SEGURIDAD INFORMÁTICA

ASPECTOS IMPORTANTES

1. RECOMENDACIONES BÁSICAS DE SEGURIDAD INFORMÁTICA.

- Verificar WEBS que solicitan info. Confidencial sean: SEGURAS (Candado y https://).
- No clicar en links de webs desconocidas.
- No abrir archivos adjuntos de emails desconocidos.
- No usuario, contraseña o email de Renfe a sitios ajenos.
- No conectar dispositivos personales a sistemas o redes de Renfe.
- No conectarse a WIFI personal o no aprobado dentro de instalaciones de Renfe.
- No USB abandonados ni de desconocidos.
- Informar a CENTRO DE SERVICIOS (200 100) sobre: correos, enlaces, ficheros u otro incidente de ciberseguridad sospechoso.

DECÁLOGO DE RECOMENDACIONES BÁSICAS EN CIBERSEGURIDAD.

- **TIC:** Tecnologías de la Información y Comunicación.
- ¿Dudas de que la seguridad de tu entorno laboral ha sido comprometida? Contacta con: **CENTRO DE SERVICIO (200 100)** o **ÁREA DE CIBERSEGURIDAD DE RENFE** (ciberseguridad@renfe.es).
- **10 consejos** para trabajar de forma segura.

2. ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

- **Definición** Análisis de Riesgo: "*Proceso que permite identificar las amenazas y vulnerabilidades de una aplicación o servicio con el objetivo de identificar los controles que minimicen los riesgos, el cual implica determinar qué o cuáles activos proteger, de qué o de quién hay que protegerlos y cómo hacerlo".*

Normativa de aplicación para Renfe que le obliga a hacer análisis de riesgos:

- **Esquema Nacional de Seguridad (ENS).**
- **Ley de Protección de Infraestructuras Críticas (Ley 8/2011).**
- **Ley Orgánica de Protección de Datos y Garantías de los Derechos Digitales.**

- **2ª Definición** de Análisis de Riesgos (Tener en cuenta ambas y memorizarlas por si preguntan una u otra): "*Mecanismo que nos permite gestionar el riesgo de una determinada aplicación y servicio y nos ayuda a contar son los mecanismos de defensa necesarios para prevenir, responder o detectar un posible incidente de seguridad".*

Gerencia de Ciberseguridad y Privacidad: Tienen a la Oficina de Riesgo y Marco (con presencia en las sociedades del Grupo Renfe). Mails de contacto: rmviajeros.seguridad.tic@renfe.es, rm.seguridad.tic@renfe.es, ciberseguridad@renfe.es

¿Quién elabora los Análisis de Riesgos?: **Oficina de Riesgo y Marco**.

¿Con quién se colabora para realizar los Análisis de Riesgos?:

- **1. Responsable de la Información:** Responsable Final para establecer las medidas para el tratamiento del riesgo. ("SOMOS NOSOSTROS") ⟶ ¿Cómo gestionamos el riesgo?: Evitar riesgo, Reducir o Mitigar riesgo, Transferir riesgo y Aceptar el riesgo sin implementar controles adicionales (monitorizarlo para confirmar que no se incrementa).
- **2. Responsable Funcional:** Responsable con mayor conocimiento del sistema o aplicación desde un punto de vista FUNCIONAL.
- **3. Responsable Técnico:** Responsable con mayor conocimiento del sistema o aplicación desde un punto de vista TÉCNICO.

3. ENTORNO DE TRABAJO SEGURO.

COVID 19 ⟶ TELETRABAJO ⟶ POSIBLE NUEVA VENTANA CIBERDELINCUENCIA.

- **Consejos** para ayudar al ÁREA DE CIBERSEGURIDAD a garantizar la SEGURIDAD INFO. GRUPO RENFE (trabajando en Oficina o desde Casa):

1. ROUTER/WIFI
2. DOCUMENTOS EN LA MESA
3. DISPOSITIVOS EXTRAIBLES (USB)
4. WEBCAM
5. IMPRESORAS
6. ACTUALIZACIONES
7. PRIVACIDAD.

4. CONTRASEÑAS SEGURAS.

Historia Incidente SolarWinds.

Medidas de Seguridad de Renfe (para protegerse ante ciberataques por contraseñas):

- **Doble factor autentificación**.
- **Supervisión de cuentas privilegiadas**.
- Política de **contraseñas robustas** en los sistemas.

