La Seguridad de la Información: Desde la Antigüedad hasta el Internet de las Cosas.

INFORMATION SECURITY: FROM ANCIENT AGE TO INTERNET OF THINGS.

Recibido: 06 / 11 / 2018 ***Aprobado: 26 / 11 / 2018***

Dr. Reyson Lizardo Galvá
República Dominicana

El autor actualmente es el Director de Apoyo a la Ejecución de Proyectos del Ministerio de la Presidencia y miembro de la Comisión Técnica del Programa República Digital, de la cual coordina el Eje de Gobierno Digital. Es Doctor en Gobierno y Administración Pública de la Universidad Complutense de Madrid (España), mención Cum Laude; Máster en Alta Dirección Pública del Instituto Universitario Ortega & Gasset (España); e Ingeniero en Sistemas de Computación de la Universidad APEC (Rep. Dominicana), mención Summa Cum Laude; con especialización en Gobierno Electrónico del Instituto de Monterrey (México) y del Instituto Nacional de Administración Pública (Argentina).Ha sido expositor en congresos celebrados en Estonia, Corea del Sur, Singapur, España y en diversos países de Latinoamérica. Además, ejerce como catedrático de Gobierno Electrónico a nivel de postgrado en la Pontificia Universidad Católica Madre y Maestra (PUCMM) y en la Universidad Autónoma de Santo Domingo (UASD); es autor de varias publicaciones, entre las que se destacan la tesis doctoral "Gobierno Electrónico y Percepción de Corrupción. Un estudio comparativo de su relación en América Latina", ensayos y artículos publicados en revistas, periódicos y su blog "Mi Visión del Mundo", así como coautor de la obra "Experiencias y Desafíos de la Descentralización de los Gobiernos Locales con Participación Social en la República Dominicana", publicada por la Dirección General de Cooperación Multilateral. Ha recibido varios reconocimientos a nivel nacional e internacional por algunos de sus ensayos y por su trayectoria en la Administración Pública. reysonl@hotmail.com

RESUMEN

Con la invención de la escritura, las antiguas civilizaciones encontraron la necesidad de proteger valiosas informaciones de no caer en las manos equivocadas, sea para garantizar el éxito en la guerra o en el comercio. La era de las computadoras trajo la necesidad de sofisticar los mecanismos de protección de esas informaciones, ahora resguardadas en medios informáticos, y con el advenimiento de la 4ta. Revolución Industrial y el Internet de las Cosas (IoT), el volumen de datos viajando por el ciberespacio lo que ha hecho es aumentar los riesgos y vulnerabilidades por lo que la Ciberseguridad ha emergido como un aspecto, no solo deseable o saludable, sino como imprescindible para construir la Sociedad de la Información y el Conocimiento.

Palabras clave:

Seguridad de la información, encriptación, ciberseguridad, amenazas, malware, internet de las cosas.

ABSTRACT

With the invention of writing, the ancient civilizations found the need to protect valuable information not to fall into the wrong hands, either to ensure success in war or trade. The computer era brought the need of more sophisticated mechanisms for the protection of these information now sheltered in electronic means and with the advent of the 4th Industrial Revolution and the Internet of Things (IoT), the volume of data traveling through cyberspace has increased risks and vulnerabilities by what Cybersecurity has emerged as an aspect, not only desirable or healthy, but as essential to build the Society of information and knowledge.

Keywords:

Information security, encryption, cybersecurity, threats, malware, internet of things, IoT.

Introducción

Desde el surgimiento de la especie humana, el hombre ha sentido la necesidad de garantizar su estabilidad, sus bienes, su bienestar. Ya sea de especies depredadoras, de inclemencias del tiempo o, incluso, de otros hombres. A ese concepto de "protección", es a lo que los romanos le llamaron "securitas", que incluso estaba personificada en una deidad con ese mismo nombre.

