San Marcos

SEGURIDAD INFORMÁTICA

AUTOR: WALTER MADRIGAL CHAVES

DICIEMBRE: 2019

CONTENIDO

INTRODUCCIÓN

El acelerado crecimiento tecnológico de los últimos tiempos, nos genera una dependencia de sus servicios que crece día con día, es casi una utopía imaginarnos un mundo sin tecnología. Este crecimiento y dependencia crea nuevos problemas a la sociedad, algunos de ellos son la i***nseguridad digital, el robo de datos y la suplantación de identidad.***

A la tecnología le confiamos información valiosa como datos personales y cuentas bancarias, si hablamos a nivel de empresas el caso es más preocupante, ya que en todos los procesos hay ambientes tecnológicos que los controlan, de aquí surge la necesidad de establecer mecanismos que nos protejan y con ello la ***ciberseguridad.***

La seguridad informática es la disciplina que se encarga de proteger los sistemas informáticos tales como las redes, los computadores y los datos que ellos contienen, de agentes externos o internos que pudieran robarlos o dañarlos.

PREGUNTA DISPARADORA

¿Qué es la seguridad informática?

ABSTRACT O RESUMEN

La Seguridad Informática es la disciplina que se encarga de proteger los sistemas informáticos tales como las redes, los computadores y los datos que ellos contienen, de agentes externos o internos que pudieran robarlos o dañarlos.

Los ***datos*** son el principal ***activo*** de las organizaciones la seguridad informática busca que esos datos sean: íntegros, confiables, disponibles y confidenciales.

Existen una gran variedad de virus, estos se clasifican según su forma de actuar, algunos ejemplos son: ***Gusano, troyanos, Adware, etc.***

No hay una técnica específica para no infectarse de un virus, lo que si hay son recomendaciones que puede ayudar a evitar una infección. esas sugerencias se analizarán en el cuerpo de la lectura.

PALABRAS CLAVE

Datos

Virus

Antivirus

Seguridad informática

Integridad de los datos

SEGURIDAD INFORMÁTICA

Baca (2016), define la seguridad informática como: La disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físico-cosmológicos, a los que están expuesta. Pág. 12

Como bien lo indica Baca, la seguridad informática busca proteger la información contra ataques de terceros, no solo a nivel personal sino de las empresas. Recordemos que los datos son el principal activo de las organizaciones.

Para dimensionar la importancia de los datos a nivel empresarial vamos a exponer un par de ejemplos.

Ejemplo 1: imaginen el lanzamiento al mercado de un producto nuevo e innovador, ¿qué pasaría si la competencia logra identificar con anticipación los detalles de este producto?

- La competencia puede copiar la idea.
- Una divulgación anticipada, restaría en el impacto sorpresa de los clientes.
- La posibilidad de realizar sabotaje al producto.
- Pérdida de credibilidad de la empresa

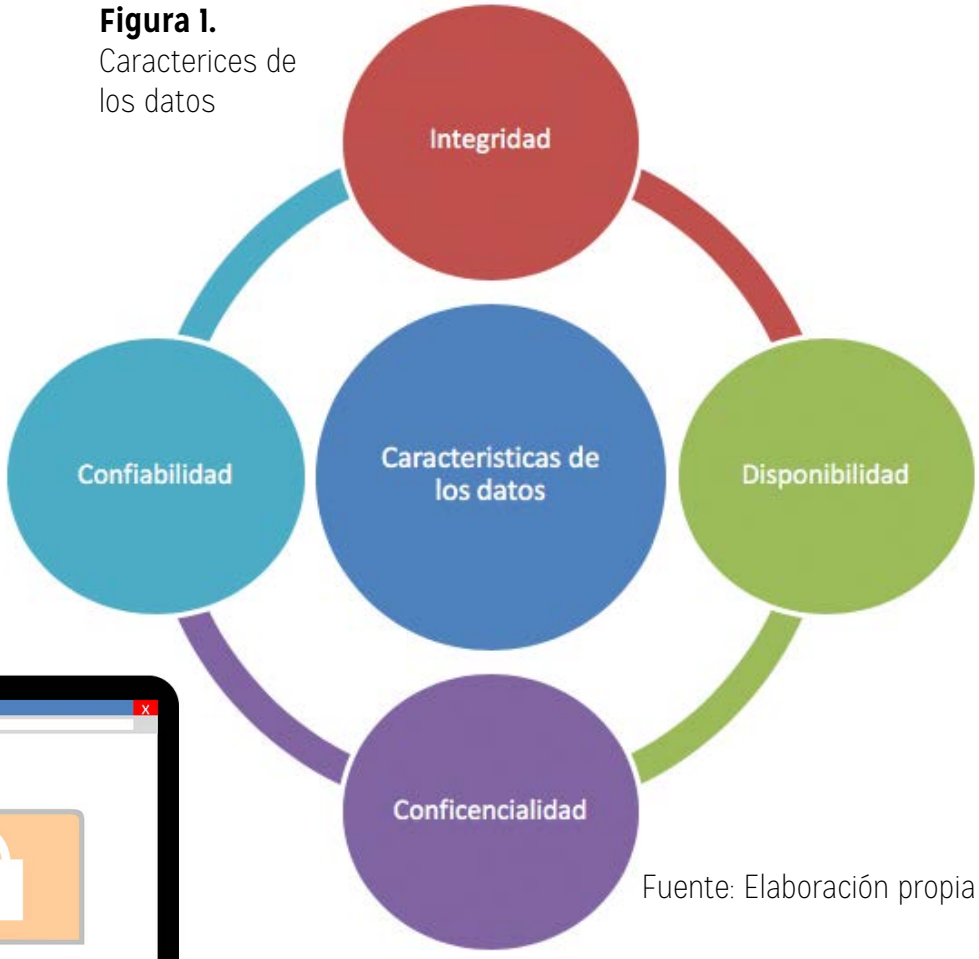
Ejemplo 2: si pensamos en un panorama más complicado en donde se roben la información de las cuentas bancarias de los clientes de un banco, las consecuencias serían catastróficas tanto para el banco, como para las personas que tienen comprometido su dinero.