Contraseña segura:

- No contraseñas "mono": ej. Renfe123.
- No palabras de diccionario.
- Sí 8 caracteres (al menos).
- Sí 1 Mayúscula (al menos).
- Sí 1 Símbolo (al menos).

Importante recordar:

- ❖ Usuario + Contraseña = IDENTIDAD DIGITAL.
- ❖ No compartas, No divulgues (la contraseña).
- ❖ No email profesional de Renfe en RRSS o WEBS AJENAS.
- ❖ No misma contraseña que usas en Renfe en RRSS o WEBS AJENAS.

5. CREDENTIAL STUFFING.

Definición Credential Stuffing: (Término en inglés) "*Tipo de ataque que aprovecha la reutilización de credenciales por parte de los usuarios, en diferentes webs.*

*El ciberdelincuente una vez robadas de una web que haya sido comprometida (por él o por un tercero) las credenciales e información complementaria, puede utilizar dichas contraseñas e información complementaria para iniciar sesión **en otras** webs en las que la víctima haya **reutilizado** esa información y credenciales".*

Medidas de protección de Renfe ante Credential Stuffing:

- ❖ **Doble Factor Autentificación.**
- ❖ **Supervisión Cuentas Privilegiadas.**
- ❖ **Contraseñas Robustas.**
- ❖ *"Estamos trabajando"* en implantar **Logs (Registros) detallados de seguridad** en el 100% de aplicaciones expuestas a internet (con el objetivo de: detectar lo antes posible el Credential Stuffing).

Importante recordar:

- ❖ Usuario + Contraseña = IDENTIDAD DIGITAL.
- ❖ No reutilizar Credenciales.
- ❖ No usar Usuario y Contraseña de Renfe en WEBS AJENAS.
- ❖ No compartas, No divulgues (la contraseña o usuario).
- ❖ **Cambiar contraseñas de TODAS WEBS** a las que tengas acceso (cuando se te informe de Credential Stuffing).

6. PARCHEO DE EQUIPOS.

- A lo largo de la vida de un Software se le descubren FALLOS: (FUNCIONALES o SEGURIDAD). ¿Solución?: "Tapar los fallos": **ACUTALIZACIÓN SOFTWARE (PARCHE)**.
- Caso MICROSOFT.

Medidas de protección de Renfe.

- **Técnicos de Sistemas** y **Procedimientos** (para correcto parcheo).
- **RENFE-CERT (Servicio de Inteligencia del equipo de respuesta a incidentes)**: está al día de:
  1.- Vulnerabilidades *ZERO DAY* publicadas.
  2.- Comunicaciones realizadas por nuestros proveedores.
- RENFE-CERT: ¿*Cómo*, *a quién* y *para qué* comunica las vulnerabilidades?
  - ¿Cómo?: A través de la **GERENCIA DE CIBERSEGURIDAD** mediante comunicaciones.
  - ¿A quién?: Al **COMITÉ DE SEGURIDAD TIC**.
  - ¿Para qué?: Para las necesidades de Parcheo de los equipos para hacer frente a las vulnerabilidades.
- ¿Por qué es importante lo anterior?:
  1.- Comunicaciones proactivas.
  2.- Parchear lo antes posible.

Importante recordar:

- ❖ Parcheo de equipos lo antes posible (tras recibir comunicaciones de vulnerabilidades).
- ❖ No parchear equipos en tiempo y forma puede suponer ciberataque.
- ❖ No parchear puede provocar pérdidas (económicas y reputacionales).
- ❖ Seguir indicaciones de RENFE-CERT y colaborar con los Responsables de Servicios.

7. CIBERSEGURIDAD EN DISPOSITIVOS. INTERNET DE LAS COSAS (IoT).

- **Definición** de IoT: *Tecnologías y dispositivos que detectan información y la comparten a través de Internet y, en algunos casos, actúan en función de ella*.
- La mayoría de dispositivos inteligentes permiten intercambio de info. a través de conexiones inalámbricas.
- Conocer los riesgos nos permite protegernos adecuadamente.
- Ejemplos de IoT en la sociedad: Tráfico, Suministros, Domótica, Salud y Comercios.

- Ventajas de IoT:
  - **1.- Ahorro económico**.
  - **2.- Personalización**.
  - **3.- Interacción**.

