Esquema/Resumen del Tema: Seguridad Informática (Grupo Renfe)

I. Fundamentos y Concienciación General

1. Recomendaciones básicas de ciberseguridad:

- Verificación de sitios web seguros (HTTPS, candado).
- Mantener navegador, plugins y extensiones actualizados.
- Precaución con correos y adjuntos sospechosos: nunca abrir enlaces ni descargar ficheros si no se conoce al remitente o presenta indicios fuera de lo habitual.
- La concienciación, el sentido común y las buenas prácticas son las mejores defensas.
- Importancia de contactar con el Centro de Servicio (200100) o Área de Ciberseguridad de Renfe (ciberseguridad@renfe.es) ante incidencias o cualquier sospecha de compromiso de la seguridad.
- Uso de VPN en redes públicas para conexiones fiables.
- No dar usuario, contraseña o email de Renfe en sitios ajenos a la empresa.
- No conectar dispositivos personales a sistemas o redes de Renfe.
- No conectarse a Wi-Fi personales o no aprobadas dentro de las instalaciones de Renfe.
- No aceptar USBs de desconocidos o abandonados.

2. Análisis de riesgos de seguridad de la información:

Definición: Proceso para identificar las amenazas y vulnerabilidades de una aplicación o servicio, con el objetivo de identificar controles que

minimicen los riesgos. Implica determinar qué o cuáles activos proteger, de qué o de quién y cómo hacerlo.

Segunda definición: Mecanismo para gestionar el riesgo de una aplicación/servicio y contar con defensas para prevenir, responder o detectar incidentes.

Obligatoriedad por normativas aplicables a Renfe: Esquema Nacional de Seguridad (ENS), Ley de Protección de Infraestructuras Críticas (Ley 8/2011), y Ley Orgánica de Protección de Datos Personales y garantías de los derechos digitales.

Renfe lo enfoca a través de la Oficina de Riesgo y Marco de la Gerencia de Ciberseguridad y Privacidad, con presencia en las sociedades del Grupo.

Roles clave en el análisis:

Responsable de la Información: Responsable final de establecer las medidas para el tratamiento del riesgo (somos nosotros).

Responsable Funcional: Mayor conocimiento funcional del sistema o aplicación.

Responsable Técnico: Mayor conocimiento técnico del sistema o aplicación.

Estrategias de gestión del riesgo: Evitar, Reducir o Mitigar, Transferir (la responsabilidad del tratamiento, no el riesgo en sí), y Aceptar (monitorizándolo).

II. Entorno de Trabajo y Acceso Seguro

3. Entorno de trabajo seguro:

Importancia debido al incremento del uso de equipos portátiles (teletrabajo) como posible ventana de ataque.

Configurar el router de forma segura y tener cuidado con las redes públicas.

Privacidad de webcam: mantener el control, tapar la cámara cuando no se usa.

Priorizar impresoras corporativas; evitar impresoras públicas o de establecimientos.

Guardar documentos estrictamente necesarios bajo llave, no dejarlos en cajones.

Conexión diaria a la VPN de Renfe (al menos una vez al día) para mantener equipo y software de protección actualizados.

Bloqueo de sesión y uso de filtros de privacidad al abandonar el equipo.

Evitar compartir información mediante USB para reducir vulnerabilidad a ficheros infectados.

4. Contraseñas seguras:

Caso de SolarWinds (2020-2021) como ejemplo de ciberataque por contraseña débil ("SolarWinds123").

Medidas de seguridad en Renfe: Doble Factor de Autenticación (DFA) para sistemas expuestos en internet, supervisión de cuentas privilegiadas, y política de contraseñas robustas.

Recomendaciones para contraseñas seguras:

No usar contraseñas "mono" (ej. "Renfe123").

No usar directamente palabras de diccionario.

Utilizar al menos 8 caracteres, incluyendo al menos una mayúscula y un símbolo.

Importante recordar: la combinación de usuario y contraseña es la identidad digital.

No compartir ni divulgar la contraseña.

No usar el email profesional de Renfe ni la misma contraseña de Renfe en redes sociales o webs ajenas a la empresa, para evitar que una brecha

de seguridad externa comprometa sistemas internos.

5. Credential Stuffing:

Definición: Ataque que explota la reutilización de credenciales por parte de los usuarios en diferentes webs. El ciberdelincuente usa credenciales robadas de una web comprometida para iniciar sesión en otras donde la víctima reutilizó esa información.

Medidas de protección de Renfe: Doble Factor de Autenticación (DFA) (dificulta el ataque), supervisión de cuentas privilegiadas y política de contraseñas robustas.

Renfe está implantando logs (registros) detallados de seguridad en el 100% de las aplicaciones expuestas a internet para detectar estos ataques lo antes posible.

Importancia de no reutilizar credenciales.

En caso de ser informado de una brecha de seguridad en una compañía, cambiar la contraseña de acceso en todas las páginas web a las que se tenga acceso, no solo las que compartan el mismo modo de acceso.

III. Protección de Dispositivos y Software

6. Parcheo de equipos:

Necesidad de mantener el software actualizado (parchearlo) para corregir fallos (funcionales o de seguridad) que pueden ser explotados por delincuentes.

Ejemplo: Vulnerabilidades críticas en servidores Microsoft Exchange (marzo 2021) que afectaron a organizaciones como la Autoridad Bancaria Europea (EBA).

Medios de protección en Renfe: Técnicos de sistemas y procedimientos de parcheo.

El servicio de inteligencia RENFE-CERT está al día sobre vulnerabilidades Zero Day y comunicaciones de proveedores para actuar rápidamente.

El RENFE-CERT comunica las necesidades de parcheo a la Gerencia de

Ciberseguridad para el Comité de Seguridad TIC.

Es crucial realizar el parcheo de equipos de usuario y servidores lo antes posible para evitar la explotación de vulnerabilidades y graves pérdidas económicas y reputacionales.

7. Internet de las cosas (IoT):

Definición: Tecnologías y dispositivos que detectan, comparten información a través de Internet y, a veces, actúan en función de ella (ej. teléfonos móviles, tabletas, televisiones, aspiradoras).

Riesgos/Vulnerabilidades:

Diseño sin controles de seguridad, falta de medidas contra accesos no autorizados.

Conexión a smartphones sin más seguridad que usuario y contraseña, susceptibles a tácticas de ciberdelincuentes.

Privacidad: almacenan gran cantidad de información personal que, si cae en malas manos, expone la privacidad.

Pérdida de Control: pueden ser inutilizados, mal funcionar o ser usados para actividades ilícitas.

Recomendaciones de uso:

Buscar información sobre vulnerabilidades del dispositivo.

Entender las políticas de privacidad del fabricante (qué información recogen, cómo la usan, etc.).

Mantener el dispositivo actualizado para parchear vulnerabilidades.

Desconectar o actualizar a una versión soportada si el fabricante ya no da soporte.

Ventajas (mencionadas en el documento, pero no detalladas en tu resumen): Permiten ahorro económico (monitorización, control), personalización e interacción entre dispositivos.

14. Malware:

Definición general de software malicioso.

Consecuencias de infección: probable reinstalación del equipo y pérdida de ficheros (estarán infectados).

Recomendaciones:

Tener copias de seguridad de documentos importantes.

Trabajar con documentos en servidores de Renfe.

Actualizar el antivirus de los portátiles por la VPN cuando se esté fuera de la empresa.

Confiabilidad del diagnóstico de infección del departamento de Seguridad TIC de Renfe.

No tener privilegios de administrador con el usuario de trabajo cotidiano, ya que facilita la propagación del malware.

Cuidado con dispositivos extraíbles (USBs).

IV. Ataques y Amenazas Comunes (Ingeniería Social y Ciberestafas)

8. Ataques de ingeniería social:

Suponen el 93% de las brechas de seguridad.

Principio básico: "el usuario es el eslabón más débil". Se busca explotar esto apelando a motivaciones personales para conseguir información o control del equipo.

Es más "fácil/barato" engañar a un usuario que vulnerar sistemas de seguridad.

Técnicas:

Pretexting: Creación de historias ficticias para que la víctima comparta información que normalmente no revelaría.

Phishing/Smishing/Vishing: "Pescar" víctimas usando correos, SMS o llamadas haciéndose pasar por una entidad de confianza.

Quid Pro Quo: Prometen un beneficio (regalo, dinero, acceso gratuito) a cambio de información personal.

Extorsión: Amenazan con distribuir contenido comprometido de la víctima si no acceden a peticiones (generalmente pagos).

Shoulder Surfing: Observar "por encima del hombro" para obtener información útil.

Redes Sociales: Técnicas de engaño a través de cupones, juegos y concursos.

Recomendaciones generales: Tratar con especial cuidado mensajes de remitente desconocido, desconfiar de chantajes/extorsiones, verificar comunicaciones sospechosas (ej. con el CAU o banco), y entidades bancarias nunca solicitan información confidencial por correo/SMS.

9. Ciberestafas:

España, en 2021, entre los países con más correos electrónicos de engaño para robar información o con contenido peligroso. Destacan los intentos de engaño a través de cobros de facturas falsas.

Consejos para comprobar la legitimidad de un mensaje de pago:

Mantenerse alerta ante correos de pago de facturas.

Revisar campos y contrastar información con facturas anteriores si se recibe por otro canal.

Contrastar cambios de número de cuenta con el personal de la empresa por otro canal (ej. teléfono).

Prestar atención a posibles cambios en el número de cuenta.

Comprobar que el dominio del correo remitente coincida con el oficial de la empresa.

Contactar directamente con la empresa si se recibe una factura duplicada.

No introducir datos personales o bancarios en webs accedidas por enlace de email.

No realizar transferencias bancarias sin confirmar legitimidad y autenticidad de la factura.

No enviar facturas para "revisión" si lo solicitan, ya que es una táctica para crear facturas falsas.

10. Correo electrónico malicioso:

Renfe utiliza la herramienta Proofpoint para análisis y protección.

Indicadores de maliciosidad:

Remitente: ¿Es esperado? Comprobar que el email coincida o si hay suplantación.

Asunto: Llamativo, impactante, inesperado (ej. "¡Has ganado un premio!").

Objeto del mensaje: Entidades como bancos nunca piden datos personales por correo. Sospechar de urgencia, amenazas, ofertas increíbles.

Enlaces: Verificar la URL real al pasar el cursor (o presionar en móvil); si no coincide o no tiene "https://", no hacer clic.

Redacción: Errores ortográficos, gramaticales, mala traducción, no personalizado.

Adjuntos: Archivos inesperados o sospechosos; analizar con antivirus antes de abrir.

Actuación: Eliminar el correo del buzón, no descargarlo. En caso de duda o infección, contactar con el Centro de Servicios (200100 – 911910000).

11. Secuestro digital:

Definición: Incapacitación del propietario para acceder y gestionar una cuenta, con el objetivo de obtener un rescate a cambio del control.

Basado en ingeniería social (phishing, smishing, vishing) para obtener datos personales/bancarios, haciendo creer que se comparte con alguien de confianza.

Ejemplo: Una persona que gestiona su negocio en una plataforma social popular, recibe un correo falso para "verificar su cuenta" solicitando cambio de contraseña.

Prevención: No facilitar demasiada información en redes sociales, activar el Doble Factor de Autenticación (DFA), usar contraseñas robustas y diferentes para cada servicio.

V. Desinformación y Conectividad Externa

12. Desinformación en el ciberespacio:

Objetivo: Alterar el funcionamiento de la opinión pública.

Pautas para verificar información:

Analizar la fuente (medio, trayectoria, periodistas, empresas, países).

Leer la noticia completa, contrastar datos, buscar pluralidad de opiniones.

Comprobar imágenes (fuente original, búsqueda inversa).

Dudar de contenidos políticos patrocinados por perfiles anónimos.

13. Riesgo en el uso de redes WiFi públicas:

Riesgo principal: Exposición de información y actividad a terceros.

