La tecnología está cada vez más presente en nuestro día a día: smartphones, relojes inteligentes, altavoces inteligentes, coches autónomos, facilitando cualquier tipo de tarea y contribuyendo en el desarrollo económico, social y cultural actual.

Sin embargo, cada vez se dan más amenazas que ponen en riesgo la seguridad de los usuarios y de las empresas.

Características de una sana seguridad informática.:

Integridad: La información contenida sólo puede modificarse por personas autorizadas y mediante un protocolo acordado.

Confidencialidad: Los recursos informáticos o la información contenida en el sistema deben ser accesible sólo por personas autorizadas para ello.

Disponibilidad: Estos recursos e información deben ser accesibles en los momentos en que se requiera por personal autorizado.

Irrefutabilidad: Tanto el uso como la modificación de información o recursos informáticos deben ser irrefutables, es decir, que el responsable de dicha acción no pueda negarla.

Radiografía actual de ciberamenazas

La Concienciación en Ciberseguridad es básica para interiorizar la importancia de aplicar los consejos que explicaremos a continuación. Como sucede en cualquier Análisis de riesgos, es esencial conocer la frecuencia e impacto de las ciberamenazas:

Cada 39 segundos ocurre un ciberataque (Universidad de Maryland EEUU, 2018).

- El **100%** de las organizaciones con más de 500 teléfonos móviles sufrieron ciberataques en estos dispositivos (Mobile Cyberattacks Impact Every Business. Check Point Software).
- **3 de cada 5 empresas** que han instalado tecnologías IoT han sufrido ciberataques en estos dispositivos (Internet of Things Cybersecurity Readiness - Osterman research for Trustwave).
- **1 de cada 2 directivos** de IT de Agencias Federales consideran su mayor ciberamenaza la baja o nula formación en ciberseguridad en proveedores (Federal Cybersecurity Survey, SolarWinds).
- **1 de cada 2 víctimas de ciberataque** vuelve a ser atacada con éxito en menos de un año (FireEye, 2018).

- Las variantes de Malware en dispositivos móviles **aumentaron un 54%** en 2017 (Symantec, 2018).
- Las variantes de Ransomware **aumentaron un 45%** en 2017 (Symantec, 2018).
- **1 de cada 2 directivos de tecnología** identifican el Phishing como su principal ciberamenaza (Global Advanced Threat Landscape Report 2018 (Vanson Bourne for CyberArk).
- El coste del Ransomware para las organizaciones **aumentó un 400%**, llegando a $5.000 millones (Stroz Friedbere, 2018).

Vectores de ataque más habituales

En cuanto al modus operandi de los cibercriminales, éstos pueden utilizar diferentes rutas para conseguir acceso a una información, sistema o dispositivo. Las más habituales son:

1. Clic en un enlace: emails, archivos, webs o redes sociales.
2. Clic en una imagen: emails, pendrives, webs, etc.
3. Descarga/apertura de archivos: pop-ups, banners publicitarios, emails o archivos.
4. No tener actualizaciones al día o disponer de programas o sistemas operativos sin el debido mantenimiento y actualización.
5. Ausencia de controles: personas, programas, sistemas operativos, redes, dispositivos o infraestructura.

En los cinco vectores de ataque habituales es necesario que se dé un error por parte del usuario, la persona que utiliza los dispositivos o la que se encarga de su mantenimiento.

Consecuencias inmediatas de esos errores:

- Filtración de contraseñas (phishing)
- Secuestro de datos (ransomware)
- Secuestro de cuentas
- Robo de dinero
- Espionaje competitivo
- Denegación de servicio
- Instalación de programas no deseados (spyware, adware, bundleware, junkware.)
- Monitorización y control del dispositivo, etc.

Repercusiones habituales de un ciberataque:

- Impacto económico
- Pérdida de tiempo
- Reducción de la productividad
- Crisis reputacional personal o empresarial
- Disminución de la confianza de clientes y otros usuarios

- Posibles repercusiones legales

De ahí que sea tan importante que cualquier usuario, ya sea a nivel personal o profesional, por el mero hecho de tener contacto con la tecnología, disponga de conocimientos adecuados en Prevención de Ciberamenazas y en Cultura de Ciberseguridad.

Los usuarios: el eslabón más débil y la principal vulnerabilidad

A continuación, antes de pasar a explicar los 15 consejos de seguridad para tener una vida "cibersegura" exponemos datos e indicadores relacionados con el papel de los usuarios en lo que a la prevención de ciberataques se refiere:

