SOLUCIONES

Protección de equipos en la red

IFCT106PO

Administración y gestión

10 horas de formación

editorialcep

SOLUCIONES TEST

Soluciones Tema 1

La necesidad de protegerse en la red

1. c) Fallo eléctrico

2. b) Un evento accidental o intencionado que puede ocasionar algún daño en el sistema informático provocando pérdidas materiales, financieras o personales

3. d) Es el conjunto de programas, instrucciones y reglas informáticas que hacen posible la realización de tareas específicas

4. a) Es el conjunto de los componentes físicos de los que está hecho el equipo, es decir, la parte que se puede ver del ordenador, los componentes de su estructura física

5. d) Es completamente fiable y segura

6. b) Descuidos y errores humanos

7. c) Las amenazas pueden clasificarse de dos formas como naturales, agentes externos y agentes internos o como accidentes, errores y actuaciones malintencionadas

8. b) Usar caracteres consecutivos del teclado

9. b) No usar antivirus, es la puerta de entrada a muchos virus

10. a) Es el conjunto de herramientas diseñadas para proteger los datos durante su transmisión a través de una red de telecomunicación

Soluciones Tema 2

Los peligros posibles: los virus informáticos

1. c) Es cualquier programa, documento o mensaje susceptible de causar daños e introducirse de forma no autorizada en las redes y sistemas informáticos. Dentro de esta definición estarán incluidos los virus, troyanos, gusanos, bombas lógicas…

2. b) Es un acto inteligente y deliberado contra la seguridad del sistema derivado de una amenaza basado en eludir los servicios de seguridad y violar la política de seguridad de un sistema. Es cualquier acción que comprometa la seguridad de la información de un sistema

3. c) Un programa con la capacidad de replicarse a sí mismo sin el consentimiento del usuario y que infecta a otros programas modificándolos

4. d) Técnicas que se basan en ofrecer información falseada del sistema que ha sido infectado por el virus para no despertar sospechas. Pueden modificar la cantidad de memoria disponible, la fecha o el tamaño de los ficheros

5. c) Son el resultado de la ejecución de las rutinas del virus. Pueden ir desde bromas gráficas inofensivas hasta daños severos que afecten al rendimiento del sistema y a la seguridad de datos y ficheros

6. d) Apertura trasera de puertas

7. a) Son daños como consecuencia de la entrada del virus en el sistema independientemente del código dañino que vaya a ejecutar

8. a) Formateo de discos duros

9. b) Virus del sector de arranque

10. a) Reconocimiento de firmas de los equipos

Soluciones Tema 3

Las soluciones: el antivirus

1. a) Reducir las vulnerabilidades de los sistemas, la probabilidad de amenazas y el nivel de impacto

2. d) Son cualquier medida empleada para anular o reducir el riesgo de una amenaza. Pueden ser medidas de prevención que se aplican antes de que ocurra un incidente o medidas de detección que se ponen en marcha durante el incidente

3. a) Cualquier medida empleada para reducir el impacto cuando se está produciendo un incidente contra la seguridad del equipo. También se las conoce como medidas de corrección ya que se aplican después de que tenga lugar el incidente

4. b) Son medidas que implican el control de acceso físico a los recursos y de las condiciones ambientales en que tiene que ser utilizados (temperatura, humedad, suministro eléctrico…)

5. c) Están relacionadas con la protección mediante herramientas y técnicas informáticas como el cifrado, la autenticación de usuarios…

6. a) Detección, identificación y eliminación

7. b) Permite a los programas antivirus detectar fácilmente virus polimórficos complejos. Cuando se ejecuta el archivo que contiene el virus polimórfico, el virus puede descifrarse para activarse

8. a) Un sistema que suministra un tiempo de respuesta rápido para que los virus se puedan erradicar tan pronto como sean introducidos. Cuando un nuevo virus entra en el equipo, lo captura, analiza, añade los procedimientos de detección y protec-

ción, lo elimina y pasa la información sobre este virus a los sistemas que ejecutan el antivirus

9. d) Es el conjunto de decisiones que definen acciones futuras y los medios que se van a emplear para conseguirlas