Ataques comunes:

"Man-in-the-Middle": El atacante se interpone entre el dispositivo y la red Wi-Fi.

"Redes trampa": Redes Wi-Fi falsas creadas para engañar a los usuarios que se conectan automáticamente.

Recomendación: Priorizar el uso de datos móviles para información confidencial, especialmente en dispositivos corporativos.

VI. Aspectos Específicos de Dispositivos Móviles y Otros

18. Dispositivos móviles:

Pueden convertirse en herramientas de monitorización y geolocalización, por lo que su uso debe ser responsable.

19. Configuración segura de dispositivos móviles:

Configurar el perfil en redes sociales para proteger la privacidad.

20. Protección de la información en dispositivos móviles personales:

Mantener dispositivos y aplicaciones actualizadas, instalar un buen antivirus.

15. Phishing:

Se enfoca en correos fraudulentos, con especial énfasis en verificar sitios HTTPS y URLs.

16. Smishing:

Se enfoca en SMS fraudulentos, quid pro quo, y precaución con remitentes desconocidos.

17. Clasificación de la información (etiquetas):

(Solo mencionado como tema en el índice).

21. Vacaciones ciberseguras:

(Solo mencionado como tema en el índice).

22. Uso de dispositivos durante las vacaciones:

(Solo mencionado como tema en el índice).

23. Uso responsable de redes sociales: (Relacionado con la ingeniería social y desinformación). Implica pensar dos veces antes de publicar datos personales, planes, comportamientos inapropiados, información bancaria o sobre menores. Se debe controlar quién puede ver la información y recordar que "todo lo que se publica en internet permanecerá publicado".

24. Seguridad en compras online:

(Solo mencionado como tema en el índice, el segundo documento agrega: 3/10 consumidores compra online al menos 1 vez/mes, 2/10 cada semana. Formas de pago comunes: tarjeta, PayPal).

Resumen de Seguridad Informática - Renfe

Definiciones clave

Malware: Software malicioso diseñado para dañar, acceder o robar información de un sistema.
Phishing: Técnica de engaño para obtener información confidencial haciéndose pasar por una entidad confiable.
Smishing: Phishing realizado a través de mensajes SMS.
Vishing: Engaño telefónico para obtener datos personales o bancarios.
Credential Stuffing: Ataque que reutiliza credenciales robadas para acceder a otras cuentas del usuario.
Análisis de riesgos: Proceso para identificar amenazas, vulnerabilidades y aplicar controles que mitiguen los riesgos.
Cifrado: Mecanismo para proteger la información haciendo ilegible su contenido sin una clave de descifrado.
Secuestro digital: Pérdida de control de una cuenta o dispositivo debido a acceso indebido por parte de un atacante.

Buenas prácticas

• No abrir enlaces ni adjuntos sospechosos en correos electrónicos.
• Mantener el sistema operativo y el antivirus actualizados.
• Usar contraseñas seguras: al menos 8 caracteres, una mayúscula, un símbolo y sin datos personales.

Preguntas tipo test (1-25):

1. ¿Cuál es el principal objetivo de la seguridad informática en Renfe?

A) Prevenir incendios en servidores

B) Mejorar el rendimiento de las aplicaciones

✓ C) Proteger la confidencialidad, integridad y disponibilidad de la información

D) Aumentar el ancho de banda

2. ¿Qué tipo de información debe protegerse especialmente según el documento?

A) Información pública

B) Datos temporales

✓ C) Información confidencial y datos personales

D) Solo documentos internos de gestión

3. ¿Qué norma ISO se menciona como marco de referencia para la seguridad de la información?

✓ A) ISO/IEC 27001

B) ISO 9001

C) ISO 14001

D) ISO 20000

4. ¿Cuál es una de las funciones del Comité de Seguridad de la Información en Renfe?

A) Gestionar licencias de software

✓ B) Velar por el cumplimiento de las políticas de seguridad

C) Organizar formaciones técnicas

D) Revisar los diseños gráficos

5. ¿Qué concepto describe la capacidad de la información para estar accesible cuando se necesita?

A) Confidencialidad

B) Integridad

✓ C) Disponibilidad

D) Fiabilidad

6. ¿Qué medida técnica se implementa para garantizar la confidencialidad de la información?

A) Duplicación de servidores

✓ B) Cifrado de datos

C) Balanceo de carga

D) Instalación de antivirus

7. ¿Cuál es un ejemplo de amenaza lógica mencionado?

A) Terremoto

✓ B) Virus informático

C) Inundación

D) Corte de suministro eléctrico

8. ¿Qué se entiende por "control de accesos"?

✓ A) Limitación del acceso a los sistemas solo a personas autorizadas

B) Instalación de cámaras de vigilancia

C) Registro biométrico obligatorio

D) Cifrado de contraseñas

9. ¿Qué deben hacer los empleados si detectan un incidente de seguridad?

A) Solucionarlo por su cuenta

✓ B) Notificarlo inmediatamente al Responsable de Seguridad de la Información

C) Ignorarlo si no es grave

D) Informarlo al equipo de recursos humanos

10. ¿Qué principio se basa en dar a cada usuario solo los permisos mínimos necesarios?

A) Principio de redundancia

✓ B) Principio de mínimo privilegio

C) Principio de disponibilidad

D) Principio de acceso compartido

11. ¿Cuál de los siguientes se considera un activo de información?

A) Solamente documentos digitales

✓ B) Infraestructura, software y personal

C) Solo servidores físicos

D) Solo los datos sensibles

12. ¿Qué se debe hacer antes de introducir un nuevo sistema en producción?

A) Probarlo en el entorno real

✓ B) Realizar una evaluación de riesgos

C) Consultar al equipo de marketing

D) Publicarlo en la intranet

13. ¿Qué tipo de análisis se recomienda realizar periódicamente para detectar vulnerabilidades?

✓ A) Análisis de seguridad

B) Encuesta de satisfacción

C) Benchmarking

D) Auditoría contable

14. ¿Qué procedimiento aplica cuando se pierde un equipo portátil con datos sensibles?

A) Reemplazar el equipo sin notificación

✓ B) Seguir el protocolo de gestión de incidentes

C) Restaurar una copia de seguridad

D) Denunciarlo solo si el equipo es caro

15. ¿Cuál de los siguientes no es un principio de la seguridad de la información?

A) Confidencialidad

✓ B) Compatibilidad

C) Disponibilidad

D) Integridad

16. ¿Quién es responsable último de la protección de la información en Renfe?

✓ A) Toda la organización

B) El departamento de informática

C) El director de marketing

D) El proveedor externo

17. ¿Qué significa 'integridad' en el contexto de seguridad de la información?

A) Que la información está cifrada

✓ B) Que la información no ha sido alterada

C) Que es de acceso libre

D) Que los datos son públicos

18. ¿Cuál es un ejemplo de medida organizativa de seguridad?

A) Cortafuegos

✓ B) Políticas de seguridad

C) Antivirus

D) Cifrado de discos

19. ¿Qué herramienta permite monitorizar eventos sospechosos en sistemas?

A) Compresor de archivos

✓ B) Sistema de detección de intrusos (IDS)

C) Analizador de redes sociales

D) Impresora segura

20. ¿Qué acción se considera una buena práctica en el uso de contraseñas?

✓ A) Cambiarlas periódicamente

B) Usar fechas de nacimiento

C) Compartirlas entre compañeros

D) Escribirlas en una nota junto al monitor

21. ¿Qué elemento debe contener un Plan de Continuidad de Negocio?

✓ A) Procedimientos ante desastres

B) Listado de proveedores

C) Horario de los empleados

D) Estrategia comercial

22. ¿Qué se recomienda hacer tras resolver un incidente de seguridad?

A) Olvidarlo y seguir con las tareas

✓ B) Documentar lo ocurrido y aplicar medidas correctivas

C) Cambiar todo el sistema

D) Consultar al departamento legal

23. ¿Qué se entiende por trazabilidad en la seguridad de la información?

A) Capacidad de hacer copias

✓ B) Posibilidad de rastrear accesos y modificaciones

C) Uso de herramientas de trazado de red

D) Registro de llamadas telefónicas

24. ¿Qué función tiene el cifrado?

A) Eliminar datos obsoletos

B) Aumentar el tamaño de archivos

✓ C) Impedir el acceso a la información sin clave

D) Mejorar el rendimiento del sistema

25. ¿Qué rol tiene el Responsable de Seguridad de la Información?

A) Gestionar las bases de datos

✓ B) Coordinar e implementar las políticas de seguridad

C) Evaluar perfiles psicológicos

D) Organizar eventos internos

Preguntas tipo test (26–50):

26. ¿Qué se recomienda hacer con los documentos sensibles en la mesa de trabajo?

✓ A) Guardarlos bajo llave

B) Dejar una copia visible

C) Escanearlos y destruirlos

D) Dejarlo en la impresora

27. ¿Cuál de estos consejos aparece en el decálogo de ciberseguridad de Renfe?

✓ A) No abrir ficheros de correos sospechosos

B) Guardar claves en el navegador

C) Usar el correo de Renfe para registrarse en redes sociales

D) Desactivar el antivirus en vacaciones

28. ¿Qué es el Credential Stuffing?

A) Ataque DDoS distribuido

✓ B) Uso de credenciales robadas en múltiples sitios

C) Estafa bancaria vía SMS

D) Exfiltración de base de datos mediante malware

29. ¿Cuál es el principal riesgo de no parchear los equipos?

A) Pérdida de velocidad

✓ B) Explotación de vulnerabilidades por atacantes

C) Eliminación de archivos

D) Bloqueo de la red corporativa

30. ¿Qué ejemplo real se menciona como consecuencia del uso de contraseñas débiles?

A) Ataque a Renfe

B) Fuga de datos en Apple

✓ C) Ciberataque a SolarWinds

D) Robo de correos de Hacienda

31. ¿Qué normativa obliga a Renfe a realizar análisis de riesgos de seguridad?

✓ A) Esquema Nacional de Seguridad

B) ISO 9001

C) Reglamento Interno de Empleados

D) Convenio Colectivo de Transporte

32. ¿Qué acción es más eficaz contra el phishing?

A) Cambiar el fondo del navegador

✓ B) Verificar enlaces antes de hacer clic

C) Desactivar el antivirus

D) Usar correo personal

33. ¿Qué se debe hacer con un USB recibido de un tercero?

✓ A) No conectarlo al equipo

B) Formatearlo inmediatamente

C) Guardarlo en un cajón

D) Escanearlo y luego usarlo sin precauciones

34. ¿Qué se recomienda al navegar en redes públicas?

✓ A) Usar VPN

B) Desactivar el WiFi

C) Utilizar buscadores anónimos

D) Navegar solo por redes sociales

35. ¿Qué componente NO forma parte directa del análisis de riesgo?

A) Activos

B) Amenazas

✓ C) Política de cookies

D) Vulnerabilidades

36. ¿Qué tipo de red es más segura en vacaciones según el documento?

✓ A) Red cableada (Ethernet)

B) Red WiFi gratuita

C) Hotspot público

D) Red social interna

37. ¿Qué es un ataque “man-in-the-middle”?

A) Un tipo de ransomware

B) Un error del sistema operativo

✓ C) Interceptación de la comunicación entre dos partes

D) Control remoto autorizado

38. ¿Qué práctica reduce el riesgo de secuestro digital?

✓ A) Activar doble factor de autenticación

B) Usar siempre la misma contraseña

C) Compartir contraseñas con familiares

D) Ingresar desde redes abiertas

39. ¿Qué acción permite evitar el “shoulder surfing”?

✓ A) Usar filtros de privacidad en pantalla

B) Desactivar la webcam

C) Quitar el sonido del móvil

D) Eliminar correos antiguos

40. ¿Cuál de estas es una técnica de ingeniería social?

✓ A) Pretexting

B) Proxy inverso

C) Hashing

D) Tokenización

41. ¿Qué elemento se verifica para identificar un correo malicioso?