Moneda romana dedicada a Securitas

Cuando se inventa entonces la escritura, se suma la necesidad de proteger la "información", ya sea para garantizar el éxito tanto en el comercio como en la guerra. Por eso vemos que desde hace miles de años las primeras civilizaciones buscaron maneras de "encriptar" ciertas informaciones que entendían sensibles y las técnicas de protección de la información fueron modernizándose en la medida en que también lo hacía la tecnología disponible.

Desarrollo del tema:

Proteger la información valiosa no es cosa reciente, aunque pudiera pensarse que es algo que surgió con las dos primeras revoluciones industriales[1] . Muy por el contrario, desde los albores de la Historia se vio la utilidad de ingeniar mecanismos que garantizaran que los mensajes transmitidos fueron recibidos e interpretados exclusivamente por sus destinatarios.

Encriptación en la Antigüedad y Era Medieval

Las primeras evidencias de encriptación de información se remontan a miles de años antes de Cristo, como veremos:

- **1900 a.C.**: En la tumba egipcia de Khnumhotep II había un escrito con 222 inscripciones que utilizaban jeroglíficos no comunes para que el mensaje no fuera entendible para todos, excepto aquellos que conocieran la tabla de equivalencia de los símbolos.
- **1500 a.C.**: Existía una tablilla de Mesopotamia que contenía una fórmula cifrada para la fabricación de vidrio de cerámica.
- **500-600 a.C.**: Un escribano hebreo empleó un sistema de cifrado por sustitución para encriptar un trabajo realizado sobre el libro de Jeremías

Scytale griego para encriptar mensajes

- **487 a.C.**: Los griegos inventaron el dispositivo llamado Scytale, consistente en un bastón donde se enrollaba un listón de cuero sobre el que se escribía. Solo quien tuviera un bastón con las mismas dimensiones podía leer correctamente el mensaje escrito.
- **Siglo I a.C.**: Julio César implementa una sencilla pero efectiva técnica de encriptación, consistente en el desplazamiento del alfabeto en unos cuantos caracteres para que el mensaje fuera ilegible
- **855 d.C.**: Aparece el primer libro de criptografía en Arabia
- **1412 d.C.**: En Arabia se publica una enciclopedia de 14 tomos con distintas técnicas de encriptación.

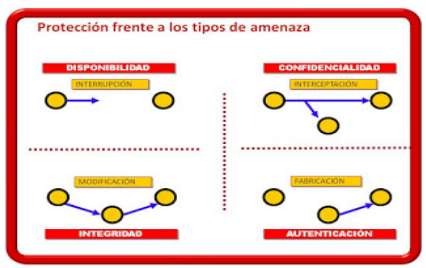
En los siguientes siglos se fueron perfeccionando las técnicas, apareciendo nuevas modalidades en Italia, Alemania y Francia, que sentaron las bases de la criptografía moderna.

1 Se les denomina así a los grandes procesos de cambio protagonizados por la industria que han trascendido el orden social, económico, político y cultural. La 1ra Revolución Industrial surgió en el siglo XVIII con la invención de la máquina de vapor, la 2da. en el siglo XIX con la invención de la electricidad y el motor de combustión, la 3ra. en el siglo XX con la invención de las computadoras y la 4ta. a principios del siglo XXI con la Inteligencia Artificial.

La Era de las Computadoras y el Internet

Con el surgimiento de las computadoras en los años 40s, las informaciones empiezan a ser generadas, transmitidas y almacenadas en medios electrónicos. Por ende, se comienzan a tomar medidas preventivas para resguardarlas sobre la base de estos cuatro principios o propiedades de la información:

- **Confidencialidad**: Es el aseguramiento del acceso a la información de aquellos que cuenten con la autorización para hacerlo.
- **Integridad**: Consiste en mantener la información libre de modificaciones no autorizadas. Por tanto, la información debe ser mantenida sin alteraciones ni manipulaciones de terceros no autorizados.
- **Disponibilidad**: La información debe ser accesible por las personas autorizadas en el momento en que lo requieran.
- **Autenticación**: Es el aseguramiento de quién es el generador de la información para así evitar la suplantación de identidad en la remisión del mensaje o información.



