# La seguridad informática, una disciplina que no debemos desconocer

S. E. Vergara

***Abstract*—Desde que existe la información digital, se ha tenido la necesidad de proteger los datos, es por esto que existe la seguridad informática, el cual consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. Dicho esto, existirá siempre el riesgo de pérdida o robo y una de las técnicas que utilizan los atacantes es por medio del ransomware.***

*Palabras Claves*— **Información, Ransomware, Riesgo, Seguridad Informática, Vulnerabilidad**

## I. INTRODUCCIÓN

Con el avance de la tecnología, la protección de los datos ha sido parte fundamental de las empresas, encontramos temas como: el firewall, los dispositivos de almacenamiento de USB, organizaciones criminales en internet, antivirus entre otras.

Si bien es cierto que todos los componentes informáticos están expuestos a un ataque, son los datos y la información los que se deben proteger para que esto no suceda, por esto existen tres fundamentos básicos de la seguridad informática que se deben considerar no solo en las organizaciones sino también en los hogares

- Confidencialidad: se trata de la cualidad que debe poseer un archivo para que este solo sea leído por la persona o sistema que esté autorizado

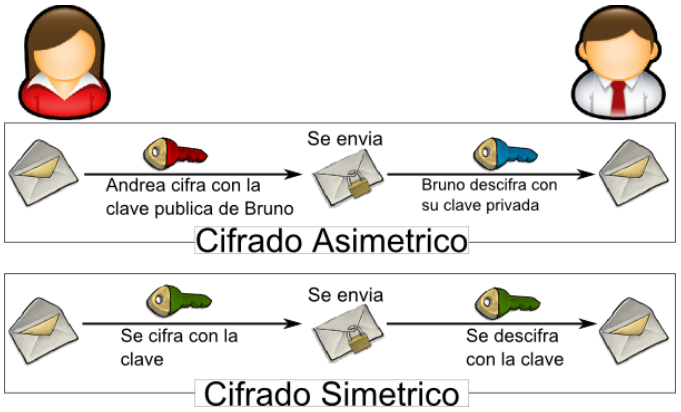


Fig. 1. Envío de un dato confidencial

- Integridad: Es la cualidad que posee un archivo que no ha sido alterado y que además permite comprobar que no se ha manipulado. Esta comprobación se puede realizar por medio de una función criptográfica usualmente conocida como "hash", el cual es una función matemática y/o lógica que nos permite transformar un conjunto de datos (texto, imágenes, archivos) en un único valor numérico, si se cambia algún dato del archivo, así sea el más mínimo el hash que se genera cambia lo que supone que se ha violado la integridad.

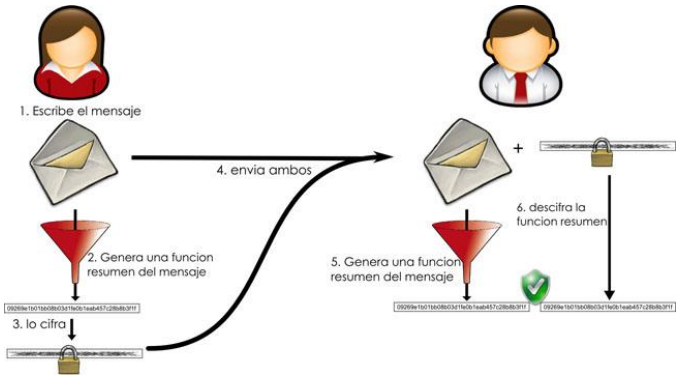


Fig. 2. Comprobación de integridad de los datos

- Disponibilidad: Se trata de la capacidad de un servicio, de unos datos o de un sistema, estar accesibles para los usuarios o procesos cuando estén los requiera.

Por lo general, deben existir los 3 aspectos para que haya seguridad de la información.