- Robo de dinero de los usuarios.
- Desprestigio del banco.
- Las personas y empresas saldrían corriendo a retirar su dinero.
- Quiebra del banco.

CARACTERÍSTICAS DE LOS DATOS

La seguridad informática vela por el cumplimiento de ciertas características que los datos deben de cumplir. En la siguiente imagen se muestras estas características:

Figura 1.
Caracterices de los datos



Fuente: Elaboración propia

INTEGRIDAD

Significa que la información debe permanecer íntegra o sea debe estar completa.

DISPONIBILIDAD

La Información y servicios deben estar al alcance de los usuarios cada vez que se necesite.

CONFIDENCIALIDAD

El acceso a la información debe estar permitido sólo a entidades o personas autorizadas.

CONFIABILIDAD

Asegurar que la información no haya sido alterada inapropiadamente.

CIBERATAQUE

Desde el nacimiento de las computadoras y su posterior conexión mediante internet, los ataques informáticos han sido el dolor de cabeza de la mayoría de los usuarios, actualmente existen varias herramientas en la web que personas con poco conocimiento pueden provocar un ataque informático, esto provoca una gran proliferación de ellos.

Según la página Web www.auditool.org (2018) Los ciberataques son actos en los cuales se cometen agravios, daños o perjuicios en contra de las personas o grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio de computadoras y a través de la Internet.

En la siguiente imagen muestra los diferentes focos de infección según la empresa Panda Security en el 2018, de aquí podemos concluir que de los tres el más peligro son las Webs poco seguras.

