Píldora Informativa

GPIT

Consejos de Seguridad para evitar ciberataques

No. 009

Universidad Nacional Abierta y a Distancia

Gerencia de Plataformas e Infraestructura Tecnológica - GPIT

Grupo Funcional Seguridad Informática - GFSI

https://gpit.unad.edu.co/seguridad-de-la-informacion

seguridad.informacion@unad.edu.co

601-3443700 Ext 1687

Septiembre 15 de 2023

Alcance

Ilustración 1. https://www.shutterstock.com

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 ciudadanos, empresas e instituciones públicas, exponiendo su información privada, robando su dinero o afectando a su reputación.

La ciberseguridad está íntimamente ligada al cumplimiento normativo. Las empresas tienen que cumplir con la regulación en el ámbito de la seguridad, con especial atención a la protección de la privacidad de los usuarios. No solo es de obligado cumplimiento, sino que son medidas necesarias para la correcta gestión de la información de sus usuarios y clientes, seguridad con terceros (proveedores) e interna con sus empleados

Objetivo

Esta píldora contribuir a que se tenga una vida más cibersegura y ser capaz de evitar el 99% de ciberataques.

Capacitar a la **plataforma Humana** sobre cómo protegerse contra las amenazas cibernéticas y cómo cumplir con las regulaciones de ciberseguridad.

Radiografía actual de ciberamenazas

Ilustración 2. https://www.shutterstock.com

La Concienciación en Ciberseguridad es básica para interiorizar la importancia de aplicar los consejos que se explicaran adelante.
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).

Fig. 1: Ciberataques subieron 65% siendo los bancos e industriales sus blancos más comunes.
Fuente: https://www.larepublica.co/empresas/reporte-ciberseguridad-2023-a-empresas-y-sectores-3701737

Los 6 vectores de ataque o canales mas habituales de los cibercriminales

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:

Ilustración 3. https://www.shutterstock.com

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 formadas, programas robustos, sistemas operativos bien configurados, redes, dispositivos o infraestructura vulnerable, etc.
6. **Ingeniería social**: engañando o manipulando a las víctimas para que les faciliten información a través de una web, llamada, sms, etc.

En los seis 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 configuración y mantenimiento. El eslabón más débil somos nosotros: las personas.

Las 9 motivaciones principales de los cibercriminales

Dependiendo del objetivo del cibercriminal, de su modus operandi y de las herramientas que utilice, estas son las principales causas o motivos del ciberataque:

1. Filtración de contraseñas en la Dark Web (obtenidas mediante fuerza bruta o phishing)
2. Pérdida de información o secuestro de datos y dispositivos (ransomware)
3. Modificación de la información existente
4. Suplantación de identidad, secuestro de cuentas de usuario o cuentas bancarias
5. Robo de dinero, blanqueo de capitales o financiación del terrorismo
6. Espionaje industrial o inteligencia competitiva
7. Denegación de servicio
8. Instalación de programas no deseados (malware del tipo spyware, keyloggers, virus, adware, bundleware, junkware,..)
9. Monitorización de la conexión y control del dispositivo, obtención de nuestra huella digital, etc.

8 repercusiones de sufrir un ciberataque a nivel personal y profesional

En función del tipo de ciberataque y de la víctima, estas son las repercusiones más habituales:

Ilustración 4. https://www.shutterstock.com

1. Perjuicio económico
2. Pérdida de tiempo
3. Pérdida de información
4. Pérdida de confianza en la información
5. Reducción de la productividad
6. Crisis reputacional personal o empresarial
7. Disminución de la confianza de clientes y otros usuarios
8. Posibles repercusiones legales

Usuarios: eslabón más débil y principal vulnerabilidad

- 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).
- 4 de cada 5 ciberataques se produjeron por el uso de contraseñas débiles o robadas (Stroz Friedberg).