S. E. Vergara. Universidad Cooperativa De Colombia, Bogotá – Colombia. sergio.vergarar@campusucc.edu.co
Corresponding author: S. E Vergara

 ISSN 2590-8758

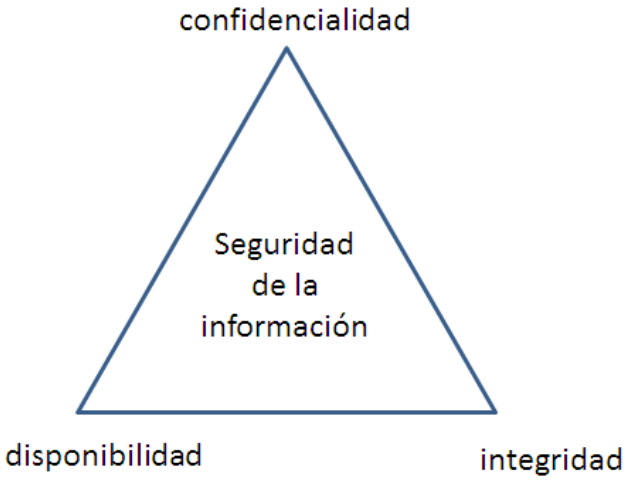

Fig. 3. Fundamentos de la seguridad de la información

## II. EL VALOR DE LOS DATOS

Establecer el valor real de la información digital es relativo, los datos representan un recurso que para muchas empresas no se presta la importancia adecuada debido a que es intangible, y al momento de realizar la inversión económica en esta área no es la suficiente, lo que implica que el riesgo de afectación de los datos, ya sea por un ataque cibernético o manipulación indebida de la información sea mayor.

## 3. AMENAZAS

Las amenazas a un sistema informático pueden provenir de un virus que ingresa a nuestro sistema, pasando por un programa que se ha descargado en páginas web no oficiales, descarga de datos adjuntos de correos sospechosos entre otros. Se pueden clasificar por tanto en amenazas provocadas por:

Amenazas lógicas: Dentro de esta categoría encontramos una innumerable cantidad de software maliciosos que pueden dañar los sistemas, ya sean generando bloqueos en los sistemas operativos o también aprovechando las vulnerabilidades existentes en los sistemas operativos y/o programas, dentro de los cuales se destacan virus, gusanos, troyanos keyloggers.

Amenazas físicas: Algunas de las amenazas físicas que pueden afectar los sistemas de información son los cortes de energía inesperados, catástrofes naturales, humedad, entre otras.

Personas: Las personas representan el mayor riesgo de daño y son estas las que ocasionan la mayor cantidad de ataques a un sistema de información, ya sea directa o indirectamente, dentro de las que pueden ocasionar daño de forma directa son parte los exempleados, hackers, intrusos remunerados, cualquier persona que haga parte de la organización. Los que realizan ataques indirectos representan un riesgo muy alto para la seguridad de la información, debido a que los atacantes aprovechan la ignorancia de algunos usuarios para acceder a los sistemas por medio de correos con software malicioso, una de las técnicas que se usan para este método es el ransomware.

## 4. RANSOMWARE

El ransomware, es el término genérico para referirse a todo tipo de software malicioso que le exige al usuario del equipo el pago de un rescate a cambio de la devolución de su información, para que el computador sea infectado en la mayoría de los casos debe tener la intervención de los usuarios y es donde se autoriza sin que lo sepa la infección del equipo.

A pesar de los diferentes mecanismos que las empresas invierten en la protección de los datos, el ransonware usa técnicas que permiten infiltrarse usando al hombre como instrumento para lograr su objetivo. Esta amenaza que ha crecido de forma exponencial en los últimos años, lo que hace es cifrar ciertos archivos con una determinada clave, que sólo el creador del ransomware conoce y proveerá al usuario que la reclame a cambio del pago de una recompensa.

¿Cómo afecta a las empresas de Latinoamérica?