A) Fondo de pantalla

✓ B) Dominio del remitente

C) Número de párrafos

D) Fecha del envío

42. ¿Qué hacer ante la recepción de una factura sospechosa?

✓ A) Verificar el número de cuenta y el remitente

B) Pagar de inmediato

C) Imprimirla y archivarla

D) Reenviarla al superior

43. ¿Qué información debemos evitar compartir en redes sociales?

✓ A) Planes de vacaciones y datos bancarios

B) Fotos de viajes

C) Opiniones políticas

D) Enlaces de noticias

44. ¿Qué técnica usan los atacantes en casos de secuestro digital?

✓ A) Phishing

B) SQL Injection

C) Escaneo de puertos

D) Man-in-the-browser

45. ¿Qué característica debe tener una contraseña segura?

A) Usar nombre de la empresa

✓ B) Contener símbolos, mayúsculas y más de 8 caracteres

C) Ser recordable y corta

D) Utilizar el DNI

46. ¿Qué implica el cifrado de un dispositivo móvil?

✓ A) Que solo con la clave se puede acceder a los datos

B) Que consume menos batería

C) Que se bloquea al apagar

D) Que solo funciona en redes corporativas

47. ¿Qué es “quido pro quo” en el contexto de ciberseguridad?

A) Nombre de un software de cifrado

B) Un tipo de ransomware

✓ C) Técnica de ingeniería social basada en un favor a cambio

D) Código malicioso

48. ¿Qué NO debe hacerse tras un viaje si sospechamos de infección?

✓ A) Conectar los dispositivos a la red corporativa

B) Notificar al área de Ciberseguridad

C) Revisar comportamientos extraños

D) Eliminar archivos dudosos

49. ¿Qué tipo de contenido puede ocultar malware en correos?

✓ A) Archivos adjuntos inesperados

B) Firmas digitales

C) Pie de página

D) Texto en mayúsculas

50. ¿Qué puede causar la falta de control en dispositivos IoT?

A) Ahorro energético

✓ B) Acceso no autorizado y pérdida de privacidad

C) Mejora de la conectividad

D) Mayor velocidad en red

✓ Preguntas 51–75

51. ¿Qué permite la implementación del doble factor de autenticación?

A) Acceso sin contraseña

B) Acceso remoto sin VPN

✓ C) Mayor seguridad en el acceso

D) Evitar actualizaciones del sistema

52. ¿Cuál de las siguientes es una acción recomendada tras las vacaciones si se sospecha de ciberataque?

A) Reiniciar el dispositivo

✓ B) No conectar a la red corporativa

C) Cambiar el fondo de pantalla

D) Borrar el historial de navegación

53. ¿Qué debe hacerse antes de irse de vacaciones según el documento?

✓ A) Eliminar documentación sensible

B) Comprar un nuevo router

C) Usar redes sociales sin restricción

D) Compartir la contraseña por seguridad

54. ¿Cuál es el objetivo principal de las campañas de desinformación?

A) Cifrar los servidores

✓ B) Manipular la opinión pública

C) Bloquear cuentas bancarias

D) Robar credenciales

55. ¿Qué etiqueta de clasificación corresponde a información pública?

A) Alta

B) Media

C) Baja

✓ D) No valorable

56. ¿Qué práctica ayuda a evitar que un atacante observe nuestra pantalla?

✓ A) Uso de filtros de privacidad

B) Uso de colores oscuros

C) Reducción de brillo

D) Navegación en modo incógnito

57. ¿Qué deben contener las contraseñas según la política de Renfe?

✓ A) Mayúsculas, símbolos y más de 8 caracteres

B) Solo letras

C) Número de empleado

D) Dirección de correo

58. ¿Cuál es un peligro de los dispositivos IoT mal configurados?

A) Reducción de rendimiento

✓ B) Pérdida de privacidad y control

C) Interferencias WiFi

D) Errores visuales

59. ¿Qué debe hacerse si se recibe un SMS sospechoso con enlace?

✓ A) No acceder y eliminarlo

B) Llamar al número del SMS

C) Reenviarlo a compañeros

D) Guardarlo para comprobarlo más tarde

60. ¿Qué herramienta usa Renfe para filtrar correos maliciosos?

A) Outlook

✓ B) Proofpoint

C) Gmail

D) Norton

61. ¿Qué permite un buen uso de la clasificación de información?

✓ A) Aplicar medidas de seguridad apropiadas

B) Evitar el cifrado

C) Eliminar contraseñas

D) Conectar dispositivos personales

62. ¿Qué puede ocurrir si no se actualiza el software del móvil?

A) Aumenta la velocidad

✓ B) Quedan vulnerabilidades abiertas

C) Mejora la conectividad

D) Se formatea el dispositivo

63. ¿Qué se debe hacer si un dispositivo ha sido comprometido?

A) Reiniciarlo

B) Ignorarlo si funciona

✓ C) Contactar con el Centro de Servicios

D) Publicarlo en redes sociales

64. ¿Qué se recomienda al conectarse a redes WiFi abiertas?

✓ A) Evitar el acceso a información confidencial

B) Descargar películas

C) Usar el correo corporativo

D) Usar siempre el mismo dispositivo

65. ¿Qué tipo de información debemos evitar subir a redes sociales?

✓ A) Vacaciones, datos bancarios y personales

B) Noticias generales

C) Opiniones sobre tecnología

D) Reseñas de libros

66. ¿Cuál de estas NO es una técnica de ingeniería social?

A) Phishing

✓ B) Antivirus

C) Vishing

D) Smishing

67. ¿Qué tipo de ataque es el “hombre en el medio”?

✓ A) Interceptación de comunicaciones

B) Ataque físico

C) Cambio de hardware

D) Análisis de tráfico legal

68. ¿Qué hacer si detectas una factura con número de cuenta diferente al habitual?

✓ A) Confirmar por otro canal

B) Enviarla al banco

C) Eliminarla

D) Guardarla para revisión

69. ¿Qué técnica engañosa promete regalos a cambio de datos personales?

A) Vishing

✓ B) Quid Pro Quo

C) Shoulder Surfing

D) Malware

70. ¿Qué información guarda un dispositivo IoT que puede vulnerar nuestra privacidad?

✓ A) Hábitos de consumo, ubicación, datos personales

B) Solo el clima

C) Información bancaria exclusivamente

D) Datos biométricos

71. ¿Qué debe hacerse con redes WiFi almacenadas anteriormente?

✓ A) Eliminarlas

B) Compartirlas

C) Conectarse de nuevo

D) Desactivar el móvil

72. ¿Qué elemento no se considera un riesgo directo en ciberseguridad?

A) Phishing

✓ B) Actualización automática

C) Smishing

D) Malware

73. ¿Qué puede pasar si se conecta un USB infectado?

✓ A) Infección del sistema y robo de datos

B) Solo se bloquea

C) Pierde garantía

D) Se borra el contenido automáticamente

74. ¿Qué puede generar una fuga de información clasificada como ALTA?

✓ A) Grave daño reputacional, legal y económico

B) Daño menor

C) No tiene consecuencias

D) Solo bloqueos temporales

75. ¿Qué redacción es sospechosa en un correo fraudulento?

A) Texto sin errores

✓ B) Traducción burda y errores ortográficos

C) Firmas digitales

D) Nombre correcto del remitente

✓ Preguntas 76–100

76. ¿Qué se debe hacer si un atacante suplanta una web de alquiler vacacional?

✓ A) No continuar el proceso y verificar fuentes

B) Pagar rápido para reservar

C) Usar redes sociales para confirmar

D) Guardar el enlace para después

77. ¿Qué tipo de ataque explota la confianza del usuario?

✓ A) Ingeniería social

B) Ransomware

C) DoS

D) Sniffing

78. ¿Qué ventaja ofrece el cifrado del dispositivo móvil?

✓ A) Protege la información ante pérdida o robo

B) Mejora la batería

C) Evita actualizaciones

D) Aumenta la velocidad

79. ¿Qué permite el sistema de gestión MDM en móviles corporativos?

✓ A) Controlar aplicaciones y seguridad

B) Instalar apps personales

C) Acceder a redes sociales

D) Compartir datos entre móviles

80. ¿Qué característica tiene una red trampa WiFi?

✓ A) Simula una red legítima

B) Mejora la velocidad

C) Requiere contraseña segura

D) Tiene cifrado avanzado

81. ¿Qué hacer si se detecta una app desconocida tras recibir un SMS?

✓ A) Eliminarla y reportar

B) Ignorarla

C) Abrirla para verificar

D) Compartirla

82. ¿Qué se recomienda sobre el acceso a cuentas bancarias desde móvil?

✓ A) Usar solo aplicaciones oficiales

B) Guardar contraseñas en notas

C) Usar WiFi públicas

D) Compartir el acceso

83. ¿Qué aplicación NO debe usarse sin validación?

A) Word

✓ B) Aplicaciones de fuentes desconocidas

C) Outlook

D) Antivirus corporativo

84. ¿Qué se debe revisar antes de pagar una factura recibida por email?

✓ A) Dominio del remitente y número de cuenta

B) Cantidad de líneas

C) Tamaño del adjunto

D) Hora de recepción

85. ¿Qué organización fue afectada por un ataque a Exchange en 2021?

✓ A) Autoridad Bancaria Europea (EBA)

B) Facebook

C) INE

D) Agencia Tributaria

86. ¿Qué se recomienda respecto al uso de permisos en apps móviles?

✓ A) Limitar acceso innecesario

B) Aceptar todos por defecto

C) Activar todos al instalar

D) Compartir con otros

87. ¿Qué debe hacerse con las apps que no se usan?

✓ A) Desinstalarlas

B) Guardarlas en una carpeta

C) Bloquear notificaciones

D) Compartirlas

88. ¿Qué es OSINT?

✓ A) Búsqueda de información en fuentes públicas

B) Una base de datos

C) Una app de Renfe

D) Antivirus

89. ¿Qué ocurre si compartimos demasiada información en redes?

✓ A) Facilitamos ataques por ingeniería social

B) Mejora nuestra reputación

C) Aumenta la seguridad

D) Protege los datos

90. ¿Qué se recomienda sobre impresoras externas?

✓ A) Evitarlas, priorizar impresoras corporativas

B) Usarlas con claves

C) Compartirlas

D) Configurarlas por Bluetooth

91. ¿Qué debe hacerse si se pierde un dispositivo?

✓ A) Activar aplicaciones antirrobo y contactar con ciberseguridad

B) Apagar el móvil

C) Formatearlo

D) Guardar una copia

92. ¿Qué es Shoulder Surfing?

✓ A) Observar físicamente el contenido de la pantalla ajena

B) Acceso remoto por VPN

C) Suplantación de identidad

D) Lectura de correos

93. ¿Qué se recomienda hacer periódicamente en dispositivos móviles?

✓ A) Copias de seguridad cifradas

B) Reinicio completo

C) Desinstalación de antivirus

D) Cambiar el fondo de pantalla

94. ¿Qué hacer si se recibe una factura duplicada?

✓ A) Contactar con la empresa para aclararlo

B) Ignorarla

C) Cancelar la suscripción

D) Enviarla al banco

95. ¿Qué es Proofpoint?

✓ A) Filtro antispam y seguridad de correo

B) Aplicación de copia de seguridad

C) Sistema de alertas móviles

D) Plataforma de redes sociales

96. ¿Qué técnica evita la instalación de malware desde correos?

✓ A) No abrir enlaces o adjuntos sin verificar

B) Compartir correos sospechosos

C) Descargar todo en una carpeta

D) Enviar a todos los contactos

97. ¿Qué debe contener el bloqueo automático de pantalla?

✓ A) Activarse tras breve inactividad

B) Esperar 10 minutos

C) Estar siempre desactivado

D) Requiere apps externas

98. ¿Qué NO se debe hacer con un móvil antes de enviarlo a reparar?