10. a) Es la definición detallada de los pasos que hay que ejecutar para llevar a cabo una serie de tareas de seguridad de los equipos

Soluciones Tema 4

Otros conceptos sobre seguridad informática

1. b) Es un dispositivo que se utiliza para proteger la red interna de una organización mediante la separación de la red interna de Internet, examinando todos los mensajes que entran y salen de la red interna o de Internet para ver si cumplen los protocolos de seguridad especificados

2. c) Son los ataques que tratan de obtener números de cuenta y claves de acceso a determinados servicios de Internet y servicios de banca electrónica, para realizar operaciones fraudulentas que perjudican a los propietarios de esas cuentas

3. a) Son los mensajes de correo electrónico con publicidad no solicitada por el destinatario

4. c) Si son muy sofisticados, van a necesitar una configuración más compleja

5. b) Protección de ataques que proceden de cualquier sitio, ya sea la red o de dispositivos externos

6. a) Bloquear todos los paquetes con un tamaño superior al mínimo permitido

7. d) Los individuos que generan millones de mensajes de correo electrónico basura y que saturan cada día las redes y los servidores de los operadores de telecomunicaciones y proveedores de acceso a Internet

8. b) Darse de baja en estos correos spam

9. a) Los atacantes usan virus y troyanos para conectar a las víctimas desde su ordenador a páginas web falsas de sus entidades bancarias y obtener sus datos, número de cuenta y claves de acceso y de operación

10. c) Las páginas web seguras comienzan por https://

Soluciones Tema 5

Actualizaciones del software

1. a) Es cualquier debilidad en el sistema informático o software que pueda permitir a las amenazas causar daños y producir pérdidas

2. c) Es un complemento del navegador que tiene capacidad de interactuar con el Sistema Operativo y con aplicaciones externas. Añade una funcionalidad adicional o una nueva característica al software

3. d) Actualizar solo los dispositivos que tengan acceso a una red

4. a) Es cualquier otro software instalado en un equipo y que también debe mantenerse actualizado

5. b) Es un software que bloquea las posibles acciones perjudiciales antes de que tengan la oportunidad de afectar al sistema

6. b) Controla los accesos de los troyanos al equipo

7. c) Sí, siempre, ya que pueden tener vulnerabilidades que deben ser corregidas

8. d) Son las actualizaciones de seguridad de un programa para corregir vulnerabilidades

9. d) Sí, deben estar siempre actualizados a la última versión disponible

10. c) Las actualizaciones no modifican la interfaz gráfica del software

SOLUCIONES ACTIVIDADES

Soluciones Tema 1

La necesidad de protegerse en la red

1.

Seguridad informática	Es el conjunto de herramientas diseñadas con el fin de proteger los datos almacenados en un equipo.
Seguridad de la información	Consiste en proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados.
Seguridad de la red	Es el conjunto de herramientas diseñadas para proteger los datos durante su transmisión a través de una red de telecomunicación.
Seguridad en internet	Son las herramientas diseñadas para proteger los recursos de una red privada frente a usuarios de otras redes.

2.

Accidentes	Averías de hardware, fallos de software, incendio, inundación, fallo eléctrico
Errores	De utilización, explotación y ejecución de los recursos
Actuaciones malintencionadas	Robos, fraudes, sabotajes, intentos de intrusión

3.

3.1

a) Usar una combinación de letras sin sentido

b) Incluir una mezcla de caracteres en mayúscula, minúscula y numéricos

c) Las contraseñas largas son más seguras

3.2

a) Usar contraseñas robustas

b) Usar siempre la protección de un antivirus

c) Usar un cortafuegos

e) No ejecutar programas de origen desconocido

4.

Es un mecanismo densocriptográfico que permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador.

Soluciones Tema 2

Los peligros posibles: los virus informáticos

1.