- Riesgos de IoT:
  - **1.- Ciberseguridad.**
  - **2.- Privacidad.**
  - **3.- Pérdida de control.**

- Recomendaciones de uso de IoT:
  - **1.- Hacer una búsqueda sobre el dispositivo y sus posibles vulnerabilidades.**
  - **2.- Entender las políticas de privacidad del fabricante y el dispositivo.**
  - **3.- Mantener el dispositivo al día con las "actualizaciones".**

8. ATAQUES DE INGIENERÍA SOCIAL.

- **Definición** Ingeniería Social: *Se basa en un principio muy básico: "**el usuario es el eslabón más débil**". A partir de esta idea, busca explotarlo apelando a sus motivaciones más personales, con el objetivo de conseguir que el usuario revele cierta información o permita tomar el control de su equipo*.

- ¿Nuestra mejor defensa?:
  - 1.- No dejarnos engañar.
  - 2.- Conocer cómo funcionan estos fraudes y engaños.

- Para el ciberdelincuente es más fácil o barato engañarnos que vulnerar los sistemas de seguridad.

Principales modos de ataques de ingeniería social:
1.- Pretexting.
2.- Extorsión.
3.- Phishing / Smishing / Vishing.
4.- Shoulder Surfing.

5.- Quid Pro Quo.
6.- Redes Sociales.

Recomendaciones para disminuir posibilidades de ser víctima:

- Mensajes de remitente desconocido: Trátalo con especial cuidado.
- Desconfía de chantajes, extorsiones o mensajes alarmantes (normalmente no tiene tu información privada).
- Desconfía del supuesto "Técnico/Trabajador" que te pide que te descargues una aplicación.
- ¿Estás seguro de que es una comunicación legítima?: Aun así, verifícalo.
- Las entidades bancarias NUNCA solicitan info. confidencial por email o SMS.
- Webs empiecen por https.

9. CIBERESTAFAS.

- **Correos maliciosos:** Intentan el cobro de **FACTURAS FALSAS**.
- **Consejos** para comprobar que no se trata de un engaño para cobrar una factura falsa.

10. CORREO ELECTRÓNICO MALICIOSO.

- **Proofpoint:** *Herramienta de análisis y protección contra el correo electrónico malicioso que dispone Renfe*.
- Desconfía de correos que piden abrir un archivo adjunto o pinchar en un enlace.
- **Pautas para distinguir entre: Correo malicioso y Correo legítimo**.
- **¿Cómo actuar si recibimos un correo malicioso**?:
  1.- Elimínalo y no lo descargues.
  2.- Ponte en contacto con **CENTRO DE SERVICIOS (200 100 – 911910000)** en caso de duda o creas que está infectado.

11. SECUESTRO DIGITAL.

- **Definición** Secuestro Digital: *"Incapacitación por parte del propietario de una cuenta a su acceso y gestión. Esta práctica es llevada a cabo por los ciberdelincuentes con el objetivo de obtener un rescate a cambio de devolverle el control de la cuenta a su propietario"*.

- Ejemplo de Secuestro digital.

Medidas de protección frente al secuestro digital.

- ❖ No facilitar demasiada info. a través de Redes Sociales.
- ❖ Desconfiar de correos que solicitan:

  1.- Enlaces que solicitan introducir info. sensible (Credenciales y Datos personales).
  2.- Descargar algún archivo sospechoso.

- ❖ **Doble Factor Autentificación.** No facilitar códigos que recibas de nadie.
- ❖ **Contraseñas Robustas** y diferentes para cada servicio.
- ❖ **Actualiza tus dispositivos y aplicaciones. Instala un buen Antivirus.**

12. DESINFORMACIÓN EN EL CIBERESPACIO.

- **Definición de Ataques de desinformación en el ciberespacio:** *"Ataques utilizando el ciberespacio contra los intereses de un país que no consisten en alterar los sistemas informáticos de empresas e instituciones, sino que tienen como objetivo alterar el funcionamiento de la opinión pública"*.

- **Principal objetivo de una campaña de desinformación:** *"Suministrar en el proceso de formación de la opinión pública de un país noticias falsas, medias verdades, información altamente subjetiva presentada como objetiva (confusión deliberada entre opinión e información) e información diseñada para producir un efecto emocional en el receptor".*

- ¿Cómo actuar frente a estos ataques?

13. RIESGO EN EL USO DE REDES WIFI PÚBLICAS.

- Riesgos de conectarse a una red wifi pública.
  1.- Man in the middle u hombre en el medio.
  2.- Redes trampa.