✓ A) Entregarlo con datos sin borrar

B) Desinstalar apps

C) Cargar la batería

D) Avisar del problema

99. ¿Qué ocurre si se entrega un móvil antiguo sin borrado seguro?

✅ A) Pérdida o filtración de datos

B) Aumenta la garantía

C) Mejora la seguridad

D) Activa el modo seguro

100. ¿Cuál es el primer paso al recibir un correo malicioso?

✅ A) Eliminarlo sin abrir

B) Descargar el adjunto

C) Enviarlo al equipo

D) Responder para verificar

Aquí tienes una selección de preguntas tipo test sobre Seguridad Informática, extraídas del documento proporcionado. He intentado incluir preguntas de diversa dificultad y cubrir los temas más relevantes, como solicitaste. Si necesitas más, por favor házmelo saber.

Cuestionario de Seguridad Informática

1. Recomendaciones básicas de ciberseguridad

¿Qué tipo de conexión deben tener las páginas web que solicitan información confidencial?

a) HTTP

b) FTP

c) HTTPS

d) SMTP

Respuesta Correcta: c) HTTPS

Razón: El documento indica que las páginas web seguras deben comenzar con "https://".

Pista: Piensa en el protocolo de comunicación segura para la web.

Cuando navegas por internet, ¿qué se debe verificar sobre el navegador, plugins y extensiones?

a) Que estén deshabilitados.

b) Que estén actualizados correctamente.

c) Que sean de código abierto.

d) Que no requieran permisos.

Respuesta Correcta: b) Que estén actualizados correctamente.

Razón: Es fundamental mantener el navegador, plugins y extensiones al día para evitar vulnerabilidades.

Pista: Considera la importancia de las últimas versiones de software.

¿Qué se debe hacer si se recibe un correo con indicios o patrones fuera de lo habitual?

a) Abrir todos los enlaces para verificar.

b) Descargar los ficheros adjuntos para analizarlos.

c) No abrir ningún enlace ni descargar ningún fichero.

d) Reenviarlo a todos los contactos para alertar.

Respuesta Correcta: c) No abrir ningún enlace ni descargar ningún fichero.

Razón: El documento advierte contra la apertura de enlaces o descarga de ficheros de correos sospechosos.

Pista: Piense en la precaución ante correos electrónicos inusuales.

¿Cuál es la mejor defensa para prevenir y detectar contratiempos en el uso de sistemas TIC?

a) Contratar un seguro cibernético costoso.

b) Instalar múltiples antivirus.

c) La concienciación, el sentido común y las buenas prácticas.

d) Desconectar todos los dispositivos de internet.

Respuesta Correcta: c) La concienciación, el sentido común y las buenas prácticas.

Razón: El documento enfatiza que la concienciación y las buenas prácticas son las mejores defensas.

Pista: Piensa en el factor humano en la ciberseguridad.

Si tienes la mínima duda de que la seguridad de tu entorno laboral ha sido comprometida, ¿con quién debes contactar?

a) Con un amigo informático.

b) Con el Centro de Servicio (200100) o el Área de Ciberseguridad de Renfe.

c) Publicarlo en redes sociales para obtener ayuda.

d) Reiniciar el equipo varias veces.

Respuesta Correcta: b) Con el Centro de Servicio (200100) o el Área de Ciberseguridad de Renfe.

Razón: El procedimiento correcto es contactar a los departamentos internos de seguridad.

Pista: Piensa en el protocolo establecido para reportar incidentes de seguridad.

¿Qué tipo de conexiones a internet se deben emplear en lugares públicos para mayor fiabilidad?

a) Redes Wi-Fi abiertas.

b) Redes privadas virtuales (VPN).

c) Cualquier red disponible sin autenticación.

d) Conexiones Bluetooth.

Respuesta Correcta: b) Redes privadas virtuales (VPN).

Razón: Se recomienda el uso de VPNs para conexiones seguras en lugares públicos.

Pista: Piensa en cómo proteger tus datos en redes no seguras.

2. Análisis de riesgos de seguridad de la información

¿Qué es el análisis de riesgo en seguridad de la información?

a) Un proceso para eliminar todas las amenazas de un sistema.

b) Un proceso para identificar amenazas y vulnerabilidades con el fin de minimizarlas.

c) Una herramienta para automatizar la protección de datos.

d) Un informe anual sobre incidentes de seguridad.

Respuesta Correcta: b) Un proceso para identificar amenazas y vulnerabilidades con el fin de minimizarlas.

Razón: El análisis de riesgo busca identificar amenazas y vulnerabilidades para implementar controles que las minimicen.

Pista: Piensa en el propósito principal de un análisis de riesgo.

¿Qué normativa de seguridad obliga al Grupo Renfe a realizar Análisis de Riesgos de Seguridad?

a) Solo la Ley de Protección de Datos.

b) El Esquema Nacional de Seguridad (ENS) y otras leyes específicas.

c) La normativa europea de privacidad.

d) Ninguna normativa específica, es una recomendación interna.

Respuesta Correcta: b) El Esquema Nacional de Seguridad (ENS) y otras leyes específicas.

Razón: El documento menciona el ENS, la Ley de Protección de Infraestructuras Críticas, la Ley Orgánica de Protección de Datos Personales, y el Real Decreto-ley 12/2018.

Pista: Busca las menciones a marcos legales y regulaciones.

¿Cuál de las siguientes figuras NO es crucial para la realización de los Análisis de Riesgo en Renfe?

a) Responsable de la Información.

b) Responsable Funcional.

c) Responsable de Compras.

d) Responsable Técnico.

Respuesta Correcta: c) Responsable de Compras.

Razón: El documento nombra al Responsable de la Información, Funcional y Técnico como colaboradores clave.

Pista: Revisa los roles definidos para el proceso de análisis de riesgos.

¿Cuál de las siguientes NO es una forma de gestionar el riesgo de la información?

a) Evitar el riesgo.

b) Reducir o mitigar el riesgo.

c) Ignorar el riesgo y esperar lo mejor.

d) Transferir el riesgo.

Respuesta Correcta: c) Ignorar el riesgo y esperar lo mejor.

Razón: El documento describe evitar, reducir/mitigar, transferir y aceptar/monitorizar el riesgo.

Pista: Recuerda las estrategias activas para manejar riesgos.

3. Entorno de trabajo seguro

Debido a la situación derivada del COVID-19, ¿qué ha incrementado significativamente el uso de equipos portátiles?

a) La necesidad de trabajar en la oficina.

b) La alternancia de trabajo en la oficina y en casa.

c) Las reuniones presenciales.

d) El uso de impresoras corporativas.

Respuesta Correcta: b) La alternancia de trabajo en la oficina y en casa.

Razón: El teletrabajo y la alternancia de ubicaciones de trabajo han aumentado el uso de portátiles.

Pista: Piensa en el cambio en los hábitos laborales recientes.

¿Qué se recomienda hacer con la webcam cuando no se está usando?

a) Dejarla encendida para monitorización.

b) Taparla para evitar fraudes y robo de información.

c) Orientarla hacia la ventana.

d) Desinstalar el controlador.

Respuesta Correcta: b) Taparla para evitar fraudes y robo de información.

Razón: Se aconseja tapar la cámara cuando no está en uso para controlar la

privacidad.

Pista: Considera las precauciones para proteger tu privacidad visual.

En caso de necesitar imprimir un documento de trabajo, ¿qué se debe priorizar?

a) El uso de impresoras públicas o de establecimientos.

b) El uso de impresoras corporativas.

c) Enviar el documento por correo electrónico.

d) Imprimirlo en casa sin seguridad.

Respuesta Correcta: b) El uso de impresoras corporativas.

Razón: Se recomienda priorizar el uso de impresoras corporativas por seguridad.

Pista: Piensa en el control y la seguridad de los dispositivos de impresión.

Si trabajas desde casa, ¿con qué frecuencia se recomienda conectarse a la VPN de Renfe para mantener el equipo actualizado?

a) Una vez a la semana.

b) Al menos una vez al día.

c) Una vez al mes.

d) Nunca, si se usa una red Wi-Fi privada.

Respuesta Correcta: b) Al menos una vez al día.

Razón: Es importante conectarse a la VPN diariamente para recibir actualizaciones.

Pista: Considera la necesidad de actualizaciones constantes para la seguridad.

¿Qué acción se debe realizar siempre que se abandone el equipo para evitar miradas indiscretas?

a) Apagar el equipo por completo.

b) Bloquear la sesión y usar filtros de privacidad en la pantalla.

c) Dejar la sesión abierta.

d) Cubrir el teclado con un paño.

Respuesta Correcta: b) Bloquear la sesión y usar filtros de privacidad en la pantalla.

Razón: Se recomienda bloquear la sesión y usar filtros de privacidad para proteger la información en pantalla.

Pista: Piensa en medidas rápidas para proteger la información cuando te alejas del equipo.

4. Contraseñas seguras

¿Qué tipo de contraseña se considera "débil" según el ejemplo de SolarWinds?

a) Una contraseña con mayúsculas y números.

b) Una contraseña como "SolarWinds123".

c) Una contraseña de más de 12 caracteres.

d) Una contraseña generada aleatoriamente.

Respuesta Correcta: b) Una contraseña como "SolarWinds123".

Razón: El documento usa "SolarWinds123" como ejemplo de contraseña débil que fue explotada.

Pista: Recuerda el ejemplo de la brecha de seguridad mencionada en el texto.

¿Qué medida de seguridad exige Renfe para acceder a los sistemas expuestos en internet?

a) Solo contraseñas alfanuméricas.

b) Doble factor de autenticación.

c) Reconocimiento facial.

d) Contraseñas de menos de 8 caracteres.

Respuesta Correcta: b) Doble factor de autenticación.

Razón: Renfe requiere doble factor de autenticación para sistemas expuestos a internet.

Pista: Piensa en una capa adicional de seguridad para el acceso.

Para una contraseña segura, ¿cuántos caracteres como mínimo se deben utilizar?

a) 4

b) 6

c) 8

d) 10

Respuesta Correcta: c) 8

Razón: Se recomienda utilizar al menos 8 caracteres para una contraseña robusta.

Pista: Piensa en la longitud mínima sugerida para una contraseña fuerte.

¿Por qué NO se debe utilizar la dirección de correo profesional o la misma contraseña de Renfe en redes sociales o webs ajenas a la empresa?

a) Porque puede ralentizar el equipo.

b) Porque los ciberdelincuentes podrían acceder a su correo profesional y otros sistemas si esa web sufre una brecha.

c) Porque consume demasiados datos.

d) Porque no es ético.

Respuesta Correcta: b) Porque los ciberdelincuentes podrían acceder a su correo profesional y otros sistemas si esa web sufre una brecha.

Razón: Reutilizar credenciales puede comprometer los sistemas de Renfe si la web externa sufre una brecha.

Pista: Considera las consecuencias de la reutilización de credenciales.

¿Qué característica debe tener una contraseña segura además de la longitud mínima?

a) Solo letras minúsculas.

b) Usar directamente palabras de diccionario.

c) Al menos una mayúscula y un símbolo.

d) Ser fácil de recordar.

Respuesta Correcta: c) Al menos una mayúscula y un símbolo.

Razón: Las recomendaciones incluyen usar mayúsculas y símbolos para fortalecer la contraseña.

Pista: Piensa en la combinación de tipos de caracteres para una contraseña fuerte.

5. Credential Stuffing

¿Qué es el "Credential Stuffing"?

a) Un tipo de ataque que consiste en rellenar formularios automáticamente.

b) Un ataque que aprovecha la reutilización de credenciales por parte de los usuarios en diferentes webs.

c) Un método para cifrar contraseñas de forma segura.

d) Una técnica para generar contraseñas únicas.

Respuesta Correcta: b) Un ataque que aprovecha la reutilización de credenciales por parte de los usuarios en diferentes webs.

Razón: El Credential Stuffing se define como el aprovechamiento de la reutilización de credenciales.