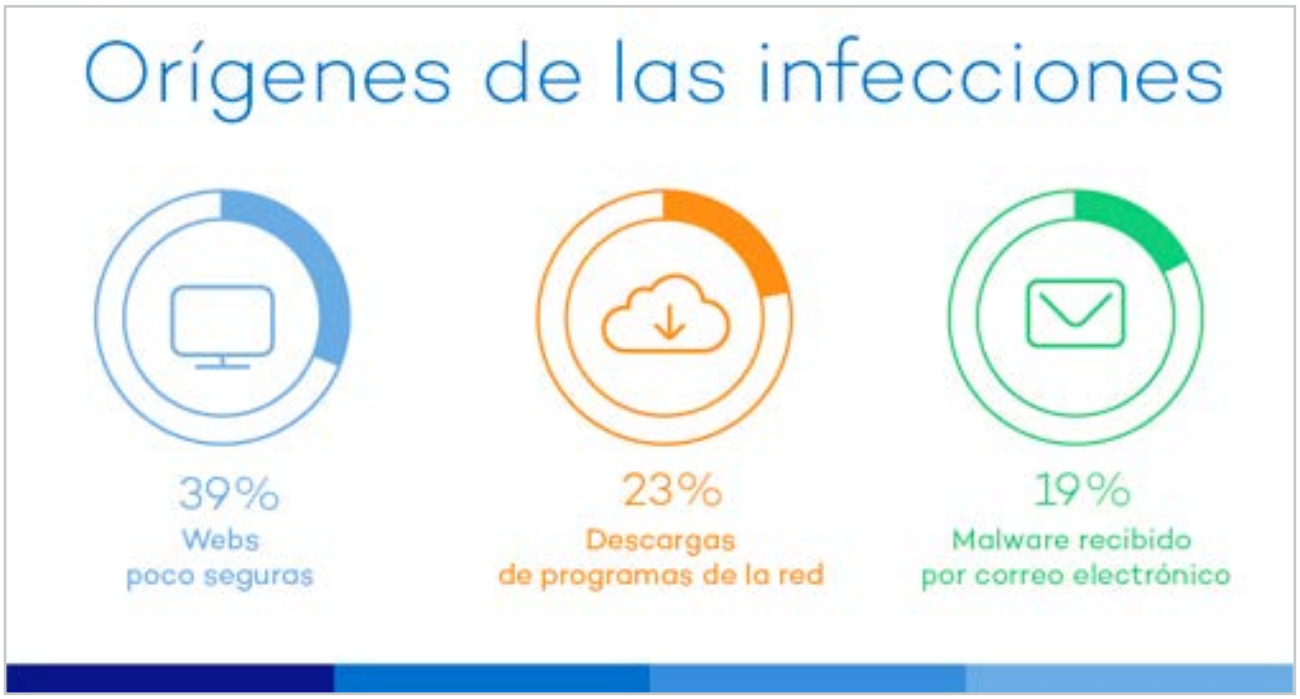


Figura 2. Origen de infecciones de virus

Fuente: PandaSecurity.com

VIRUS

Los virus son programas maliciosos creados para manipular el normal funcionamiento de los sistemas, sin el conocimiento ni consentimiento de los usuarios. Actualmente, por sencillez, el término "virus" es ampliamente utilizado para referirse, genéricamente, a todos los programas que infectan una computadora, aunque en realidad, los virus son solo un tipo específico de este tipo de programas.

Para referirse a todos ellos también se suelen emplear las palabras: código malicioso, software malicioso, software malintencionado, programas maliciosos, o la más usual: "malware", que procede de las siglas en inglés "malicious software".

A continuación, se analizan brevemente algunos tipos de malware que están en la web:

Worms: gusanos informáticos, tienen la capacidad de reproducirse por sí solos, debido a que estos programas realizan copias de sí mismos, ejemplo: si tenemos un equipo infectado y le insertamos un USB este también se infecta. El objetivo principal, por lo general, es saturar la computadora y ponerla lenta, con esto impedir el buen funcionamiento.

Troyanos: este tipo de malware instala aplicaciones en el equipo infectado para permitir el control remoto desde otros equipos, su modo de operar es engañar al usuario haciéndose pasar por un archivo inofensivo.

Adware: es un software que despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen un código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla, simulando ofrecer distintos servicios útiles para el usuario.

Keylogger: son aplicaciones o dispositivos de hardware, encargadas de almacenar en un archivo todo lo que el usuario escriba en el teclado. Se utiliza en gran manera para robar contraseñas y datos personales.

Spyware: es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas. La información que recolectan es utilizada para propósitos de mercadotecnia y representan, en muchas ocasiones, el origen de otra plaga como el SPAM, ya que pueden encarar publicidad personalizada hacia el usuario afectado.

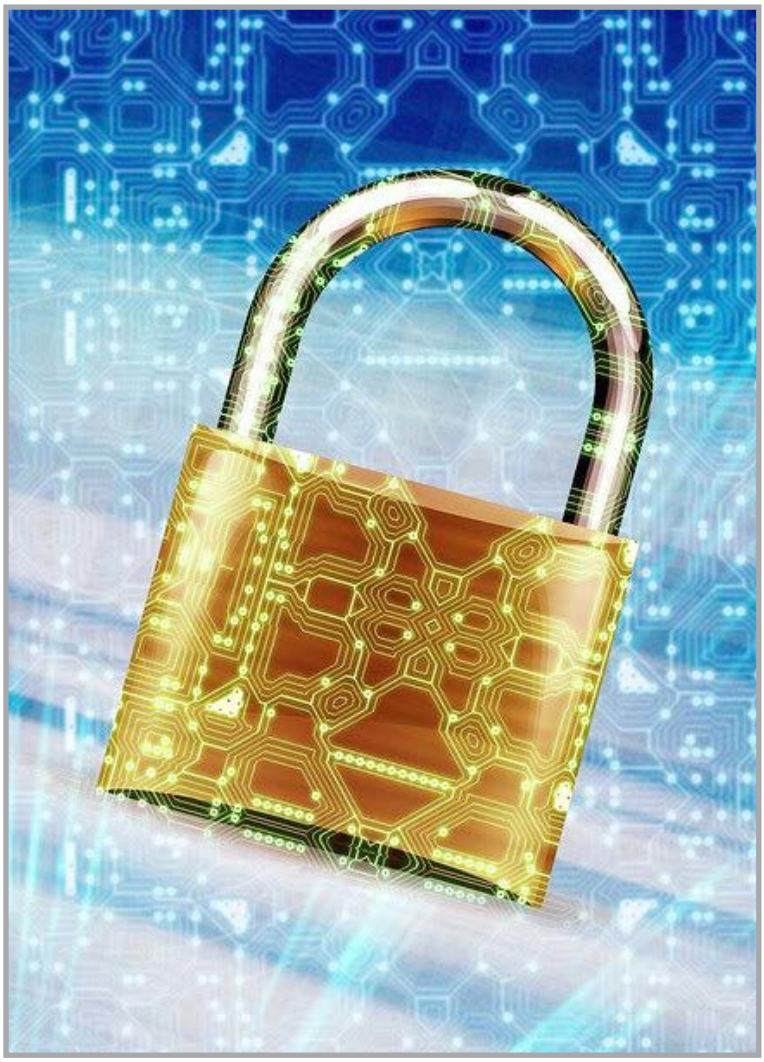
Spam: conocido como correo basura, son mensajes que en forma masiva distribuyen personas o empresas, la idea es dar a conocer algún producto, servicio o simplemente distribuir algún malware.