- El **39%** de filtraciones de información es debida a la pérdida del dispositivo móvil en el área de trabajo y el **34%** en un vehículo (Verizon Data Breach Report 2016).
- Las empresas necesitan aproximadamente 191 días para detectar una filtración de datos y además necesitan 66 días para contenerla (Cost of Data Breach Study 2017 - Ponemon Institute for IBM Security).
- **1 de cada 3** personas abre emails de phishing, mientras que **1 de cada 5** abre archivos adjuntos maliciosos (Verizon Data Breach Report 2016).
- **4 de cada 5** ciberataques se produjeron por el uso de contraseñas débiles o robadas (Stroz Friedberg, 2018).
- Cada vez más, la ingeniería social se está sofisticando mediante la personalización avanzada, el uso de datos reales y la omnicanalidad (email, SMS, publicidad web, etc.).
- El **47%** de filtraciones son causadas por Malware, el **28%** por errores humanos y el **25%** por un fallo de procesos o configuración (Cost of Data Breach Study 2017 - Ponemon Institute for IBM Security).
- Las filtraciones de datos e información han aumentado un **45%** respecto al año anterior (Annual DataBreach Year-end Review 2017 - Identity Theft Resource Center).
- **4 de cada 5** empresas reconocen haber sufrido al menos, una filtración de datos (Global Threat Report 2018 - 451 Group for Thales).
- **1 de cada 5** filtraciones fue por error de un empleado interno (Data Breach Investigations Report 2017 - Verizon).
- El coste medio de una filtración de datos es de 3,6 millones de dólares (Cost of Data Breach Study 2017 - Ponemon Institute).
- **1 de cada 2 emails son SPAM** y 1 de cada 20 emails tiene contenido malicioso (Trustwave Global Security Report 2016).

Lista de 15 Consejos de Ciberseguridad para tener una vida cibersegura

CUENTA CON UN PROGRAMA ANTIVIRUS INSTALADO Y ACTUALIZADO SIEMPRE

- Ya sea el más potente del mercado o, como mínimo, uno gratuito.
- Siempre será mejor tener el plan más básico, barato o gratuito que no tener nada.
- Sí que es importante contar con la última versión del programa y, como no, descargarse e instalárselo de forma oficial para que haga su trabajo correctamente.

2. VIGILA LAS DESCARGAS Y ARCHIVOS ADJUNTOS FRAUDULENTOS

- Ten cuidado a la hora de descargarte archivos de Internet, en especial aquellos ejecutables tipo ".exe", ya que pueden contener código malicioso y dañar tu equipo.
- Recuerda que también puedes encontrarte con este tipo de amenazas en forma de archivo adjunto en un correo electrónico.
- El consejo básico es: Si te encuentras frente a un archivo que no esperas, de alguien que no corresponde o de procedencia desconocida, no lo abras y mándalo a la papelera de inmediato.

3. DUDA DE E-MAILS EXTRAÑOS, PHISHING Y SPAM

- Como decíamos, el correo electrónico es una de las principales vías de entrada de amenazas de seguridad. Nadie está exento de poder recibir un mensaje sospechoso.
- Por tanto, ante cualquier mail extraño elimínalo y no abras ni descargues el archivo adjunto. Si es verdaderamente importante, te volverán a contactar por otra vía.
- Sospecha especialmente de que estás ante algo anómalo si el e-mail está mal redactado, desconoces el remitente o la dirección es sospechosa o está incompleta, si está escrito en un idioma que no es con el que habitualmente te comunicas con ese interlocutor, si te piden dinero por correo (aunque el remitente asegure ser tu banco), etc.
- Si acabas aterrizando en una web en la que debes introducir tus datos, fíjate antes que es https (más info en el Consejo nº 9) y que el enlace es correcto. De lo contrario, podría tratarse de phishing. Siempre que puedas, intenta acceder directamente a esa web desde tu navegador y no después de haber hecho clic en un enlace de un email o de otra fuente sospechosa.

4. MANTÉN SIEMPRE TU SISTEMA OPERATIVO ACTUALIZADO

- Esto es muy importante a tener cuenta ya que, al igual que los malware evolucionan constantemente, tu SO también debería actualizarse al mismo ritmo.
- Las actualizaciones del sistema operativo de tus dispositivos suelen traer parches para solucionar problemas técnicos o brechas de seguridad.

5. HAZ UNA BUENA GESTIÓN DE TUS CONTRASEÑAS

- Suelen ser también otra de las grandes brechas de seguridad. Podemos cometer varios errores con las contraseñas: desde poner una fácil de descifrar (año de nacimiento, número de teléfono, matrícula del coche,123456...), a poner la misma contraseña para todos los sitios.
- Es importante tener una contraseña única para cada sitio, que sea robusta con multitud de caracteres y cambiarla de forma periódica.
- También puedes crear contraseñas mediante generadores de claves de forma aleatoria (en los que se incluyen números, símbolos, letras en mayúscula y minúscula, etc).
- Por último, te recomendamos guardar tu contraseña en un gestor de contraseñas que te ayuda a tener contraseñas complejas sin tener que recordarlas.

6. RECUERDA, TU MÓVIL O TABLET TAMBIÉN DEBEN ESTAR PROTEGIDOS Y SON TAN VULNERABLES COMO UN ORDENADOR

- No pases por alto este aspecto. ¿A caso no utilizamos nuestros dispositivos móviles tanto o más que un ordenador de mesa o portátil?
- Debemos tener en cuenta que nuestro móvil o tablet pueden ser víctimas de un virus y por eso mismo, debemos extremar precauciones cuando los usemos para navegar por internet o realizar alguna compra online.
- Igualmente, también es recomendable la instalación de un sistema antivirus que garantice el pago seguro y el acceso seguro a tu banca online.