Propiedades de la Información y sus amenazas.

Por tanto, todos los protocolos de seguridad de la información tienen como objetivo garantizar esos cuatro aspectos o propiedades de la información.

Amenazas a la seguridad de la información

En una era caracterizada por el intensivo uso de la tecnología en las comunicaciones y transmisión de información, son muchas las amenazas que se ciernen sobre la confidencialidad, integridad, disponibilidad y autenticación de los datos:

- **Usuarios**: Resulta que son los propios usuarios una de las principales vulnerabilidades ya sea revelando a terceros su clave de acceso, utilizando claves de acceso poco seguras o teniendo políticas de seguridad en la organización que son muy flexibles o poco restrictivas.
- **Programas maliciosos**: Conocidos como **malware**, son aquellos desarrollados por expertos desarrolladores cuyo fin es acceder a informaciones o recursos de los sistemas de forma no autorizada. Hay diversas modalidades: **Troyanos** (programa aparentemente legítimo que le abre al intruso una puerta de acceso al sistema), **Gusanos informáticos** (programa capaz de duplicarse a sí mismo rápidamente para infectar un sistema de información), **Virus informáticos** (software que altera el funcionamiento normal de un dispositivo y que entra al sistema incorporado en el código de un programa infectado), **spyware** (programa espía que recopila información no autorizada del usuario para transmitirla a una entidad externa), etc. Muchos de los ataques procuran simplemente producir una Denega-

ción de Servicio (**DDos** por sus siglas en inglés) para hacer colapsar un servicio o página web.

- **Errores de programación:** Muchas veces en el desarrollo de los sistemas informáticos se crean involuntariamente "brechas" de seguridad que son detectadas y explotadas por programadores expertos llamados "**crackers**".
- **Intrusos**: Es todo aquel que logra entrar a un sistema o acceder a información sin estar autorizado para ello, ya sea auxiliado por malwares, por suplantación de identidad de usuarios o por la detección de brechas de seguridad.
- **Siniestros**: Un incendio, terremoto, robo o inundación puede producir la pérdida de información, especialmente por la destrucción física del medio de almacenamiento de los datos.
- **Personal técnico interno**: Personas con legítimo acceso a los sistemas de información pueden producir pérdida o filtrado de información de forma intencional ya sea por razones de espionaje, disputas internas, despidos, etc.
- **Fallas electrónicas de los sistemas**: Cuando algunos componentes clave del centro de datos falla y produce una caída del sistema o su mal funcionamiento.

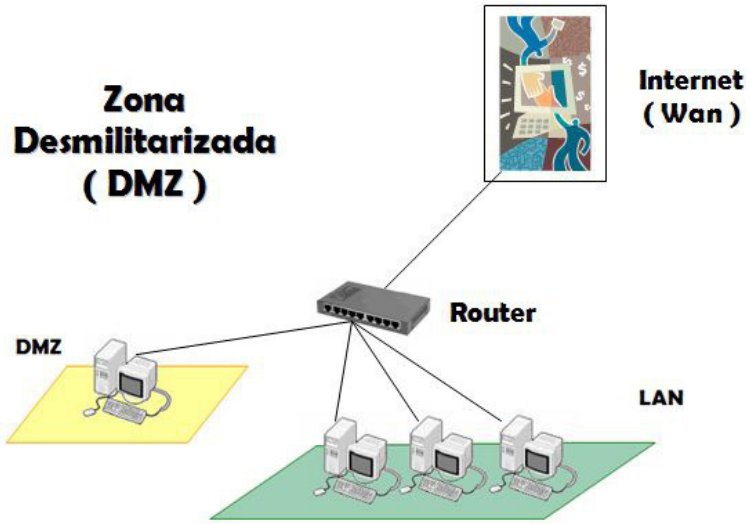
Anonymous es uno de los grupos de hackers más conocidos en todo el mundo.