Ramsonware: un método muy de moda consiste en un código malicioso que cifra la información de la computadora e ingresa en él, una serie de instrucciones para que el usuario no pueda recuperar sus archivos. Para obtener la contraseña que libera la información, la víctima debe pagar al atacante una determinada suma de dinero, según las instrucciones que este disponga.

SEGURIDAD

Posiblemente después de conocer los malware más importantes que encontramos en la web, se encuentre un poco asustado de lo expuestos que estamos, afortunadamente hay medidas de prevención que podemos tomar y con esto reducir el riesgo de una infección. A continuación, se enlistan algunas recomendaciones a seguir:

- La más importante de todas es desconfiar de programas, información y personas que no estemos 100% seguras de su procedencia.
- Contar con un buen antivirus y más importante aún que esté actualizado, dentro del mercado encontramos versiones gratuitas que no son muy recomendadas como Avast free y AVG free, esto porque sus funciones son reducidas, por otro lado, encontramos los antivirus de pago, se pueden mencionar algunos muy buenos como: Panda Security, Kaspersky, Windows Defender, McAfee, entre otros.
- No instalar en su computadora software pirata, esto incluye sistema operativo y software de aplicación con Office, estos pueden estar infectados.
- Estar en constante actualización de los parches del sistema operativo mediante el Windows Update.
- Al navegar por la red, evitar ingresar a páginas de dudosa procedencia.
- No utilizar redes públicas para realizar transacciones bancarias u otras de importancia.
- No dejar expuestas claves de accesos.



Inversión en seguridad

A nivel empresarial la inversión en seguridad informática, debe ser un punto importante en el presupuesto establecido como cargo fijo. El constante crecimiento de malware y los novedosos métodos de hackeo utilizados, obligan a las empresas a una constante inversión en este campo, lo anterior con hardware especializado como Firewall, software moderno y actualizado como antivirus, contratación de personal calificado en área y la más importante en capacitación a su población laboral en temas de prevención.

La inversión necesaria para combatir la inseguridad en la web, depende de que tan importante o critica es la información para resguardar. Por ejemplo, las medidas de seguridad que se implemente en una empresa pequeña, en donde se maneja un sistema de facturación y que no hay involucrados datos importantes de clientes, no van a ser las mismas que utilizan entidades financieras como bancos.

CONCLUSIONES

Sin lugar a duda la protección de la información debe estar en las tareas prioritarias, tanto para las personas como para las empresas.

El crecimiento desmedido de los delitos informáticos y la importancia que han tomado los datos provoca que la inversión en este tema deba ser mayor y constante.

Las buenas prácticas de los usuarios ayudan en mucho, a repeler ataques informáticos.

Contar con un antivirus actualizado, software original, sistema operativo actualizado, no visitar páginas web de dudosa procedencia, son otras técnicas que ayudan para la protección de datos.

REFERENCIAS BIBLIOGRÁFICAS

Urbina, G. B. (2016). Introducción a la seguridad informática. México: Grupo Editorial Patria.

www.pandasecurity.com. (14 de 09 de 2019). Recuperado de https://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/others/

www.pandasecurity.com. (14 de 09 de 2019). Recuperado de https://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/worm/

www.Auditool.com. (14 de 09 de 2019). Recuperado de https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque