User Security Awareness

Reactivos

Pregunta 1

Selecciona, ¿cuáles son los dispositivos con los que el usuario interactúa para comunicarse?

Opciones:

a. Telecomunicación
b. Almacenamiento
c. Comunicación
d. Usuario final

Pregunta 2

Establece cuáles son algunos de los dispositivos de usuario final.

Opciones:

a. Tabletas
b. Software
c. Smart TV
d. USB

Pregunta 3

Elige la protección utilizada para el dispositivo mediante *software* anti-espionaje.

Opciones:

a. Protección de acceso al dispositivo
b. Protección familiar
c. Protección antispyware
d. Backup/Restore

Pregunta 4

Selecciona, ¿cuál es el dispositivo que se conecta mediante aplicaciones y/o asistentes de voz?

Opciones:

a. Teléfonos
b. Smart TV
c. Dispositivos inteligentes
d. Asistente de voz

Pregunta 5

Elige la protección que aplica para el disco duro externo y almacenamiento en la nube.

Opciones:

a. Uso de antivirus
b. Uso de antivirus y políticas personales de uso
c. Políticas personales de uso
d. Contraseña de bloqueo

Pregunta 6

Selecciona el *malware* más antiguo del mundo.

Opciones:

a. Virus
b. Troyano
c. Gusano
d. *Spyware*

Pregunta 7

Establece el tipo de virus que tiene la peculiaridad de copiarse a sí mismo dentro de varias localidades del sistema operativo

Opciones:

a. Gusano
b. Virus
c. Troyano
d. *Spyware*

Pregunta 8

Elige cuál es el programa que se encarga de espiar la información de alguien más.

Opciones:

a. Gusano
b. *Spyware*
c. Virus
d. Troyano

Pregunta 9

Selecciona, ¿cuál es el software que instala publicidad no deseada en un dispositivo?

Opciones:

a. Gusano
b. *Adware*
c. Virus
d. Troyano

Pregunta 10

Elige, ¿cuál es el malware desarrollado por personas que obtendrán un beneficio de aquellas empresas que son visitadas gracias a la publicidad?

Opciones:

a. Troyano
b. Virus
c. Gusano
d. *Adware*

Pregunta 11

Selecciona, ¿qué es una política de ciberseguridad?

Opciones:

a. Las políticas de ciberseguridad son *softwares* que se encuentran en cada uno de los dispositivos para protegerlos.
b. Las políticas de ciberseguridad no son lineamientos que se contraponen a los riesgos para proteger los dispositivos e información de los usuarios.
c. Las políticas de ciberseguridad son lineamientos que propagan a los riesgos hacia los dispositivos y la información de los usuarios.
d. Las políticas de ciberseguridad son lineamientos que se contraponen a los riesgos para proteger los dispositivos e información de los usuarios.

Pregunta 12

Elige, ¿cuál de las opciones no es una política de seguridad?

Opciones:

a. Tener instalado en el navegador un *plugin* que verifique los sitios *web* que visitamos y alerte antes de visitar un sitio sospechoso.
b. No aceptar archivos desconocidos que se envíen mediante *bluetooth*.
c. Proporcionar información personal, bancaria, claves de acceso, etc.
d. No adquirir *software* pirata ni buscar o utilizar crackers para obtener credenciales apócrifas de software pirata.

Pregunta 13

Selecciona, ¿cuál es la opción para hacer una contraseña robusta?

Opciones:

a. Usar letras solamente.
b. Tener más de 8 caracteres.
c. Usar números solamente.
d. Que la contraseña esté relacionada con un dato personal.

Pregunta 14

¿Quién implementa las políticas de ciberseguridad?

Opciones:

a. El responsable de seguridad de la información.
b. TI.
c. Recursos Humanos.
d. La empresa en conjunto con todos los empleados.

Pregunta 15

Elige, ¿para qué se crea una política de uso?

Opciones:

a. Son creadas para evitar y/o mitigar los incidentes digitales que se puedan presentar en un dispositivo.
b. Son creadas para evitar y/o mitigar los incidentes físicos que se puedan presentar en un dispositivo.
c. Son creadas para evitar y/o mitigar los incidentes naturales que se puedan presentar en un dispositivo.
d. Son creadas para evitar y/o mitigar los ataques que se puedan presentar en un dispositivo.

Pregunta 16

Selecciona, ¿qué es la mitigación de riesgos?

Opciones:

a. Es el proceso en el cual ya no existe un riesgo para la compañía.
b. Es el proceso en el cual se eliminan las incidencias existentes.
c. Es el proceso de desarrollo de opciones y acciones que, al ser implementadas, mejorarán las oportunidades y reducirán el impacto negativo o la probabilidad de ocurrencia de un evento en particular.
d. Es el proceso para eliminar todos los riesgos existentes.

Pregunta 17

Establece, ¿qué niveles de seguridad existen en un navegador?

Opciones:

a. Baja, regular, alta.
b. Baja, media, alta.
c. Menor, mayor.
d. No existe nivel de seguridad para un navegador.

Pregunta 18

Selecciona el nivel de seguridad para Microsoft Edge que inhabilita secciones de los sitios *web.*

Opciones:

a. Estricta
b. Equilibrada
c. Básica
d. Nula

Pregunta 19

Elige, ¿qué tipo de tecnología se utiliza para mitigar los riesgos que existan para los menores de edad al momento de usar dispositivos tecnológicos?

Opciones:

a. Seguridad en el navegador
b. AntiSpyware
c. Antivirus
d. Control parental

Pregunta 20

Elige, ¿qué elemento debe tener un sitio *web* para saber que es seguro?