7. USA LA CREACIÓN DE USUARIOS PARA DIFERENTES PERSONAS

- Si compartes un equipo con varias personas (en tu hogar u oficina de trabajo) es importante que crees cuentas de diferentes usuarios y configures los permisos según el principio de necesidad de saber: que cada usuario acceda a donde realmente necesita y no a lo de todos.
- Con ello, tus datos personales, historial de navegación, archivos, etc., quedarán reservados solo para ti mismo. Si se vulnera la seguridad de otro usuario, tu información quedará mejor resguardada.

- Como es evidente, también se debe configurar una contraseña (con las indicaciones que te hemos dado anteriormente) distinta y segura para cada usuario.

8. ACTIVA EL FIREWALL O CORTAFUEGOS

Se trata de una de las herramientas a la hora de proteger nuestro dispositivo por defecto, está disponible en todos los sistemas operativos y es fácil de configurar, pudiendo escoger el nivel de protección que cada uno desea en cada momento.

9. REALIZA SIEMPRE COMPRAS EN SITIOS SEGUROS

- Las compras online pueden ser también otra vía de entrada a amenazas de seguridad, ya que pueden robarte datos y dinero.
- El consejo: no compres nada en una tienda online que no te parezca de confianza.
- Revisa que sea un lugar certificado y fiable.
- Presta atención al certificado SSL de una web (representado con un símbolo de un candado en la barra de navegación), y a que la web desde la que vas a hacer la compra tiene un dominio 'https' como es el caso de https://www.lisainstitute.com.

10. MIL OJOS CON LOS DISPOSITIVOS IOT (INTERNET OF THINGS = INTERNET DE LAS COSAS)

Altavoces, Smart TV, relojes y pulseras inteligentes... Estos dispositivos también conocidos como wearables (si se llevan puestos) o dispositivos IoT (en general) pueden ser susceptibles de ser hackeados, pues ya se han dado casos de hackeos, filtraciones y escuchas a través de los mismos.

- El consejo es que siempre sigas las instrucciones del fabricante y actualices el sistema cuando sea necesario para evitar que pasen "cosas raras".
- La innovación tiene cosas positivas, pero suele ir asociada a mayores riesgos ya que tienen menos medidas de seguridad por defecto. De ahí que en las empresas u organizaciones más innovadoras, necesiten de expertos en Ciberseguridad en IoT.

11. REVISA LAS APP Y EXTENSIONES AUTORIZADAS

- Mucho cuidado con extensiones del tipo "ver quién me ha dejado de seguir" o juegos de Facebook porque, de otorgarles permisos a dichas extensiones, podemos estar expuestos a un filtrado de nuestros datos.
- Registrarse en webs o App con nuestros perfiles de Facebook, Google+ o Twitter es más rápido, pero estamos facilitando información de dichas redes. Normalmente esta acción no implica que estemos dando nuestra contraseña a la página, pero

debemos estar atentos a quien le facilitamos información personal y qué medidas de ciberseguridad realmente tiene esa web o App para protegerla.

12. REALIZA COPIAS DE SEGURIDAD

- Ante cualquier riesgo o amenaza de ver comprometidos nuestros archivos (por robo o por daño), es interesante contar con una solución de backup.
- Realiza copias de seguridad de forma permanente, son la única medida eficaz (y gratis) en caso de que sufras un cibersecuestro de tu dispositivo (Ransomware).

13. CIERRA SESIÓN, SOBRE TODO EN SITIOS PÚBLICOS

- ¿Dejarías la puerta de tu casa abierta o las llaves de tu coche puestas? Bueno, depende del país en el que residas quizás no te ocurra nada, pero en lo que a Ciberseguridad se refiere, nunca dejes la sesión abierta en un ordenador público (de la oficina, de una biblioteca...). Recuerda cerrar todas las sesiones antes de desconectarte y apagar el ordenador.
- Asegúrate que no está seleccionada la opción de "Recordar contraseña", ya que, aunque salgas de la sesión, cualquier que utilice dicho dispositivo podrá acceder de nuevo a tu sesión sin necesidad de conocer la contraseña.

14. SOSPECHA SIEMPRE DEL WIFI DEL AEROPUERTO (O DE CUALQUIER SITIO PÚBLICO)

- El cartel del "WiFi gratis" puede ser un gran reclamo para ti, pero también para quien intente quedarse con tus datos.
- Intenta evitar conectarte a una red abierta. Si no te queda otra, evita por encima de todo acceder a datos sensibles (bancos, correos, insertar contraseñas de redes sociales, etc). Todos los datos que circulen por esa red son plenamente visibles.
- Valora utilizar una conexión VPN para que la información que transmitas vaya cifrada de punto a punto.

15. SI NO ESTÁS USANDO INTERNET, APÁGALO

- Si no estás usándolo, desconéctalo y reducirás posibilidades de sufrir un ataque informático. Tan sencillo como apagar el router o pulsar el botón de 'modo avión' y asegurarte una desconexión (casi) total de redes.