Medidas de protección y mejora de la seguridad en nuestras conexiones.

- ❖ No usar Red WIFI Pública para acceder a info. confidencial (bancaria, pagos, reservas, etc.).
- ❖ Para acceder a info. confidencial mejor usar: Datos móviles o dispositivos corporativos.
- ❖ Conexión cifrada y paginas https.
- ❖ Verifica siempre que el certificado de la página web a la que te estás conectando sea válido y no esté revocado, y sea emitido por una entidad de certificación válida.
- ❖ Usa antivirus en tus dispositivos personales.
- ❖ Borra las redes wifi a las que te hayas conectado previamente.

❖ Desactiva la conexión WIFI si no las estás usando.

14. MALWARE.

- **Definición Malware:** *"Software malicioso específicamente desarrollado por delincuentes para robar información (contraseñas, documentos, entre otras), controlar remotamente el equipo infectado o provocar daños a sistemas de información"*.

- **Riesgos por infección con Malware**.

- 2 ideas claves:

  1.- "En internet si no pagas por el producto, es que el producto eres tú".
  2.- "Tú tienes que estar permanentemente actualizado, los malos lo están".

- ¿Cómo si introduce la infección en el equipo?: A través de los fallos de los programas que tienes instalados.
- ¿Cómo se eliminan las vulnerabilidades?: A través de las actualizaciones de seguridad de los programas (Parches de seguridad).
- **Buenas prácticas** para luchar contra el Malware.

15. PHISHING.

- **Definición de Phishing:** *"Forma de ingeniería social (engaño) en la cual un atacante intenta de forma fraudulenta adquirir información confidencial de una víctima, haciéndose pasar, generalmente por una empresa, o por una persona, de confianza".*

- **Riesgos del Phishing**.

- Los riesgos de Phishing no solo están en el correo electrónico, sino también en el SMS (Smishing), llamadas telefónicas (Vishing) o RRSS, mensajería instantánea (Whats App etc.).

- Usa el correo electrónico corporativo.

- Identifica los correos electrónicos sospechosos de Phishing (suelen pedir – directamente o a través de un enlace web - contraseñas, datos bancarios, números de teléfono, etc.).

- Buenas prácticas para luchar contra el Phishing.

16. SMISHING.

- **Definición de Smishing:** *"Palabra que está compuesta por "SMS" (mensajes de texto) y "phishing" (pescar).*
  "Estafa que consiste en el envío de mensajes SMS al móvil con la finalidad de convencer al usuario para que introduzca su información personal o que instale una aplicación maliciosa (que les da acceso a sus datos personales, a sus claves y a sus SMS, etc.)".

- **Objetivo del Smishing:** *"Llegar a controlar todo lo que pasa en nuestra pantalla y acceder a todos los datos que se muestren en ella, como contraseñas, identificadores como DNI, etc. Todos ellos pueden ser utilizados para acceder a las cuentas bancarias y hacer transferencias sin que las víctimas tengan constancia".*

¿Cómo evitar picar en Smishing?:

- Desconfía de SMS (de trabajos "que no existen", de premios "sin haber jugado" o paquetes recibidos "sin haberlos pedido".
- Desconfía SMS con enlace (aunque provenga de un contacto que tienes identificado).
- No acceder a ninguna web que te llegue a través de SMS.
- No des datos bancarios a través de SMS o LLAMADA TELEFÓNICA.

Medidas de protección de Renfe frente al Smishing.

- **Control de las aplicaciones** instaladas en los dispositivos corporativos (a través de **GESTIÓN DE DISPOSITIVOS "MDM"**).
- **Control de la navegación del usuario** (a través del **PROXY**).
- **Antimalware** instalados en dispositivos móviles.
- Con todo lo anterior, tener en cuenta que "La seguridad 100% no existe".

¿Cómo saber si estamos infectados?

- Consulta al DEPARTAMENTEO DE CIBERSEGURIDAD DE RENFE.
- Verificar si nuestra aplicación de SMS (la de Google o del fabricante) ha cambiado a una que desconocemos.
- Ante cualquier sospecha, contactar con: CENTRO DE SERVICIO (200 100) o ÁREA DE CIBERSEGURIDAD DE RENFE (ciberseguridad@renfe.es).