- Las empresas necesitan aproximadamente 191 días para detectar una filtración de datos y además necesitan 66 días para contenerla (Cost of Data Breach Study - 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).
- 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 - Ponemon Institute for IBM Security).
- Las filtraciones de datos e información han aumentado un 45% respecto al año anterior (Annual DataBreach Year-end Review - Identity Theft Resource Center).
- 4 de cada 5 empresas reconocen haber sufrido al menos, una filtración de datos (Global Threat Report - 451 Group for Thales).
- 1 de cada 5 filtraciones fue por error de un empleado interno (Data Breach Investigations Report - Verizon).
- El coste medio de una filtración de datos es de 3,6 millones de dólares (Cost of Data Breach Study - Ponemon Institute).
- 1 de cada 2 emails son SPAM y 1 de cada 20 emails tiene contenido malicioso (Trustwave Global Security Report).

Consejos de seguridad para evitar los ciberataques

1. CONTAR 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
   - Tener cuidado a la hora de descargar archivos de Internet, en especial aquellos ejecutables tipo "*.exe*", ya que pueden contener código malicioso y dañar su 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 EMAILS 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 elimínelo y no abrir ni descargar el archivo adjunto. Si es verdaderamente importante, lo volverán a contactar por otra vía.
   - Sospechar especialmente que se está ante algo anómalo si el e-mail está mal redactado, se desconoce el remitente o la dirección es sospechosa o está incompleta, si está escrito en un idioma que no es con el que habitualmente se comunica con ese interlocutor, si le piden dinero por correo (aunque el remitente asegure ser su banco), etc.
   - Si acaba aterrizando en una web en la que debe introducir sus datos, fijarse 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 se pueda, intentar acceder directamente a esa web desde un navegador y no después de haber hecho clic en un enlace de un email o de otra fuente sospechosa.
4. MANTENER SIEMPRE EL SISTEMA OPERATIVO ACTUALIZADO
   - Esto es muy importante a tener cuenta ya que, al igual que los malware evolucionan constantemente, el 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. HACER UNA BUENA GESTION DE LAS CONTRASEÑAS
   - Suelen ser también otra de las grandes brechas de seguridad.
   - Se pueden 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 se pueden crear contraseñas mediante generadores de claves de forma aleatoria (en los que se incluyen números, símbolos, letras en mayúscula y minúscula, etc.)
- Por último, se recomienda guardar su contraseña en un gestor de contraseñas que le ayuda a tener contraseñas complejas sin tener que recordarlas.

6. EL MOVIL O TABLET TAMBIEN DEBEN ESTAR PROTEGIDOS Y SON TAN VULNERABLES COMO UN COMPUTADOR.
   - No se debe pasar por alto este aspecto ya que utilizamos nuestros dispositivos móviles tanto o más que un computador de mesa o portátil.
   - Se debe tener en cuenta que nuestro móvil o Tablet pueden ser víctimas de un virus y por eso mismo, se deben extremar precauciones cuando se usen para navegar por internet o realizar alguna compra online.
   - Igualmente, también es recomendable la instalación de un sistema antivirus que garantice el pago y el acceso seguros a la banca online.
7. USAR LA CREACION DE USUARIOS PARA DIFERENTES PERSONAS.
   - Si se comparte un equipo con varias personas (en el hogar u oficina de trabajo) es importante crear cuentas de diferentes usuarios y configurar 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, los datos personales, historial de navegación, archivos, etc., quedarán reservados solo para ti mismo. Si se vulnera la seguridad de otro usuario, la información propia quedará mejor resguardada.
   - Como es evidente, también se debe configurar una contraseña (con las indicaciones que se han dado anteriormente) distinta y segura para cada usuario.
8. ACTIVAR EL FIREWALL
   - 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. REALIZAR SIEMPRE COMPRAS EN SITIOS SEGUROS
   - Las compras online pueden ser también otra vía de entrada a amenazas de seguridad, ya que alguien puede robar datos y dinero.
   - El consejo: no compre nada en una tienda online que no parezca de confianza. Revise que sea un lugar certificado y fiable.
   - Prestar 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 se va 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 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 se sigan las instrucciones del fabricante y se actualice 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.
    - REVISAR LAS APPS 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, se puede 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 se está facilitando información de dichas redes. Normalmente esta acción no implica que se esté 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.
11. REALIZAR 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*.