Pista: Recuerda el concepto de "relleno" o "abuso" de credenciales.

¿Qué debe hacer un usuario si una compañía que tiene su información personal o credenciales ha sido comprometida?

a) No hacer nada, la empresa lo resolverá.

b) Cambiar la contraseña de acceso solo en la web comprometida.

c) Cambiar la contraseña de acceso en todas las páginas web a las que tenga

acceso, especialmente si compartió el mismo modo de acceso.

d) Reutilizar la misma contraseña pero añadiendo un número.

Respuesta Correcta: c) Cambiar la contraseña de acceso en todas las páginas web a las que tenga acceso, especialmente si compartió el mismo modo de acceso.

Razón: Es crucial cambiar las contraseñas en todas las webs afectadas, no solo en la comprometida, debido a la posible reutilización de credenciales o de otros datos complementarios.

Pista: Considera el impacto de una brecha en una cuenta cuando se reutilizan contraseñas.

¿Qué medida de seguridad dificulta los ataques de Credential Stuffing en Renfe?

a) Solo contraseñas alfanuméricas.

b) No usar el correo electrónico como identificador.

c) Requerir doble factor de autenticación para los sistemas expuestos en internet.

d) Limitar el número de intentos de inicio de sesión.

Respuesta Correcta: c) Requerir doble factor de autenticación para los sistemas expuestos en internet.

Razón: El doble factor de autenticación es una defensa clave contra el Credential Stuffing.

Pista: Piensa en cómo una verificación adicional puede frustrar a los atacantes.

¿Qué está trabajando Renfe en implantar para detectar ataques de Credential Stuffing lo antes posible?

a) Sistemas de reconocimiento facial.

b) Logs (registros) detallados de seguridad en el 100% de las aplicaciones expuestas a internet.

c) Nuevos algoritmos de cifrado.

d) Un equipo de hackers éticos.

Respuesta Correcta: b) Logs (registros) detallados de seguridad en el 100% de las aplicaciones expuestas a internet.

Razón: Renfe está implantando registros de seguridad detallados para una detección temprana de ataques.

Pista: Considera la importancia de la trazabilidad y el monitoreo para la detección de ataques.

6. Parcheo de equipos

¿Por qué es importante mantener los equipos "parcheados"?

a) Para mejorar la velocidad del equipo.

b) Para evitar que los delincuentes aprovechen los fallos de seguridad.

c) Para cambiar la interfaz de usuario.

d) Para instalar nuevas aplicaciones.

Respuesta Correcta: b) Para evitar que los delincuentes aprovechen los fallos de seguridad.

Razón: El parcheo es esencial para "tapar" las fallas de seguridad que los delincuentes explotan.

Pista: Piensa en el propósito de las actualizaciones de seguridad.

¿Qué caso real se menciona en el documento como ejemplo de la importancia del parcheo?

a) Un ataque a un sistema de Renfe.

b) Un ciberataque a los servidores de Microsoft Exchange de la Autoridad Bancaria Europea (EBA) en 2021.

c) Un robo de datos en una red social.

d) Un ataque de denegación de servicio a un banco.

Respuesta Correcta: b) Un ciberataque a los servidores de Microsoft Exchange de la Autoridad Bancaria Europea (EBA) en 2021.

Razón: El incidente de la EBA con los servidores Microsoft Exchange es el ejemplo principal.

Pista: Recuerda el ejemplo específico de una vulnerabilidad de software mencionada.

¿Qué puede provocar el no realizar el parcheo de los equipos en tiempo y forma?

a) Pequeñas fallas estéticas en el sistema.

b) Que un atacante explote una vulnerabilidad para hacerse con el control del equipo.

c) Un aumento en el rendimiento del equipo.

d) Una reducción en el consumo de energía.

Respuesta Correcta: b) Que un atacante explote una vulnerabilidad para hacerse con el control del equipo.

Razón: La falta de parcheo a tiempo puede permitir a los atacantes explotar vulnerabilidades y tomar el control.

Pista: Piensa en las consecuencias más graves de una vulnerabilidad no corregida.

¿Qué equipo de Renfe está al día sobre las vulnerabilidades Zero Day y las comunicaciones de proveedores para actuar rápidamente?

a) El equipo de Recursos Humanos.

b) El Servicio de Inteligencia del equipo de respuesta a incidentes RENFE-CERT.

c) El departamento de Marketing.

d) El equipo de Soporte Técnico General.

Respuesta Correcta: b) El Servicio de Inteligencia del equipo de respuesta a incidentes RENFE-CERT.

Razón: El RENFE-CERT es responsable de mantenerse informado sobre vulnerabilidades y comunicaciones de proveedores.

Pista: Busca la entidad específica encargada de la inteligencia de amenazas.

7. Internet de las cosas (IoT)

¿Qué son los dispositivos IoT?

a) Dispositivos que solo detectan información.

b) Tecnologías y dispositivos que detectan, comparten información a través de Internet y, en algunos casos, actúan en función de ella.

c) Dispositivos que solo se usan en entornos industriales.

d) Equipos que no requieren conexión a internet.

Respuesta Correcta: b) Tecnologías y dispositivos que detectan, comparten información a través de Internet y, en algunos casos, actúan en función de ella.

Razón: La definición de IoT incluye la detección, el intercambio de información y la capacidad de acción.

Pista: Piensa en la naturaleza interconectada y funcional de estos dispositivos.

¿Cuál es la principal vulnerabilidad de seguridad en el diseño de muchos dispositivos IoT?

a) Su alto costo.

b) La falta de medidas de seguridad que los protejan de accesos no autorizados.

c) Su tamaño reducido.

d) La dificultad de uso.

Respuesta Correcta: b) La falta de medidas de seguridad que los protejan de accesos no autorizados.

Razón: El documento destaca la falta de controles de seguridad, especialmente la protección contra accesos no autorizados, como la principal vulnerabilidad.

Pista: Piensa en las deficiencias de seguridad inherentes al diseño de ciertos dispositivos.

¿Qué tipo de información personal almacenan los dispositivos IoT, lo que supone un riesgo para la privacidad?

a) Solo información de uso del dispositivo.

b) Una gran cantidad de información personal.

c) Ninguna información personal.

d) Solo datos técnicos del dispositivo.

Respuesta Correcta: b) Una gran cantidad de información personal.

Razón: Los dispositivos IoT a menudo almacenan mucha información personal, lo que expone la privacidad si cae en malas manos.

Pista: Considera la cantidad de datos que estos dispositivos pueden recopilar sobre los usuarios.

Si un fabricante deja de dar soporte a un dispositivo IoT, ¿qué se recomienda hacer con él?

a) Seguir usándolo normalmente.

b) Desconectarlo o actualizarlo a una versión soportada.

c) Intentar parchearlo por cuenta propia.

d) Venderlo a otro usuario.

Respuesta Correcta: b) Desconectarlo o actualizarlo a una versión soportada.

Razón: En caso de fin de soporte, se aconseja desconectar el dispositivo o actualizarlo a una versión con soporte.

Pista: Piensa en la falta de actualizaciones de seguridad en dispositivos sin soporte.

¿Qué beneficio económico aportan los dispositivos IoT?

a) Aumento del consumo de energía.

b) Ahorro económico al permitir monitorizar y controlar el funcionamiento de

dispositivos.

c) Mayor costo de mantenimiento.

d) Necesidad de más personal para su gestión.

Respuesta Correcta: b) Ahorro económico al permitir monitorizar y controlar el funcionamiento de dispositivos.

Razón: Los dispositivos IoT pueden generar ahorro al permitir la monitorización y control.

Pista: Piensa en la eficiencia y automatización que ofrecen estos dispositivos.

8. Ataques de ingeniería social

¿Qué porcentaje de las brechas de seguridad se atribuyen a ataques de ingeniería social?

a) 50%

b) 75%

c) 93%

d) 100%

Respuesta Correcta: c) 93%

Razón: El documento afirma que los ataques de ingeniería social suponen el 93% de las brechas de seguridad.

Pista: Recuerda el dato estadístico específico sobre el impacto de la ingeniería social.

¿Cuál es el principio básico en el que se basa la ingeniería social?

a) La tecnología es el eslabón más débil.

b) El usuario es el eslabón más débil.

c) El hardware es vulnerable.

d) El software siempre tiene fallos.

Respuesta Correcta: b) El usuario es el eslabón más débil.

Razón: La ingeniería social se fundamenta en la premisa de que "el usuario es el eslabón más débil".

Pista: Piensa en el punto de ataque más común en la ingeniería social.

¿Qué técnica de ingeniería social implica crear un escenario/historia ficticia para que la víctima comparta información que normalmente no revelaría?

a) Phishing.

b) Extorsión.

c) Pretexting.

d) Shoulder Surfing.

Respuesta Correcta: c) Pretexting.

Razón: El Pretexting se describe como la elaboración de un escenario ficticio para obtener información.

Pista: Considera la creación de una "excusa" o "pretexto" para engañar.

¿Qué es el "Shoulder Surfing"?

a) Un ataque que usa mensajes SMS.

b) Consiste en mirar por "encima del hombro" para obtener información.

c) Un tipo de fraude con regalos.

d) Una técnica para suplantar identidades en línea.

Respuesta Correcta: b) Consiste en mirar por "encima del hombro" para obtener información.

Razón: El Shoulder Surfing se define como la observación de lo que escribe o tiene en pantalla otro usuario.

Pista: Piensa en la vigilancia visual de la información.

¿Por qué los ciberdelincuentes utilizan la ingeniería social en lugar de vulnerar sistemas de seguridad?

a) Porque es más costoso y difícil.

b) Porque es más fácil o "barato" engañar a alguien para que revele su contraseña.

c) Porque no tienen conocimientos técnicos.

d) Porque los sistemas de seguridad son invulnerables.

Respuesta Correcta: b) Porque es más fácil o "barato" engañar a alguien para que revele su contraseña.

Razón: La ingeniería social es preferida por ser un método más "fácil o barato" para obtener información.

Pista: Considera la eficiencia y el costo-beneficio para el atacante.

9. Ciberestafas

¿Qué tipo de correos maliciosos destacan en España en 2021 por intentar engañar a la víctima a través de cobros?

a) Correos con ofertas de empleo falsas.

b) Correos de facturas falsas.

c) Correos de donaciones benéficas.

d) Correos de supuestas herencias.

Respuesta Correcta: b) Correos de facturas falsas.

Razón: El documento destaca los correos con cobros de facturas falsas como una modalidad prevalente de ciberestafa.

Pista: Piensa en un tipo de engaño económico común.

Si te notifican por correo electrónico un cambio en el número de cuenta de una empresa, ¿qué se recomienda hacer antes de actuar?

a) Realizar la transferencia inmediatamente para evitar recargos.

b) Contrastar esta información con el personal de la empresa contratada utilizando otro canal (ejemplo: teléfono).

c) Asumir que es legítimo si el logo de la empresa aparece.

d) Responder al correo pidiendo más detalles.

Respuesta Correcta: b) Contrastar esta información con el personal de la empresa contratada utilizando otro canal (ejemplo: teléfono).

Razón: Es crucial verificar cambios de cuenta por un canal alternativo para confirmar la legitimidad.

Pista: Piensa en la necesidad de doble verificación para información crítica.

¿Qué se debe hacer si recibes una factura duplicada?

a) Ignorarla y esperar una nueva.

b) Contactar directamente con la empresa contratada para notificar el error.

c) Pagarla de nuevo por si acaso.

d) Borrarla sin investigar.

Respuesta Correcta: b) Contactar directamente con la empresa contratada para notificar el error.

Razón: Se aconseja contactar a la empresa para informar sobre facturas duplicadas.

Pista: Considera el paso lógico para resolver una inconsistencia en la facturación.

¿Qué se debe evitar hacer, incluso si lo solicitan, con una factura para que "sea revisada antes de tramitarla"?

a) Pagarla sin revisar.

b) Enviarla para su revisión.

c) Imprimirla.

d) Guardarla en un lugar seguro.