Trampa	Entrada secreta a un programa que permite el acceso sin pasar por los procedimientos de acceso de seguridad.
Bomba lógica	Código introducido en programa legítimo que explota cuando se dan ciertas condiciones como la presencia o ausencia de ciertos archivos, una fecha...
Caballo de Troya	Programa, aparentemente útil, que contiene un código oculto que al invocarse lleva a cabo funciones perjudiciales, no deseadas o no autorizadas.
Zombi	Programa que, sin ser percibido, toma el control del sistema conectado a internet y usa ese ordenador para lanzar ataques que hacen difícil seguir la pista al creador.
Gusanos	Pueden propagarse de un sistema informático a otro si los dos sistemas están conectados por la red, por ejemplo, mediante el uso del correo electrónico.
Bacterias	Consumen la memoria del sistema infectado mediante la realización de múltiples copias sucesivas de sí mismos.

2.

Virus parásito	Se adjunta por sí mismo a los archivos ejecutables y se replica cuando el programa infectado se ejecuta, infectando a otros archivos ejecutables.
Virus furtivo	Un virus diseñado para evitar la detección por parte de un antivirus.

Virus polimórfico	Un virus que se modifica con cada una de las infecciones, haciendo imposible la detección por la "firma" del virus.
Gusanos (worms)	Son capaces de replicarse a sí mismos, no necesitan la intervención de un usuario para su propagación. Una vez que infectan un sistema crean copias en la memoria y se extienden a otros equipos conectados a la misma red.
Software espía o Spyware	Este tipo de software cuando infecta a un sistema guarda información sobre la actividad del usuario sin que este lo sepa.
Virus de correo electrónico	Es un software dañino que llega a través del email y usa las características del software del correo electrónico para replicarse a través de Internet.

3.

Fase latente o inactiva	El virus está inactivo por lo que no realiza ninguna actividad. No todos los virus tienen esta fase en su ciclo de vida.
Fase de propagación	El virus coloca copias idénticas a sí mismo en otros programas o en áreas del sistema haciendo que ahora cada programa infectado contenga copias del virus, que a su vez entrarán en fase de propagación.
Fase de activación	El virus se activa para llevar a cabo la función para la que se creó.
Fase de ejecución	El virus realiza la actividad para la que se programó, que puede ser inofensiva como un mensaje en la pantalla, o perjudicial como la destrucción de programas o archivos.

Soluciones Tema 3

Las soluciones: el antivirus

1.

Motor de análisis	Indica al software dónde y cómo realizar la búsqueda. Compara archivos que contiene el ordenador con los virus conocidos que hay en los archivos de firma.
Archivos de firma	Son una base de datos de virus conocidos y sus acciones. Contiene los patrones de los virus conocidos.
Módulo de control	Lleva a cabo las siguientes funciones: - Seguimiento de la actividad en el sistema informático - Protección y prevención del sistema - Detección de códigos maliciosos - Configuración del funcionamiento del antivirus.
Módulo de respuesta	Desempeña las siguientes tareas: - Genera alarmas y lleva a cabo un registro de las incidencias - Bloquea servicios y programas sospechosos - Desinfecta programas y documentos infectados.

2.

Primera generación	Eran exploradores simples que detectaban virus conocidos, reconociendo su patrón y estructura o buscando cambios en la extensión.
Segunda generación	Son exploradores heurísticos, es decir, emplean reglas heurísticas para buscar posibles infecciones por virus. Buscan fragmentos de código y comprueban la integridad de los programas.

Tercera generación	Son programas que detectan la actividad. Residen en la memoria e identifican un virus por su acción más que por su estructura.
Cuarta generación	Este software ofrece una protección integral. Son paquetes compuestos por una gran variedad de técnicas antivirus usadas conjuntamente. Incluye componentes de exploración y detección de acciones y capacidad de control de acceso que limita la posibilidad en entrada de los virus en el sistema.

3.

b) Escáner basado en el reconocimiento de "firmas", de códigos maliciosos y de patrones conocidos en un código ejecutable, empleando una base de datos de virus conocidos

c) Monitor residente que ofrece protección en tiempo real analizando cualquier archivo antes de ser utilizado o de ser descargado de internet

d) Análisis heurístico para detectar virus nuevos al reconocer un código con comportamiento sospechosos

e) Comprobación de la integridad de los archivos del sistema para alertar al usuario de cualquier cambio de tamaño en los archivos

f) Análisis del comportamiento para detectar cualquier acción sospechosa o peligrosa que se realice en el sistema informático

4.