- Realizar copias de seguridad de forma permanente, son la única medida eficaz (y gratis) en caso de sufrir un ciber secuestro de nuestro dispositivo (Ransomware).
    1. CERRAR SESION, SOBRE TODO EN SITIOS PUBLICOS
- ¿Dejaría la puerta de su casa abierta o las llaves de su automóvil puestas? Bueno, depende del país en el que resida, quizás no le ocurra nada, pero en lo que a Ciberseguridad se refiere, nunca deje la sesión abierta en un computador público (de la oficina, de una biblioteca...). Recuerde cerrar todas las sesiones antes de desconectarse y apagar el ordenador.
- Asegúrese que no está seleccionada la opción de "Recordar contraseña", ya que, aunque salga de la sesión, cualquiera que utilice dicho dispositivo podrá acceder de nuevo a su sesión sin necesidad de conocer la contraseña.

12. SOSPECHE SIEMPRE DEL WIFI DEL AEROPUERTO (O DE CUALQUIER SITIO PUBLICO)
    - El cartel del "WiFi gratis" puede ser un gran reclamo para usted, pero también para quien intente quedarse con sus datos.
    - Intente evitar conectarse a una red abierta. Si no le queda otra, evite 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.
    - Valore utilizar una conexión VPN para que la información que transmita vaya cifrada de punto a punto.
13. SI NO ESTA USANDO INTERNET, APÁGUELO
    - Si no está usándolo, desconéctelo y reducirá posibilidades de sufrir un ataque informático. Tan sencillo como apagar el router o pulsar el botón de 'modo avión' y asegurarse una desconexión (casi) total de redes.