Respuesta Correcta: b) Enviarla para su revisión.

Razón: El documento advierte que enviar la factura para "revisión" es una técnica de los atacantes para conformar una factura falsa.

Pista: Piensa en cómo los atacantes podrían usar una factura original para crear una falsa.

10. Correo electrónico malicioso

¿Qué herramienta de Renfe ayuda a eliminar la mayoría de correos electrónicos maliciosos?

a) Un filtro de spam genérico.

b) La herramienta de análisis y protección contra el correo electrónico malicioso Proofpoint.

c) Un antivirus de escritorio.

d) Un sistema de bloqueo de remitentes.

Respuesta Correcta: b) La herramienta de análisis y protección contra el correo electrónico malicioso Proofpoint.

Razón: Proofpoint es la herramienta específica de Renfe mencionada para la protección de correo electrónico.

Pista: Recuerda el nombre de la solución de seguridad de correo electrónico.

Para distinguir un correo electrónico malicioso de uno legítimo, ¿qué se debe hacer con los enlaces?

a) Hacer clic inmediatamente para comprobar la página.

b) Situar el cursor encima del enlace (o mantener presionado en móvil) para ver la URL real.

c) Confiar en el texto del enlace.

d) Compartirlo con un amigo para que lo revise.

Respuesta Correcta: b) Situar el cursor encima del enlace (o mantener presionado en móvil) para ver la URL real.

Razón: Es una pauta clave para verificar la legitimidad de los enlaces.

Pista: Piensa en cómo verificar la dirección de destino de un enlace sin hacer clic.

¿Qué característica en la redacción de un correo electrónico puede indicar que es malicioso?

a) Estar personalizado.

b) No tener errores ortográficos.

c) Tener errores ortográficos o parecer una mala traducción.

d) Ser formal y profesional.

Respuesta Correcta: c) Tener errores ortográficos o parecer una mala traducción.

Razón: Los errores de ortografía, gramaticales o redacciones que parecen traducciones automáticas son indicadores de correos maliciosos.

Pista: Piensa en las señales de falta de profesionalidad en un correo electrónico.

Si un correo tiene un archivo adjunto que no esperabas o es sospechoso, ¿qué se recomienda hacer?

a) Abrirlo para ver el contenido.

b) Analizarlo con el antivirus de Renfe antes de abrirlo.

c) Reenviarlo para pedir confirmación.

d) Cambiar la extensión del archivo.

Respuesta Correcta: b) Analizarlo con el antivirus de Renfe antes de abrirlo.

Razón: Se aconseja analizar los adjuntos antes de abrirlos, confiando en el antivirus.

Pista: Piensa en el riesgo de abrir archivos adjuntos no solicitados.

Si recibes un correo electrónico con características de ser malicioso, ¿cuál es la primera acción que debes tomar?

a) Abrir todos los enlaces y adjuntos para investigar.

b) Proceder a eliminarlo de tu buzón de correo y no descargarlo.

c) Reenviarlo al Centro de Servicios.

d) Publicarlo en redes sociales para alertar.

Respuesta Correcta: b) Proceder a eliminarlo de tu buzón de correo y no descargarlo.

Razón: La acción inmediata es eliminarlo y no descargarlo.

Pista: Piensa en la acción más directa para evitar una amenaza de correo electrónico.

11. Secuestro digital

¿A qué se refiere el término "secuestro digital"?

a) Al robo de un dispositivo físico.

b) A la incapacitación por parte del propietario de una cuenta a su acceso y gestión, con el objetivo de obtener un rescate.

c) Al cifrado de archivos personales.

d) Al robo de identidad para abrir nuevas cuentas.

Respuesta Correcta: b) A la incapacitación por parte del propietario de una cuenta a su acceso y gestión, con el objetivo de obtener un rescate.

Razón: El secuestro digital se define como la incapacitación del acceso a una cuenta para pedir un rescate.

Pista: Piensa en una situación donde pierdes el control de tus cuentas online por un fin monetario.

¿Qué tipo de fraude se menciona como base de muchos ciberataques de secuestro digital?

a) Malware.

b) Phishing, smishing o vishing.

c) Ataques de fuerza bruta.

d) DDoS.

Respuesta Correcta: b) Phishing, smishing o vishing.

Razón: Estos ataques de ingeniería social son la base para obtener datos personales y bancarios, facilitando el secuestro digital.

Pista: Recuerda las técnicas de ingeniería social que buscan obtener información personal.

¿Qué recomendación se da para protegerse del secuestro digital en redes sociales?

a) Facilitar la mayor cantidad de información personal posible.

b) No facilitar demasiada información a través de tus redes sociales.

c) Compartir todas las credenciales con amigos de confianza.

d) Usar la misma contraseña para todas las cuentas.

Respuesta Correcta: b) No facilitar demasiada información a través de tus redes sociales.

Razón: Publicar menos información en redes sociales reduce el riesgo de ser objetivo.

Pista: Piensa en la precaución al compartir detalles personales en plataformas públicas.

¿Qué medida de seguridad esencial se recomienda activar en tus cuentas para protegerte del secuestro digital?

a) Solo cambiar la contraseña con frecuencia.

b) Desactivar las notificaciones.

c) Activar el doble factor de autenticación.

d) No usar contraseñas robustas.

Respuesta Correcta: c) Activar el doble factor de autenticación.

Razón: Activar el doble factor de autenticación es una recomendación clave.

Pista: Piensa en una capa adicional de seguridad que verifica tu identidad.

¿Qué se recomienda hacer con las contraseñas para cada servicio?

a) Usar la misma contraseña para todos los servicios.

b) Establecer contraseñas robustas y diferentes para cada servicio.

c) Usar contraseñas cortas y fáciles de recordar.

d) No usar contraseñas, solo el nombre de usuario.

Respuesta Correcta: b) Establecer contraseñas robustas y diferentes para cada servicio.

Razón: Usar contraseñas únicas y robustas para cada servicio previene el secuestro masivo de cuentas.

Pista: Piensa en cómo una brecha en una cuenta puede afectar a otras si las contraseñas se repiten.

12. Desinformación en el ciberespacio

¿Cuál es el principal objetivo de una campaña de desinformación en el ciberespacio?

a) Alterar los sistemas informáticos de empresas.

b) Alterar el funcionamiento de la opinión pública.

c) Recopilar datos personales.

d) Realizar ciberataques financieros.

Respuesta Correcta: b) Alterar el funcionamiento de la opinión pública.

Razón: El objetivo principal es influir en la opinión pública a través de noticias falsas, medias verdades, etc.

Pista: Piensa en el impacto de la desinformación en la percepción colectiva.

¿Qué se debe analizar sobre la fuente de una noticia antes de confiar en ella?

a) Solo su popularidad.

b) Qué medio la publica, su trayectoria, y qué periodistas, empresas o países se encuentran detrás de la publicación.

c) Si tiene muchas "me gusta" en redes sociales.

d) Si la noticia es sensacionalista.

Respuesta Correcta: b) Qué medio la publica, su trayectoria, y qué periodistas, empresas o países se encuentran detrás de la publicación.

Razón: Es fundamental analizar la fuente, su trayectoria y los actores detrás de la publicación.

Pista: Piensa en la necesidad de verificar la credibilidad de la fuente.

Al informarse en formatos digitales, ¿qué se recomienda hacer más allá de solo leer el titular y ver una fotografía?

a) Compartirla inmediatamente.

b) Leer la noticia completa y analizar si los datos están contrastados y si las citas recogen pluralidad de opiniones.

c) Buscar si la noticia ha sido publicada en un blog.

d) Ignorar el contenido y solo ver los comentarios.

Respuesta Correcta: b) Leer la noticia completa y analizar si los datos están contrastados y si las citas recogen pluralidad de opiniones.

Razón: Se aconseja una lectura completa y un análisis crítico de la información.

Pista: Piensa en la importancia de ir más allá del contenido superficial.

¿Qué se debe hacer para comprobar si una imagen es original o ha sido copiada de internet?

a) Solo confiar en el texto que la acompaña.

b) Acudir siempre a la fuente original o hacer una "búsqueda inversa".

c) Compartirla para que otros la verifiquen.

d) Descargarla y modificarla.

Respuesta Correcta: b) Acudir siempre a la fuente original o hacer una "búsqueda inversa".

Razón: La búsqueda inversa y la verificación de la fuente original son métodos clave.

Pista: Piensa en herramientas o técnicas para rastrear el origen de una imagen.

¿Por qué se debe dudar de todo contenido político patrocinado por perfiles anónimos o no identificados?

a) Porque no son estéticos.

b) Porque pueden obtener ingresos económicos a cambio de patrocinar

determinado contenido.

c) Porque suelen ser muy aburridos.

d) Porque la política es un tema sensible.

Respuesta Correcta: b) Porque pueden obtener ingresos económicos a cambio de patrocinar determinado contenido.

Razón: Los perfiles anónimos o no identificados podrían estar patrocinando contenido a cambio de dinero, lo que afecta la objetividad.

Pista: Piensa en la posible motivación económica detrás de la difusión de contenido político anónimo.

13. Riesgo en el uso de redes WiFi públicas

¿Cuál es el mayor riesgo al conectarse a una red Wi-Fi pública?

a) La lentitud de la conexión.

b) Dejar expuesta toda nuestra información y actividad a terceros.

c) Que el dispositivo se descargue rápidamente.

d) La dificultad para acceder a ciertas páginas web.

Respuesta Correcta: b) Dejar expuesta toda nuestra información y actividad a terceros.

Razón: El riesgo principal es la exposición de datos y actividad a ciberdelincuentes.

Pista: Piensa en la falta de seguridad inherente a estas redes abiertas.

¿Qué tipo de ataque permite a un ciberdelincuente situarse entre tu dispositivo y la conexión Wi-Fi para monitorear tu tráfico de datos?

a) Ataque de fuerza bruta.

b) Ataque de denegación de servicio (DDoS).

c) "Man-in-the-Middle" u "hombre en el medio".

d) Ataque de phishing.

Respuesta Correcta: c) "Man-in-the-Middle" u "hombre en el medio".

Razón: Este ataque se describe como el intermediario entre el dispositivo y la conexión Wi-Fi para espiar el tráfico.

Pista: Piensa en un atacante que intercepta la comunicación.

¿Qué tipo de ataque en redes públicas implica crear una red Wi-Fi con las mismas características que la original para engañar a los usuarios?

a) Ataques de inyección SQL.

b) "Redes trampa".

c) Ataques de día cero.

d) Ransomware.

Respuesta Correcta: b) "Redes trampa".

Razón: Las "redes trampa" son creadas por atacantes para imitar redes legítimas y monitorear la actividad del usuario.

Pista: Piensa en una red Wi-Fi falsa que atrae a los usuarios.

¿Qué opción suele tener activada el dispositivo, lo que lo hace vulnerable a las "redes trampa"?

a) El modo avión.

b) La opción de "conectarse automáticamente a la red Wi-Fi más cercana".

c) El Bluetooth activado.

d) El modo de ahorro de energía.

Respuesta Correcta: b) La opción de "conectarse automáticamente a la red Wi-Fi más cercana".

Razón: Esta función puede hacer que el dispositivo se conecte automáticamente a una red trampa.

Pista: Piensa en la configuración de conectividad automática que podría ser perjudicial.

¿Qué se recomienda priorizar en caso de acceder a información confidencial cuando se usa un teléfono corporativo?

a) El uso de redes Wi-Fi públicas.

b) El uso de datos móviles.

c) Desactivar todas las conexiones.

d) Conectarse a cualquier red disponible.

Respuesta Correcta: b) El uso de datos móviles.

Razón: Se aconseja priorizar los datos móviles, especialmente en dispositivos

corporativos, para navegar desde la red interna de Renfe.