17. CLASIFICACIÓN DE LA INFORMACIÓN (ETIQUETAS).

- Niveles de clasificación de la info.
  1.- RESERVADA (RSV): TLP RED (Etiqueta Roja).
  2.- RESTRINGIDA (RST): TLP AMBER (Etiqueta Ámbar).
  3.- USO INTERNO (UIN): TLP GREEN (Etiqueta Verde).

4.- INFORMACIÓN PÚBLICA (IPU): TLP WHITE (Etiqueta Blanca).

- Normas que establecen los pasos a seguir para clasificar la info. según el nivel adecuado:
  1.- NS-04 Norma de Clasificación de la Información.
  2.- IT. 10 Clasificación de la Información por el Responsable.
- ¿Dónde reflejar la clasificación de un documento mediante etiquetas?: **Margen superior derecho**.
- **ETIQUETAS:**
  1.- TLP RED: "Confidencialidad de la info." ALTA.
  2.- TLP AMBER: "Confidencialidad de la info." MEDIA.
  3.- TLP GREEN: "Confidencialidad de la info." BAJA.
  4.- TLP WHITE: "Confidencialidad de la info." NO VALORABLE.
- Herramienta de clasificación.

18. DISPOSITIVOS MÓVILES.

- ¿Cómo te roban los datos?
- ¿Qué riesgos implica?
- ¿Qué puedo hacer?

19. CONFIGURACIÓN SEGURA DE DISPOSITIVOS MÓVILES.

- **Pautas y recomendaciones** de ciberseguridad para el uso de dispositivos móviles.

20. PROTECCIÓN DE LA INFORMACIÓN EN DISPOSITIVOS MÓVILES PERSONALES.

- **Consejos** para proteger la info. en nuestros dispositivos móviles.
  1.- Protección física del dispositivo.
  2.- Gestión de cuentas del usuario.
  3.- Cifrado de la info.
  4.- Creación de copias de seguridad.

No olvidar:

- ❖ Protege tu dispositivo de manera física (no permitas que otros accedan a él).
- ❖ Crea cuentas de usuario en tu dispositivo.
- ❖ Crea copias de seguridad y almacénala de forma cifrada.

21. VACACIONES CIBERSEGURAS.

- Ojo con los fraudes en alquileres vacacionales.
- **Pistas** para detectar estos fraudes.

22. USO DE DISPOSITIVOS DURANTE LAS VACACIONES.

- Cuando salgas fuera cuidado con: Redes WIFI a la que te conectas y con el uso de tus dispositivos electrónicos.
- **Buenas prácticas** ante desplazamientos vacacionales.
  1.- Antes del desplazamiento.
  2.- Durante el desplazamiento.
  3.- Después del desplazamiento.

23. USO RESPONSABLE DE REDES SOCIALES.

- Caso Facebook (ataque sufrido por la compañía).

¿Cómo proteger adecuadamente nuestro perfil?

- Todos tenemos una Huella Digital.
- **OSINT (Búsqueda de info. en fuentes públicas)**. Es aquello que ponemos nosotros mismos en Redes Sociales. El Responsable de la info. somos nosotros mismos.
- **OSINT** puede ser empleado por ciberdelincuentes para:
  - Recopilar info. por medio de ingeniería social para obtener nuestras credenciales.
  - Suplantar nuestra identidad.
  - Saber dónde estamos, rutinas, hábitos y aspectos de personalidad.

Piensa dos veces antes de publicar la siguiente info. en RRSS:

- Datos personales.
- Planes y vacaciones.
- Comportamientos inapropiados.
- Info. bancaria.
- Info. sobre menores.

Niveles de privacidad:

- Alto: Controlaremos, en todo momento, quién puede ver nuestra info. y publicaciones.

- Medio: Solo las personas que tengamos agregadas podrán visualizar nuestra info. y publicaciones.
- Bajo: Cualquier persona fuera de nuestro "círculo de contactos" puede tener acceso a toda nuestra info. y publicaciones.

"Todo lo que publicamos en internet permanecerá publicado, y aunque tengamos derecho a eliminarlo, puede haber sido recopilado, almacenado y compartido por terceros".

24. SEGURIDAD EN COMPRAS ONLINE.

- Un estudio reciente revela:

  1.- 3/10 consumidores asegura comprar online al menos 1 vez/mes.
  2.- 2/10 consumidores adquiere productos o servicios en la red cada semana.

- Formas de pago más comunes en España*:* ***Pago con Tarjeta***, ***PayPal*** y ***Bizum***.
- Medidas de seguridad y recomendaciones para cada una de ellas.