Fig. 4. Usuarios afectados por ransomware

Fig. 5. Problemas con ransomware

Muchas empresas de antivirus generan diversas recomendaciones para no ser blanco de este tipo de ataques uno de ellos es educar a los usuarios de la organización, dado que en la mayoría de los casos la infección comienza a causa de un error humano que se da por la ignorancia acerca de esta amenaza, la educación y capacitación a todos los usuarios de la organización se vuelve fundamental para prevenirla y evitarla.

## 5. MÉTODOS DE INFECCIÓN DEL RANSOMWARE

El principal método de propagación es a través de troyanos en sitios web malintencionados o legítimos que han sido comprometidos por los cibercriminales. Las vías de infección más habituales son las páginas web con contenido pornográfico o de juegos, de modo que, cuando los usuarios seleccionan alguno de los anuncios, se le redirige a otra página comprometida que les infecta con ransomware u otro malware.

Un segundo método de contagio se realiza mediante enlaces a sitios comprometidos en correos masivos, mensajería instantánea, redes sociales, o bien descargándolo con algún programa de compartición de archivos (P2P).

Otra técnica a destacar se lleva a cabo a través de ataques usando el Protocolo de Escritorio Remoto (RDP), ya sea aprovechando alguna vulnerabilidad en el sistema o con ataques de fuerza bruta. Si el ataque tiene éxito, los criminales pueden cifrar los datos del servidor y después pedir un rescate por la contraseña.

Como último caso a destacar, comentar que este tipo de ataque también está afectando a dispositivos móviles, sobre todo dispositivos basados en el sistema operativo Android. Estos dispositivos son infectados cuando los usuarios instalan una aplicación que resulta no ser lo que anunciaba ser. Un ejemplo de este tipo de ransomware es el Android.Fakedefender, un troyano que muestra falsas alertas de seguridad en un intento de convencer al usuario de pagar por la versión completa de la aplicación con el fin de eliminar el malware inexistente.

## 6. WANACRY

El ataque con ransomware, bautizado como wannacry, se aprovecha de una falla de seguridad en Windows, descubierta en primer lugar por la Agencia Nacional de Seguridad de Estados Unidos (NSA, por sus siglas en inglés). La herramienta para explotarla fue robada de este organismo de inteligencia para ser publicada luego en internet por un grupo llamado Shadow Brokers, del que no se tienen mayores pistas hasta ahora.

Microsoft hizo pública la vulnerabilidad entre marzo y abril del año 2017 y procedió a publicar actualizaciones para cubrirla. Los usuarios afectados no poseían la actualización.

## 7. RESPONSABILIDAD DIGITAL

Si bien el hecho de no tener las últimas actualizaciones en el sistema operativo representa un riesgo latente en los equipos de cómputo, es necesario crear una cultura informática donde deben intervenir todos los que actores en un sistema de información, La seguridad digital es un asunto que, por la forma como se han construido las redes, implica a todos los usuarios que interactúan en estas. No es un tema para delegarle solo a las autoridades, ni para dejar exclusivamente en manos de los ingenieros.

## 8. RESULTADOS SOBRE ATAQUES DE INFORMACIÓN

Con fines de analizar las personas que pueden caer en este tipo de trampas, se realizó un ejercicio con una técnica llamada pixel tracking o técnica del pixel, el cuál por medio de un correo electrónico se introduce una imagen de 1 pixel por 1 pixel, de manera que cuando la víctima abre el correo la cual es totalmente transparente, se carga la imagen, cuando el usuario abre este tipo de correos, automáticamente se obtiene información sobre los datos del equipo, dirección ip (IP), el país de origen, el sistema operativo, navegador, fecha y hora en la cual se abre el correo.