Pista: Piensa en la seguridad de la red interna de la empresa frente a las redes públicas.

14. Malware

¿Qué es el Malware?

a) Software que mejora el rendimiento del sistema.

b) Un término genérico para software malicioso diseñado para dañar, interrumpir o acceder sin autorización a sistemas informáticos.

c) Un tipo de hardware de seguridad.

d) Un programa para optimizar la batería.

Respuesta Correcta: b) Un término genérico para software malicioso diseñado para dañar, interrumpir o acceder sin autorización a sistemas informáticos.

Razón: (Este concepto se deduce del contexto general del documento sobre seguridad informática, aunque no haya una definición literal de una sola frase).

Pista: Piensa en el significado amplio de "software malicioso".

Si tu equipo se infecta, ¿qué es lo más probable que tengas que hacer y qué ocurrirá con tus ficheros?

a) Solo reiniciar el equipo y los ficheros estarán intactos.

b) Reinstalar todo el equipo y no podrás utilizar los ficheros infectados.

c) Solo ejecutar un antivirus y los ficheros se recuperarán automáticamente.

d) Desconectar el equipo de la red y seguir trabajando.

Respuesta Correcta: b) Reinstalar todo el equipo y no podrás utilizar los ficheros infectados.

Razón: El documento indica que, si te infectas, es probable que tengas que reinstalar y los ficheros estarán infectados.

Pista: Piensa en las consecuencias severas de una infección por malware.

¿Qué se recomienda tener de los documentos más importantes para protegerse contra el malware?

a) Guardarlos solo en el equipo infectado.

b) No hacer copias de seguridad.

c) Tener copias de seguridad.

d) Compartirlos en la nube pública.

Respuesta Correcta: c) Tener copias de seguridad.

Razón: Se aconseja tener copias de seguridad de documentos importantes.

Pista: Piensa en la resiliencia de los datos ante un ataque.

Si tienes acceso a servidores de almacenamiento en la red de Renfe, ¿qué se aconseja hacer con los documentos?

a) Trabajarlos solo localmente en tu equipo.

b) Trabajar con los documentos en esos servidores.

c) Copiarlos a un USB personal.

d) Eliminarlos después de usarlos.

Respuesta Correcta: b) Trabajar con los documentos en esos servidores.

Razón: Se recomienda trabajar con documentos en los servidores de almacenamiento de Renfe.

Pista: Piensa en la seguridad y centralización de la información corporativa.

¿Qué deben hacer los portátiles de Renfe cuando están fuera de la empresa para actualizar el antivirus?

a) Conectarse a cualquier red Wi-Fi pública.

b) No necesitan actualizarse fuera de la empresa.

c) Actualizar el antivirus por la VPN.

d) Desactivar el antivirus.

Respuesta Correcta: c) Actualizar el antivirus por la VPN.

Razón: Los portátiles deben actualizar el antivirus mediante la VPN cuando están fuera de la empresa.

Pista: Piensa en cómo se mantiene la seguridad de los equipos portátiles móviles.

15. Phishing

¿Qué es el Phishing?

a) Un tipo de ataque que instala software malicioso directamente.

b) Un ataque que usa correos electrónicos fraudulentos para engañar a la víctima y obtener información confidencial.

c) Un método para acelerar la conexión a internet.

d) Una técnica para hacer copias de seguridad.

Respuesta Correcta: b) Un ataque que usa correos electrónicos fraudulentos para

engañar a la víctima y obtener información confidencial.

Razón: El Phishing se describe como una técnica que utiliza correos electrónicos, SMS o llamadas telefónicas donde el atacante se hace pasar por una organización/persona de confianza para que la víctima revele información privada.

Pista: Piensa en el anzuelo para obtener información.

¿Qué técnica de engaño se emplea comúnmente en el Phishing, Smishing y Vishing?

a) Amenazas directas de daño físico.

b) Hacerse pasar por una organización/persona de confianza.

c) Interceptar el tráfico de red sin interacción del usuario.

d) Bloquear el acceso a archivos del usuario.

Respuesta Correcta: b) Hacerse pasar por una organización/persona de confianza.

Razón: En estas técnicas, el atacante se hace pasar por una entidad de confianza.

Pista: Piensa en la suplantación de identidad.

¿Qué se debe verificar en las páginas web al navegar por internet para asegurar que son seguras?

a) Que tengan muchos colores.

b) Que comiencen con https y que la dirección del portal pertenezca a la URL de la entidad.

c) Que sean populares en redes sociales.

d) Que no pidan ningún tipo de información.

Respuesta Correcta: b) Que comiencen con https y que la dirección del portal pertenezca a la URL de la entidad.

Razón: Se recomienda verificar que la página sea segura (https) y que la URL sea la oficial de la entidad.

Pista: Piensa en los indicadores de seguridad en la barra de direcciones del navegador.

¿Qué es una de las principales señales de un correo malicioso, relacionada con el remitente?

a) Que sea de un remitente conocido y esperado.

b) Que el email no coincida con la persona o entidad remitente que dice ser o que esté suplantando a alguien.

c) Que el remitente sea un servicio oficial del gobierno.

d) Que contenga solo texto y no imágenes.

Respuesta Correcta: b) Que el email no coincida con la persona o entidad remitente que dice ser o que esté suplantando a alguien.

Razón: Comprobar la identidad del remitente es crucial para detectar suplantaciones.

Pista: Piensa en la autenticidad del origen del mensaje.

16. Smishing

¿Qué es el Smishing?

a) Un ataque de ingeniería social realizado a través de llamadas telefónicas.

b) Un ataque de ingeniería social realizado a través de mensajes SMS fraudulentos.

c) Un tipo de virus informático.

d) Una técnica para robar contraseñas de redes Wi-Fi.

Respuesta Correcta: b) Un ataque de ingeniería social realizado a través de mensajes SMS fraudulentos.

Razón: El documento lo clasifica junto al phishing y vishing como técnicas que emplean correos electrónicos, SMS o llamadas telefónicas.

Pista: Piensa en la variación del phishing que utiliza mensajes de texto.

¿Qué prometen a menudo los ataques de Quid Pro Quo (relacionados con Phishing/Smishing/Vishing)?

a) Amenazas de cárcel.

b) Un beneficio a cambio de información personal, a menudo en formato regalo.

c) Un aumento salarial.

d) La mejora de la conexión a internet.

Respuesta Correcta: b) Un beneficio a cambio de información personal, a menudo en formato regalo.

Razón: El Quid Pro Quo se describe como una promesa de beneficio a cambio de información personal, a menudo regalos.

Pista: Piensa en el intercambio de algo por algo ("quid pro quo").

¿Qué se recomienda si se recibe algún mensaje de remitente desconocido?

a) Abrirlo y responder de inmediato.

b) Tratarlo con especial cuidado.

c) Compartirlo con todos los contactos.

d) Marcarlo como leído.

Respuesta Correcta: b) Tratarlo con especial cuidado.

Razón: Se aconseja tratar con especial cuidado los mensajes de remitentes desconocidos.

Pista: Piensa en la precaución ante mensajes de fuentes no verificadas.

17. Clasificación de la información (etiquetas)

Aunque el documento menciona la "Clasificación de la información (etiquetas)" como un tema, ¿qué información detallada se proporciona sobre este concepto en los snippets?

a) Una descripción detallada de cómo etiquetar la información.

b) Un listado de diferentes categorías de etiquetas.

c) Ejemplos de sistemas de clasificación de Renfe.

d) No se proporciona información detallada sobre este tema en los snippets disponibles.

Respuesta Correcta: d) No se proporciona información detallada sobre este tema en los snippets disponibles.

Razón: El índice del temario lo lista, pero el contenido de los snippets no profundiza

en ello.

Pista: Revisa si hay texto explicativo más allá del título del tema.

18. Dispositivos móviles

¿En qué pueden convertirse los dispositivos móviles, lo que requiere un uso responsable?

a) En simples teléfonos.

b) En dispositivos de monitorización y geolocalización.

c) En herramientas exclusivas de ocio.

d) En equipos sin capacidad de almacenamiento.

Respuesta Correcta: b) En dispositivos de monitorización y geolocalización.

Razón: Se señala que los dispositivos móviles pueden usarse para monitorizar y geolocalizar.

Pista: Piensa en las capacidades de seguimiento de los dispositivos móviles modernos.

19. Configuración segura de dispositivos móviles

Para proteger la privacidad en redes sociales, ¿qué se debe hacer con la configuración del perfil?

a) Dejarla predeterminada.

b) Configurar el perfil de manera que permita proteger la privacidad.

c) Compartir toda la información públicamente.

d) Conectar la cuenta con todas las aplicaciones posibles.

Respuesta Correcta: b) Configurar el perfil de manera que permita proteger la privacidad.

Razón: Se recomienda configurar el perfil en redes sociales para proteger la privacidad.

Pista: Piensa en los ajustes de privacidad que puedes controlar en tus perfiles.

20. Protección de la información en dispositivos móviles personales

¿Qué se recomienda hacer para evitar posibles vulnerabilidades en dispositivos y aplicaciones móviles?

a) No actualizar nunca el software.

b) Mantener los dispositivos y aplicaciones actualizados.

c) Desinstalar todas las aplicaciones.

d) Usar redes Wi-Fi públicas sin seguridad.

Respuesta Correcta: b) Mantener los dispositivos y aplicaciones actualizados.

Razón: Se aconseja mantener los dispositivos y aplicaciones actualizados para evitar vulnerabilidades.

Pista: Piensa en cómo se tapan las brechas de seguridad en el software.

Además de mantener actualizados los dispositivos y aplicaciones, ¿qué otra medida de seguridad se recomienda instalar en dispositivos móviles personales?

a) Un navegador web específico.

b) Un buen antivirus.

c) Un bloqueador de anuncios.

d) Un gestor de contraseñas.

Respuesta Correcta: b) Un buen antivirus.

Razón: Se recomienda instalar un buen antivirus para mantener los dispositivos protegidos.

Pista: Piensa en la protección contra software malicioso.

21. Vacaciones ciberseguras

Aunque el documento menciona "Vacaciones ciberseguras", ¿qué tipo de información se ofrece en los snippets sobre este tema?

a) Consejos detallados para asegurar dispositivos en vacaciones.

b) Una lista de destinos seguros para vacaciones.

c) No se proporciona información específica sobre este tema en los snippets.

d) Recomendaciones para compras online durante las vacaciones.

Respuesta Correcta: c) No se proporciona información específica sobre este tema en los snippets.

Razón: El índice del temario lo lista, pero el contenido de los snippets no profundiza en ello.

Pista: Revisa si hay texto explicativo más allá del título del tema.

22. Uso de dispositivos durante las vacaciones

Si bien se menciona el "Uso de dispositivos durante las vacaciones", ¿se proporciona algún consejo específico sobre este punto en los snippets?

a) Sí, sobre cómo usar el VPN en hoteles.

b) No, solo se lista como tema.

c) Sí, sobre cómo proteger fotos de vacaciones.

d) Sí, sobre la configuración de cámaras.

Respuesta Correcta: b) No, solo se lista como tema.

Razón: El índice del temario lo lista, pero el contenido de los snippets no profundiza en ello.

Pista: Revisa si hay texto explicativo más allá del título del tema.

23. Uso responsable de redes sociales

¿Qué técnica de engaño es común a través de las redes sociales, mediante cupones descuento, juegos y concursos?

a) Ataque de día cero.

b) Extorsión.

c) Ingeniería social a través de redes sociales.

d) Shoulder Surfing.

Respuesta Correcta: c) Ingeniería social a través de redes sociales.

Razón: El documento lista "Redes Sociales" como una de las técnicas de engaño.

Pista: Piensa en las trampas comunes en plataformas sociales.

