocer, comprender y analizar los riesgos de seguridad más habituales en una microempresa, adquiriendo habilidades para el análisis y síntesis en la toma de decisiones en los ataques informáticos.

Debemos contemplar Internet como un entorno con peligros y virtudes similares al mundo real, donde podemos encontrar excelentes amigos, debates o puntos de encuentro, pero también plagado de delincuentes. “Seguridad” debe ser sinónimo de “tranquilidad”, y para nosotros utilizar las nuevas tecnologías debe suponer un avance, no una amenaza a nuestra seguridad ni a la de los que nos rodean.

Metodología

Didáctica con apoyo de prácticas y ejemplos. Se debe asistir con ordenador propio tanto presencial como por videoconferencia.

En el seguimiento por videoconferencia, para un máximo aprovechamiento del curso, es conveniente disponer de 2 PCs, en uno de ellos podrá seguir la videoconferencia y en el otro para realizar las prácticas. También es posible tener un único PC con 2 monitores o un PC con un monitor grande > 24 pulgadas.

Programa

MÓDULO 1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

1.1 La importancia de la seguridad

1.2 Falsos mitos de la seguridad

1.3 Protección

MÓDULO 2: NAVEGACIÓN SEGURA

2.1 Consejos de navegación segura

2.2 Elementos de seguridad
2.2.1. Protección frente a ataques
2.2.2 Gestión de la información Privada

2.3 Fortalecer la seguridad
2.3.1 Fortalecer la seguridad I
2.3.2 Fortalecer la seguridad II
2.3.3. Fortalecer la seguridad III
3.2.4. Fortalecer la seguridad IV

2.4 Herramientas y complementos
2.4.1 NoScript
2.4.2 Adblock Plus
2.4.3 WOT
2.4.4 Otras herramientas

MÓDULO 3. INTRODUCCION AL MALWARE

3.1 Malware

3.2 Tipos de Malware

3.3. Monetización

3.4. Consejos para minimizar riesgos

Programa

MÓDULO 4: SEGURIDAD CORREO ELECTRÓNICO

4.1 Consideraciones según la forma de acceso

4.2. Envío de correo: Para, CC y CCO

4.3 Certificados, firma digital y cifrado

4.3.1 Certificados

4.3.2. Firma Digital

4.4. Spam o publicidad no deseada

4.5. Engaños y estafas

4.6 Phishing

MÓDULO 5. SEGURIDAD EN DISPOSITIVOS MÓVILES

5.1. IMEI, PIN, PUK

5.2 Bloqueando el terminal

5.3 Seguridad en telefonía móvil

5.4. Actualizaciones de software

5.5. Conectividad de dispositivos móviles

5.5.1. Bluetooth

5.5.2. WiFi

5.5.3. NFC

5.6. Copias de seguridad

5.7 Cifrado de información móviles

Programa

MÓDULO 6. SEGURIDAD EN EQUIPOS PORTÁTILES

6.1. Protección lógica

6.1.1 Copias de seguridad

6.1.2 Contraseñas de acceso

6.1.3 Controles avanzados de acceso

6.1.4 Cifrado

6.1.5 Recuperación de equipos robados

6.1.7 Deshabilitar conectividad innecesaria

6.2 Protección física

6.3. Otras consideraciones

MÓDULO 7. DELITOS TECNOLÓGICOS

7.1 Delitos Tecnológicos

7.1.1 Delitos por abuso de menores (grooming) y pornografía infantil

7.1.2. Delito contra la intimidad. Descubrimiento y revelación de secretos ciberespionaje, accesos no autorizados, cracking o black hacking)

7.1.3 Delito de fraude informático.

7.1.3.1 Estafas utilizando medios tecnológicos

7.1.4. Delito de utilización abusiva de cualquier equipo terminal de telecomunicación

7.1.5 Destrucción o daño a sistemas de información (sabotaje informático)

7.1.6 Delitos contra la propiedad intelectual

7.1.7 Robo de información empresarial

7.1.8 Acceso ilícito a servicios de comunicación

7.1.9 Delitos contra la intimidad y el honor. Publicaciones ofensivas

7.1.10 Otros delitos

7.2. Denuncias

Programa

MÓDULO 8. SEGURIDAD EN REDES INALÁMBRICAS

8.1 Seguridad en WiFi

8.2 Protocolos de seguridad
8.2.1 WEP
8.2.2 WPA
8.2.3. WPA2
8.2.4 WPA30

8.3 Seguridad en NFT

8.4 Seguridad en Bluetooth

8.5. Recomendaciones de seguridad

MÓDULO 9. SEGURIDAD EN LAS REDES SOCIALES

9.1 Chats

9.2 Mensajería instantánea

9.3 Redes sociales
9.3.1 Privacidad en Facebook
9.3.2 Privacidad en LinkedIn
9.3.3 Otras redes sociales

9.4 Acoso a través de la RED

MÓDULO 10. APÉNDICE

10.1 Catálogo de medidas preventivas y herramientas para proteger la privacidad

10.2 Información sobre seguridad tecnológica

10.3 SIM Swapping (Duplicado SIM)

10.4. Geolocalización por terceros

12 horas lectivas.

Miércoles 17, jueves 18, lunes 22 y miércoles 24 de mayo de **16:00 a 19:00h** (horario peninsular).

Presencial o por videoconferencia *online* en directo.
Las grabaciones de las sesiones no se facilitan, salvo justificación o caso excepcional.

Plazas limitadas, es necesario inscribirse previamente antes del **11 de mayo** a las **13:00 h** (horario peninsular).

SEDE del Colegio Oficial de Aparejadores, Arquitectos Técnicos e Ingenieros de Edificación de Albacete
Avda. Isabel la Católica, 19, bajo, 02005, Albacete
967 216 307· administracion@aparejadoresalbacete.es

Precio **colegiados COAATIE: 40 €**
Precio **no colegiados: 60 €**

Profesorado

Miguel Cortés Astilleros

- *Auditor ISO27001*
- *Consultor y Perito Judicial*
- *Delegado de Protección de Datos*

CALENDARIO MAYO

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

INSCRIPCIONES A TRAVÉS DE iCOLEGIA