Es un protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura. Permite una autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro.

Soluciones Tema 4

Otros conceptos sobre seguridad informática

1.

Control de servicio	Determina los tipos de servicio de Internet a los que se puede acceder. Filtrará el tráfico valiéndose de las direcciones IP y del número de puertos TCP.
Control de dirección	Determina en qué dirección se pueden iniciar las solicitudes de servicios particulares y en qué dirección se les permite el paso a través del firewall.
Control de usuario	Controla el acceso a un servicio, en función de qué usuario es el que está intentando acceder.
Control de comportamiento	Controla como se utilizan los particulares. El cortafuegos puede filtrar el correo spam o puede permitir el acceso externo sólo a una parte de la información de un servidor web local.

2.

IP	Es un número que permite identificar, de manera jerárquica y lógica, la interfaz de un equipo que se encuentra conectado a la red y que emplea un protocolo de seguridad.
TCP	Es uno de los principales protocolos que permite que las máquinas que están comunicadas controlen el estado de la trasmisión y lo hagan de manera segura.
UDP	Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.
Proxy	Es una red informática o un servidor, que actúa como intermediario entre las peticiones de recursos que realiza un cliente a un servidor.

3.

Filtros de paquetes	Filtran el tráfico basándose en combinaciones de diferentes campos de las cabeceras IP, TCP y UDP de cada mensaje.
Gateways de aplicaciones o servidores Proxy	Funcionan como "pasarelas de aplicación". Analizan todos los paquetes de datos de un determinado servicio o aplicación teniendo en cuenta las reglas del protocolo y el estado de la sesión.
Stateful inspection o de filtrado dinámico de paquetes	Actúan a nivel de circuito, es decir, mantienen el estado de cada sesión a través del cortafuegos y cambian las reglas del filtrado dinámicamente según lo definido en la política seguridad.
Híbridos	Tienen propiedades que son la combinación de las propiedades de los cortafuegos anteriores.

Soluciones Tema 5

Actualizaciones del software

1.

Navegador web	Es la primera puerta de entrada por la que puede pasar cualquier tipo de malware, ya que es con el que accedemos directamente a Internet y es uno de los elementos imprescindibles y más utilizados en los equipos.
Plugins	Es un complemento del navegador que tiene capacidad de interactuar con el sistema operativo y con aplicaciones externas.
Sistema operativo	Es el programa o conjunto de programas que efectúan una gestión de los procesos básicos de un sistema informático y que permite la ejecución del resto de operaciones.
Programas de seguridad	Extra de seguridad importante para proteger los equipos y dispositivos, pero también contienen vulnerabilidades.

2.

b) Controla las modificaciones en la lógica de archivos ejecutables

c) Evitar contenido ejecutable en correo electrónico y mensajería instantánea

d) Controla la iniciación de las comunicaciones en la red

Podemos apoyarnos en el empleo de software de bloqueo de acciones cuya función es bloquear las posibles acciones perjudiciales antes de que tengan la oportunidad de afectar al sistema. Es capaz de controlar los siguientes comportamientos:

- Intentos de abrir, visualizar, borrar y modificar archivos.
- Intentos de formatear unidades de disco.
- Modificaciones en la lógica de archivos ejecutables.
- Modificaciones de las configuraciones críticas del sistema.
- Evitar contenido ejecutable en correo electrónico y mensajería instantánea.

– Iniciación de las comunicaciones en la red.

3.

Algunos ejemplos podrían ser:

- SECUNIA PSI: herramienta de seguridad diseñada para detectar programas y plugins vulnerables y desactualizados que requieran de parches de seguridad y que pueden exponer al equipo a ataques que rara vez son bloqueados por antivirus tradicionales.
- TECHTRACKER FREE: permite informar al usuario cuando algún programa de los que se encuentra en su base de datos y está instalado en el equipo del usuario se encuentra desactualizado.