Para una opinión bien formada, crítica y contrastada en el contexto de la desinformación, ¿qué se recomienda sobre las fuentes de información?

a) Quedarse solo con las fuentes que nos muestran los algoritmos.

b) Obtener fuentes de información alternativas a las que nos muestran los algoritmos en las plataformas digitales.

c) Solo confiar en lo que comparten los amigos.

d) Buscar solo noticias que confirmen nuestras ideas.

Respuesta Correcta: b) Obtener fuentes de información alternativas a las que nos muestran los algoritmos en las plataformas digitales.

Razón: Se aconseja buscar fuentes alternativas para una opinión crítica.

Pista: Piensa en la burbuja de filtro y la necesidad de diversidad de información.

24. Seguridad en compras online

Aunque el documento menciona "Seguridad en compras online", ¿qué tipo de información detallada se proporciona sobre este concepto en los snippets?

a) Recomendaciones específicas para pagos seguros.

b) Ejemplos de tiendas online seguras.

c) No se proporciona información detallada sobre este tema en los snippets.

d) Cómo usar tarjetas de crédito online.

Respuesta Correcta: c) No se proporciona información detallada sobre este tema en los snippets.

Razón: El índice del temario lo lista, pero el contenido de los snippets no profundiza en ello.

Pista: Revisa si hay texto explicativo más allá del título del tema.

Preguntas Rebuscadas / Profundas (Basadas en Inferencias o Detalles)

Si un usuario de Renfe tiene un usuario de trabajo cotidiano con privilegios de administrador y se infecta con malware, ¿cuál es la consecuencia principal mencionada en el documento?

a) La infección se limitará a su equipo.

b) La propagación del malware será más fácil.

c) Solo afectará a sus documentos personales.

d) El antivirus lo detectará de inmediato sin problemas.

Respuesta Correcta: b) La propagación del malware será más fácil.

Razón: El documento advierte que si el usuario es administrador y se infecta, la propagación del malware será más sencilla.

Pista: Piensa en el nivel de acceso y su impacto en la seguridad.

¿Cuál es la implicación de que un certificado de una página web en una red Wi-Fi pública pueda ser "emitido al vuelo por un atacante"?

a) El atacante solo puede ver la dirección IP.

b) La comunicación está completamente segura.

c) El atacante puede monitorear todo el tráfico de datos del usuario, incluso si la comunicación parece cifrada.

d) El usuario debe actualizar su navegador.

Respuesta Correcta: c) El atacante puede monitorear todo el tráfico de datos del usuario, incluso si la comunicación parece cifrada.

Razón: Esto es una característica del ataque "Man-in-the-Middle" donde el atacante intercepta y monitorea el tráfico.

Pista: Piensa en la falsificación de certificados en una conexión insegura.

¿Qué se menciona como una de las mecánicas que están empleando los atacantes para conformar una factura falsa, partiendo de una original?

a) Pedir al usuario que envíe una factura para "ser revisada antes de tramitarla".

b) Enviar la factura en un formato de imagen inmodificable.

c) Solicitar el número de tarjeta de crédito para verificar la factura.

d) Usar un dominio de correo electrónico completamente diferente.

Respuesta Correcta: a) Pedir al usuario que envíe una factura para "ser revisada antes de tramitarla".

Razón: Esta técnica se describe específicamente como un método para que los atacantes creen facturas falsas a partir de originales.

Pista: Piensa en cómo un atacante podría obtener una plantilla para una factura falsa.

En el contexto de los ataques de desinformación, ¿por qué es importante "dudar de los pantallazos que recibas en redes sociales"?

a) Porque tienen baja resolución.

b) Porque una imagen puede haber sido publicada antes y manipulada, lo que se puede comprobar con una "búsqueda inversa" o información EXIF.

c) Porque ocupan mucho espacio en el dispositivo.

d) Porque no se pueden compartir fácilmente.

Respuesta Correcta: b) Porque una imagen puede haber sido publicada antes y manipulada, lo que se puede comprobar con una "búsqueda inversa" o información EXIF.

Razón: La recomendación de dudar de los pantallazos se basa en la posibilidad de que las imágenes hayan sido manipuladas o sean antiguas.

Pista: Piensa en la facilidad de edición y reutilización de imágenes digitales.

¿Cuál es el riesgo de que la Oficina de Riesgo y Marco, encargada de la elaboración de los Análisis de Riesgos en Renfe, no cuente con la colaboración de un "Responsable Técnico"?

a) Que el análisis de riesgos se enfoque solo en aspectos funcionales.

b) Que no se identifiquen las amenazas y vulnerabilidades desde el punto de vista tecnológico.

c) Que no se establezcan las medidas para el tratamiento del riesgo.

d) Que el diseño de sistemas y tratamientos sea ineficaz.

Respuesta Correcta: b) Que no se identifiquen las amenazas y vulnerabilidades desde el punto de vista tecnológico.

Razón: El Responsable Técnico tiene el mayor conocimiento del sistema desde el punto de vista técnico, y su ausencia dejaría un vacío en la identificación de vulnerabilidades tecnológicas.

Pista: Piensa en el rol específico del responsable técnico en el proceso.

¿Por qué se afirma que "en ningún caso se transfiere la responsabilidad del riesgo, sino su tratamiento" al transferir el riesgo (ej. contratando un seguro)?

a) Porque la aseguradora asume toda la responsabilidad.

b) Porque el responsable de la información sigue siendo el último en decidir sobre las medidas de tratamiento del riesgo.

c) Porque el riesgo desaparece por completo.

d) Porque es una obligación legal.

Respuesta Correcta: b) Porque el responsable de la información sigue siendo el último en decidir sobre las medidas de tratamiento del riesgo.

Razón: Aunque el tratamiento se transfiera, la responsabilidad final de la gestión del riesgo recae en el Responsable de la Información.

Pista: Piensa en la diferencia entre delegar la gestión y delegar la rendición de cuentas.

Si los ciberdelincuentes acceden a tus dispositivos IoT, ¿qué tipo de actividades ilícitas podrían llegar a realizar con ellos?

a) Solo cambiar la hora del dispositivo.

b) Inutilizarlos, provocar un mal funcionamiento o incluso realizar actividades ilícitas.

c) Encender y apagar las luces.

d) Actualizar el firmware sin tu permiso.

Respuesta Correcta: b) Inutilizarlos, provocar un mal funcionamiento o incluso realizar actividades ilícitas.

Razón: El riesgo de pérdida de control incluye la posibilidad de que los atacantes realicen actividades ilícitas con los dispositivos.

Pista: Piensa en el control que un atacante podría obtener sobre un dispositivo conectado.

¿Qué ventaja de los dispositivos IoT permite que el GPS del coche, a cierta distancia de casa, mande una señal al termostato para encender la calefacción?

a) Ahorro económico.

b) Personalización.

c) Interacción.

d) Monitoreo de constantes vitales.

Respuesta Correcta: c) Interacción.

Razón: El ejemplo describe la comunicación entre diferentes dispositivos para facilitar la vida del usuario, lo cual es parte de la interacción IoT.

Pista: Piensa en la comunicación entre dispositivos como una característica clave.

Si el departamento de Seguridad TIC de Renfe asegura que un equipo está infectado, ¿cuál debe ser la reacción del usuario según el documento?

a) Dudar y pedir una segunda opinión.

b) No dudarlo, está infectado.

c) Intentar desinfectarlo por sí mismo.

d) Ignorar la advertencia.

Respuesta Correcta: b) No dudarlo, está infectado.

Razón: El documento es categórico: "Si el departamento de Seguridad TIC de Renfe te asegura que equipo está infectado, no lo dudes, está infectado."

Pista: Piensa en la autoridad y el conocimiento de los expertos en seguridad interna.

¿Cuál es el riesgo de aceptar USBs de desconocidos o utilizar USBs abandonados, incluso si parecen provenir de un stand comercial?

a) Podrían contener solo archivos promocionales.

b) Podrían contener ficheros infectados.

c) Podrían ser solo dispositivos de almacenamiento vacíos.

d) Podrían tener una capacidad de almacenamiento limitada.

Respuesta Correcta: b) Podrían contener ficheros infectados.

Razón: El documento advierte contra la conexión de dispositivos extraíbles de terceros, implicando el riesgo de infección.

Pista: Piensa en la fuente no confiable y el peligro oculto.

Si un ciberdelincuente accede a una cuenta de red social mediante un secuestro digital y cambia la contraseña y los datos para restablecer el acceso (número de teléfono y correo electrónico), ¿cuál es la consecuencia directa para el propietario?

a) El propietario puede recuperar la cuenta fácilmente con su contraseña antigua.

b) El propietario tiene que esperar a que la red social le devuelva el acceso automáticamente.

c) El propietario pierde el control de la cuenta y no puede volver a tomarlo.

d) El propietario solo pierde algunas fotos.

Respuesta Correcta: c) El propietario pierde el control de la cuenta y no puede volver a tomarlo.

Razón: El cambio de contraseña y datos de recuperación impide al propietario recuperar el control de la cuenta.

Pista: Piensa en las barreras que un atacante crea para mantener el control.

¿Por qué es importante para la seguridad que el usuario de trabajo cotidiano NO tenga privilegios de administrador?

a) Para evitar que instale software no autorizado.

b) Para que la propagación del malware sea más difícil en caso de infección.

c) Para que el equipo funcione más rápido.

d) Para reducir el consumo de recursos del sistema.

Respuesta Correcta: b) Para que la propagación del malware sea más difícil en caso de infección.

Razón: Si un usuario con privilegios de administrador se infecta, el malware se propagará más fácilmente.

Pista: Piensa en el impacto del nivel de permisos en la contención de amenazas.

¿Cuál es una de las "situaciones a evitar" relacionadas con el momento óptimo para

la realización del Análisis de Riesgos de Seguridad (AARR)?

a) Realizarlo al inicio de la "Idea de Negocio".

b) Realizarlo durante el "Diseño de Sistemas y tratamientos".

c) Realizarlo después de la "Explotación" del servicio.

d) Realizarlo antes de la "Construcción".

Respuesta Correcta: c) Realizarlo después de la "Explotación" del servicio.

Razón: El gráfico en el documento indica que el "Momento Óptimo realización AARR" está antes de la "Explotación", y las fases posteriores son "Situaciones a evitar".

Pista: Observa el diagrama de flujo y el momento ideal vs. las situaciones no recomendadas.

¿Qué se recomienda en el decálogo de ciberseguridad sobre la eliminación de documentación sensible de los dispositivos?

a) Borrarla manualmente sin herramientas especiales.

b) No eliminarla, solo moverla.

c) Eliminarla empleando herramientas de borrado seguro.

d) Imprimirla y luego borrarla.

Respuesta Correcta: c) Eliminarla empleando herramientas de borrado seguro.

Razón: Se aconseja utilizar herramientas de borrado seguro para la documentación sensible.

Pista: Piensa en la permanencia de la información al borrarla.

En el contexto de los correos electrónicos maliciosos, ¿qué se entiende por "ASUNTO" llamativo e impactante?

a) Un asunto que es muy aburrido y formal.

b) Un asunto que intenta captar la atención del usuario, como "¡Has ganado un premio!".

c) Un asunto que es una respuesta a un correo previo.

d) Un asunto que solo contiene números.

Respuesta Correcta: b) Un asunto que intenta captar la atención del usuario, como "¡Has ganado un premio!".

Razón: Los correos fraudulentos usan asuntos llamativos para captar la atención, y se da el ejemplo de "¡Has ganado un premio!".

Pista: Piensa en los titulares de correo electrónico diseñados para ser irresistibles.

¿Qué tipo de información NO deben solicitar nunca las entidades bancarias por correo electrónico, SMS o cualquier otro canal?

a) Información general sobre sus servicios.

b) Información confidencial.

c) Confirmación de citas.

d) Recordatorios de promociones.

* Respuesta Correcta: b) Información confidencial.

*

Razón: El documento enfatiza que las entidades bancarias nunca solicitan información confidencial por estos canales.

* Pista: Piensa en la política de seguridad de los bancos respecto a la solicitud de datos sensibles.