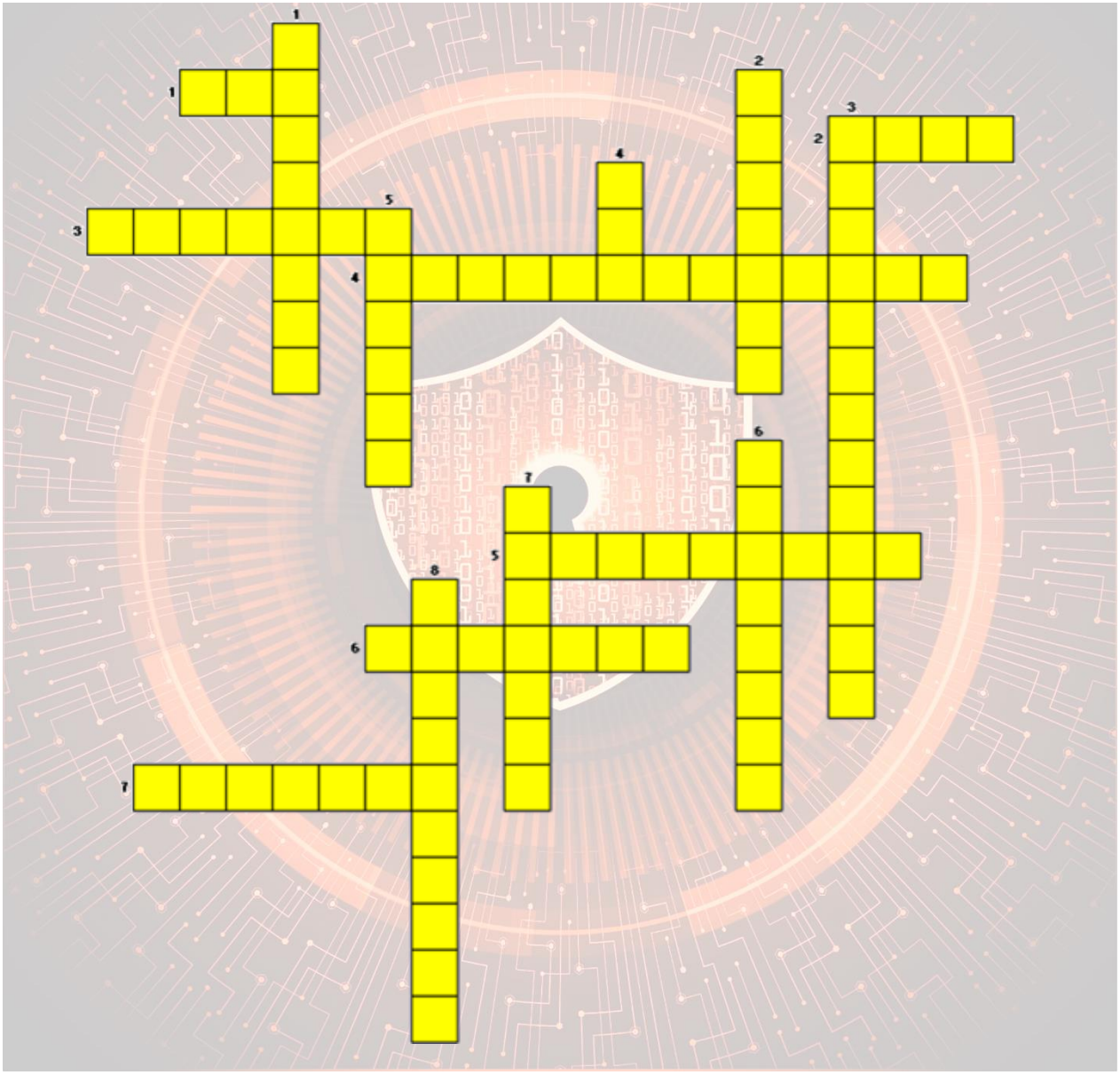
JUEGO

Horizontal

1. Técnica de seguridad que requiere más de una forma de autenticación para verificar la identidad del usuario.
2. Mensaje de correo electrónico no deseado, a menudo utilizado en ataques de phishing.
3. Parte de la web que no es indexada por motores de búsqueda y requiere acceso especial o autenticación para entrar.
4. Proceso que implica la instalación regular de parches y correcciones de seguridad para mantener un sistema protegido.
5. Software que se utiliza para buscar y eliminar malware.
6. Parte de Internet no indexada por los motores de búsqueda y a menudo asociada con actividades ilegales
7. Programa malicioso que se esconde en el código de otros programas.

Verticales

1. Secuencia de caracteres utilizada para autenticarse en sistemas y cuentas en línea.
2. Término genérico para software malicioso diseñado para dañar, robar o comprometer sistemas y datos.
3. Lugares en línea que utilizan protocolos de seguridad para proteger la información del usuario
4. Protocolo de seguridad utilizado para cifrar la comunicación entre el navegador web y el servidor.
5. Copia de seguridad de datos críticos que se crea para protegerlos contra pérdidas accidentales o ataques cibernéticos.
6. Método de ataque que involucra el envío masivo de correos electrónicos fraudulentos.
7. Práctica de obtener acceso no autorizado a un sistema informático.
8. Tipo de malware que cifra archivos y exige un rescate para su liberación.



Referencias

1. https://www.larepublica.co/empresas/los-ciberataques-suman-54-121-casos-en-lo-que-va-del-ano-y-han-crecido-mas-de-20-3509163
2. https://www.larepublica.co/empresas/reporte-ciberseguridad-2023-a-empresas-y-sectores-3701737
3. LISA Institute- Lista de 15 consejos de Ciberseguridad para evitar el 99% de ciberataques: https://www.lisainstitute.com/blogs/blog/lista-consejos-ciberseguridad-vida-cibersegura
4. INCIBE – Aprende Ciberseguridad - https://www.incibe.es/aprendeciberseguridad
5. Policía Nacional Colombiana, "Centro Cibernético Policial" [En línea]. Disponible en: https://caivirtual.policia.gov.co/categoriascibercrimen/smishing. [Accedido: 07-nov-2022]
6. "Vishing", MINTIC. [En línea]. Disponible en: https://www.mintic.gov.co/portal/inicio/5302:Vishing#:~:text= Consiste%20en%20hacer%20llamadas%20telef%C3%B3nica s,datos%20personales%20e%20informaci%C3%B3n%20banc aria. [Accedido: 12-nov-2022]