Para este caso se hicieron pruebas con 100 usuarios de los cuales se obtuvieron los siguientes datos:

TABLA I

ESTADÍSTICAS DE PERSONAS QUE SE ENVIÓ EL CORREO CON LA TÉCNICA DEL PIXEL

| | |
|---|---|
| Personas que abrieron el dato adjunto del correo | 26 |
| Personas que no abrieron el correo | 74 |
| Total | 100 |

Aunque este tipo de ataque en particular no genera un riesgo en los sistemas de información, podemos decir que el número de personas que abren datos adjuntos procedentes de correos desconocidos es alto, lo cual representa un riesgo alto para las organizaciones, ya que malware como ransomware utiliza esta clase de técnicas para acceder, robar, manipular los datos.

## Referencias


[1] Eset LA. (1992-2016). DIGALE NO AL RANSOMWARE. Disponible en http://www.eset-la.com/kit-antiransomware

[2] Amaro José Antonio (04/08/2016). Seguridad en internet. Guadalajara, México.: Universidad de Guadalajara Disponible en http://www.suv.udg.mx/paakat/index.php/paakat/article/view/280/pdf.

[3] Moure Mariano Hugo (05/12/2016). Secuestro de información por medio de Malware. Buenos aires, Argentina.: Universidad de Palermo Disponible en https://dspace.palermo.edu:8443/xmlui/bitstream/handle/10226/1510/Documento_Mariano_Hugo_Moure_51394.pdf?sequence=1

[4] J Zaharia Andra (28/02/2017) Security Alert: New TorrentLocker Variant Targets Denmark in Ransomware Attacks. Heimdal Security Disponible en https://heimdalsecurity.com/blog/security-alert-new-torrentlocker-targets-denmark-ransomware/

[5] Microsoft, Inc. Microsoft Security Intelegence Report, vol. 21 (2016). Disponible en http://www.microsoft.com/security/sir/default.aspxS.

[6] Prince, B.: CryptoLocker Could Herald Rise of More Sophisticated Ransomware (2013). Disponible en http://www.darkreading.com/attacks-breaches/cryptolocker-could-herald-rise-of-more-sophisticated-ransomware

[7] Symantec, Inc. Internet Security Threat Reporte (2014). Disponible en http://www.symantec.com/security_response/publications/threatreport.jsp

[8] Donohue, B.: Reveton Ransomware Adds Password Purloining Function (2013). Disponible en http://threatpost.com/reveton-ransomeware-adds-password-purloining-function/100712

[9] Krebs, B.: Inside a Reveton Ransomware Operation (2012). Disponible en http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

[10] Austin, R. D., & Darby, C. A. (2004). El mito de la seguridad informática. Madrid, ES: Ediciones Deusto - Planeta de Agostini Profesional y Formación S.L.. Disponible en http://www.ebrary.com

[11] Chicano, T. E. (2014). Auditoría de seguridad informática (MF0487_3). Madrid, ESPAÑA: IC Editorial. Disponible en http://www.ebrary.com

[12] Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. Madrid, ES: Macmillan Iberia, S.A.. Disponible en http://www.ebrary.com

[13] Costas, S. J. (2014). Seguridad informática. Madrid, ES: RA-MA Editorial. Disponible en http://www.ebrary.com

[14] Roa, B. J. F. (2013). Seguridad informática. Madrid, ES: McGraw-Hill España. Disponible en http://www.ebrary.com

[15] Giménez, A. J. F. (2014). Seguridad en equipos informáticos (MF0486_3). Madrid, ESPAÑA: IC Editorial. Disponible en http://www.ebrary.com

[16] Baca, U. G. (2016). Introducción a la seguridad informática. Distrito Federal, MÉXICO: Grupo Editorial Patria. Disponible en http://www.ebrary.com

[17] Costas, S. J. (2014). Seguridad informática. Madrid, ES: RA-MA Editorial. Disponible en http://www.ebrary.com

[18] Castro, E. P., Pavas, C. L. P., & García, C. O. Y. (2009). Activos intangibles. Córdoba, AR: El Cid Editor | apuntes. Disponible en http://www.ebrary.com