Opciones:

a. Localizar una "s" después de http.
b. Imágenes confiables.
c. Un antivirus para *web.*
d. Un candado en la url.

Pregunta 21

Selecciona, ¿cuáles son los sistemas operativos para dispositivos móviles?

Opciones:

a. One UI y iOS
b. iOS y Android
c. Android y Huawei
d. Huawei y Samsung

Pregunta 22

Selecciona, ¿cuál de las siguientes opciones no es una protección para dispositivos Android?

Opciones:

a. Asesor de aplicaciones

b. Protección *web*
c. Antispyware
d. Protección del dispositivo

Pregunta 23

Selecciona, ¿quién supervisa las aplicaciones de iOS?

Opciones:

a. Microsoft
b. Apple
c. Proveedor externo
d. Google

Pregunta 24

Elige la opción más segura para evitar riesgos en conexiones de redes *Wifi*.

Opciones:

a. Si utilizas una *Wifi* poco segura para abrir aplicaciones bancarias.
b. Si tu dispositivo tiene activada la opción de: conectarse en automático a cualquier red *Wifi* disponible.
c. Redes *Wifi* privadas con contraseña.
d. Las redes *Wifi* de un lugar público como cafeterías o centros comerciales, aunque requieran contraseña.

Pregunta 25

Elige la medida para disminuir el riesgo del uso de dispositivo personal en el trabajo

Opciones:

a. Capacitar a los usuarios en riesgos y medidas de seguridad.
b. Prohibir el ingreso con dispositivos personales.
c. Bloquear la señal de red dentro de la empresa.
d. Bloquear puertos USB en equipos.

Pregunta 26

¿Cómo se le llama a la práctica de engañar a alguien para que divulgue información personal de la víctima?

Opciones:

a. Ingeniería social
b. Estafa
c. Engaño
d. Denegación de servicios

Pregunta 27

Elige el modo de operación donde el usuario ingresa una USB “olvidada” a su dispositivo por curiosidad.

Opciones:

a. Carnada
b. *Phishing*
c. Pretexto
d. *Vishing*

Pregunta 28

Selecciona el modo de operación que consiste en que el usuario recibe un correo electrónico de alguien que es conocido, por lo cual abre el correo, va a alguna página web y se infecta el equipo.

Opciones:

a. *Vishing*
b. Pretexto
c. *Phishing*
d. *Hacking* de correo electrónico

Pregunta 29

Identifica la modalidad que consiste en que el atacante crea una historia ficticia para llamar la atención del usuario y obtener su información.

Opciones:

a. *Vishing*
b. *Phishing*
c. Pretexto
d. *Hacking* de correo electrónico

Pregunta 30

Elige el método de ingeniería social que tiene un acercamiento más humano.

Opciones:

a. *Phishing*
b. *Hacking* de correo electrónico
c. Pretexto
d. *Vishing*

Pregunta 31

Selecciona, ¿cuál es el *malware* diseñado para encriptar los archivos de los usuarios y/o organizaciones, de tal forma que no se pueden acceder por medio de los programas para los que fueron hechos?

Opciones:

a. *Adware*
b. *Ransomware*
c. Virus
d. Troyano

Pregunta 32

Selecciona la opción correcta:

Su objetivo es cifrar datos del usuario (documentos, fotos, videos, hojas electrónicas, etcétera) pero no afecta el funcionamiento básico de la computadora.

Opciones:

a. *Ransomware* enfocado.
b. *Ransomware* de cifrado.
c. *Ransomware* de bloqueo.
d. *Ransomware* dirigido.

Pregunta 33

Selecciona la opción correcta:

Este *malware* bloquea las funciones fundamentales de la computadora del usuario. Puede ser que te impida acceder al explorador de archivos o que inhabilite algunos de los periféricos como el ratón.

Opciones:

a. *Ransomware* de cifrado.
b. *Ransomware* dirigido.
c. *Ransomware* de bloqueo.
d. *Ransomware* enfocado.

Pregunta 34

Elige, ¿qué debes hacer ante un *Ransomware?*

Opciones:

a. Tener un antivirus.
b. Prevenir, ya que una vez que recibes este ataque es imposible desbloquear los archivos.
c. Parchar todos los equipos.
d. Cortar el acceso a la red.

Pregunta 35

¿Cómo se extiende el *Ransomware*?

Opciones:

a. Vía USB.
b. A través de ligas con sitios que contienen archivos infectados.
c. A través de correo electrónico.
d. A través de correo electrónico y ligas con sitios que contienen archivos infectados.

Pregunta 36

Selecciona el proceso en el cual el usuario debe ingresar un usuario y una contraseña correctamente para poder utilizar el dispositivo

Opciones:

a. Cifrado asimétrico
b. Bloqueo
c. Cifrado
d. Autenticación

Pregunta 37

Selecciona la técnica que consiste en revolver los datos del disco duro usando un algoritmo especial para este efecto.

Opciones:

a. Autenticación
b. Cifrado asimétrico
c. Bloqueo
d. Cifrado

Pregunta 38

Selecciona el tipo de cifrado que se caracteriza porque utiliza una misma llave para encriptar y desencriptar la información.

Opciones:

a. Simétrico
b. Asimétrico
c. Asimétrico y simétrico
d. No existe

Pregunta 39

Elige el algoritmo desarrollado por IBM quien,
inicialmente, le llamó Lucifer. La NSA lo adoptó como estándar en 1977.

Opciones:

a. DES
b. Triple DES
c. AES
d. *Twofish*

Pregunta 40

Elige el algoritmo de tipo asimétrico que lleva el nombre de sus creadores Ron Rivest, Adi Shamir y Leonard Adleman.

Opciones:

a. *Twofish*
b. AES
c. PKI
d. RSA