PROTECCIÓN DE EQUIPOS EN LA RED (IFCT106PO)

On Line

SUBVENCIONADO 100%

OBJETIVOS:

- Describir los objetivos de la seguridad física y de la lógica.
- Analizar la importancia de la seguridad en el puesto del usuario.
- Describir las características de virus informáticos y definir sus métodos de propagación.
- Identificar los sistemas que ayudan a luchar contra los ataques de código malicioso.
- Listar un conjunto de buenas prácticas que nos permitirán estar más seguros.
- Identificar las distintas arquitecturas de los sistemas cortafuegos.
- Describir las técnicas de ingeniería social que utilizan las técnicas de suplantación.
- Clasificar los tipos de actualizaciones que publican los fabricantes.
- Distinguir las técnicas de actualización más habituales.

DIRIGIDO A:

- Personas trabajadoras (Autónomos también) (Personas desempleadas: Consultar si hay plaza)

DURACIÓN:

- Horas totales: 10h.

CALENDARIO:

Inicio-Fin: 12/01/2022 – 31/01/2022 **Disponible:** 24 horas

ENERO						
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						

CONTENIDO:

1. **La necesidad de protegerse en la red**
   - 1.1. ¿Por qué hay que protegerse?
     - 1.1.1. Las evidencias
     - 1.1.2. Reflexiones
     - 1.1.3. Casos en el resto del mundo
     - 1.1.4. El valor de la información
     - 1.1.5. El valor de las infraestructuras
     - 1.1.6. Análisis de riesgos
       - 1.1.6.1. Análisis de impacto de los incidentes
       - 1.1.6.2. Formas de afrontar los riesgos
     - 1.1.7. Vulnerabilidades
   - 1.2. Objetivos de la seguridad informática
   - 1.3. La seguridad
     - 1.3.1. Seguridad física
     - 1.3.2. Seguridad lógica
   - 1.4. Seguridad en el puesto de usuario
     - 1.4.1. Escenarios de riesgo
     - 1.4.2. Medidas de seguridad
       - 1.4.2.1. Política y normativa de seguridad
       - 1.4.2.2. Política y programa de concienciación
       - 1.4.2.3. Medidas de carácter técnico y logístico
2. **Los peligros posibles: los virus informáticos**
   - 2.1. Características de los virus informáticos
     - 2.1.1. Introducción
     - 2.1.2. Características
     - 2.1.3. Situaciones y motivaciones
     - 2.1.4. Consecuencias
   - 2.2. Métodos de propagación
   - 2.3. Tipos de virus
     - 2.3.1. Según cómo se alojan en el dispositivo y su modo de actuación
     - 2.3.2. Según su forma de propagación
     - 2.3.3. Según el impacto de las acciones que realiza
   - 2.4. Tendencias
3. **Las soluciones: el antivirus**
   - 3.1. Tipos de medidas
     - 3.1.1. Medidas preventivas
     - 3.1.2. Medidas paliativas
   - 3.2. Sistemas de detección y contención de código malicioso
     - 3.2.1. Antivirus
     - 3.2.2. El navegador
     - 3.2.3. Cortafuegos, Honeypots y sistemas de detección y prevención de intrusiones
     - 3.2.4. Sistemas de correlación de eventos y utilización de entornos controlados de ejecución
     - 3.2.5. Aplicación de técnicas de ingeniería inversa
   - 3.3. Buenas prácticas para protegernos de los virus y del resto de código malicioso
4. **Otros conceptos sobre seguridad informática**
   - 4.1. Firewall
     - 4.1.1. Seguridad perimetral
     - 4.1.2. Arquitectura de cortafuegos
       - 4.1.2.1. Reglas de filtrado y servicios proxy
       - 4.1.2.2. Arquitecturas más comunes
     - 4.1.3. Spam
       - 4.1.3.1. Origen
       - 4.1.3.2. Cómo combatir el correo no deseado
       - 4.1.3.3. Phising
       - 4.1.3.4. Introducción a la ingeniería social
       - 4.1.3.5. Concepto de phishing
       - 4.1.3.6. Otras variantes
     - 4.1.4. Copias de seguridad
     - 4.1.5. Respuesta a incidentes de seguridad
     - 4.1.6. Tendencias
5. **Actualizaciones del software**
   - 5.1. Tipos de actualizaciones
     - 5.1.1. Publicación de actualizaciones
   - 5.2. Determinación de los requerimientos y técnicas de actualización
     - 5.2.1. Infraestructura de seguridad actualizada
     - 5.2.2. Actualización de los sistemas operativos
     - 5.2.3. Actualización de las aplicaciones
     - 5.2.4. Actualizaciones en los dispositivos móviles
     - 5.2.5. Actualización de las herramientas de protección

INSCRIPCIONES:

Para inscribirse envíe la ficha de inscripción del alumno (descargar aquí) al correo inscripciones@cimaformacion.es .
Tras recibir su solicitud nos pondremos en contacto con usted a la mayor brevedad.