Técnicas para asegurar la información

Los protocolos de seguridad de la información deben tomar en cuenta cada una de esas posibles amenazas, cada una de las cuales pueden ser enfrentadas y mitigado su riesgo.

- Para la potencial amenaza que representan los propios usuarios, se establecen políticas de establecimiento de **claves** o **passwords** con alto nivel de seguridad (inclusión de letras, números y caracteres especiales), el vencimiento periódico de dichas claves y restricción de los accesos según el nivel de seguridad de los usuarios, todo basado en una gestión centralizada de los permisos de acceso.
- Implementación de **cortafuegos** (firewalls) para evitar el acceso no autorizado y sistemas de detección de in-

trusos o antivirus que deben ser actualizados con regularidad.



Esquema de funcionamiento de una Red Perimetral o DMZ.

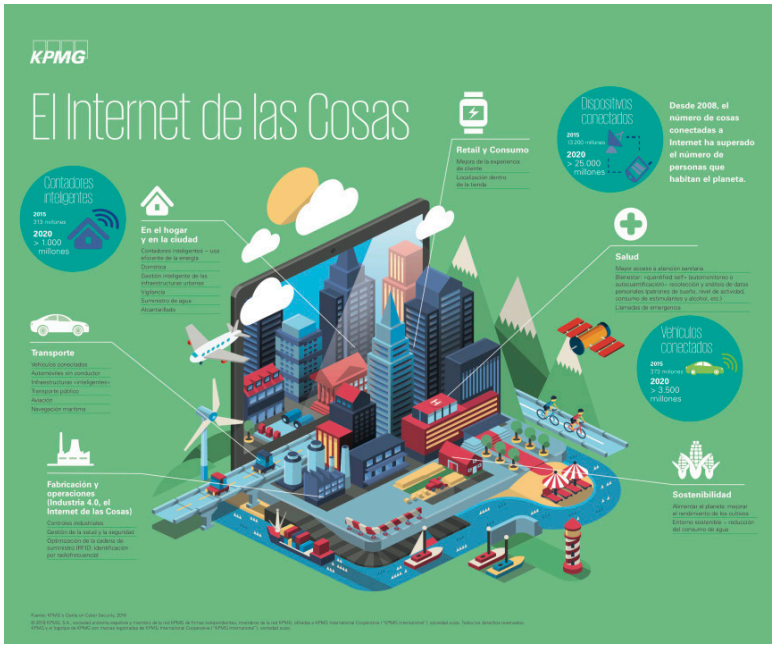
- **Habilitación de una Zona Desmilitarizada** (DMZ) o **Red Perimetral**, de forma que la red interna esté protegida ante ataques realizados a servidores de servicio externo como portal web y correos.
- **Sistemas de respaldo o backups** para poder recuperar la información o restablecer los servicios de los sistemas. Esto puede hacerse instalando sistemas que resguarden la información en sitios alternos o almacenando los datos en medios electrónicos alternos que permitan su restauración posterior.
- **Encriptación de los datos** para evitar que sean inteligibles en caso de caer en manos equivocadas.

Los villanos de la seguridad de la información

En esta era tecnológica han surgido diversos términos para identificar a los que se dedican a vulnerar los sistemas de información con distintos fines: lucro, venganza personal, espionaje industrial o militar o simplemente por desafío. Estos son los principales actores:

- **Hackers**: Es todo aquel programador experto en seguridad de los sistemas. Comúnmente tiene una connotación negativa, aunque los hackers pueden ser "**Hackers de sombrero blanco**" o los "***Ethical Hackers***" si trabajan en las organizaciones para detectar vulnerabilidades con el fin de corregirlas, o pueden ser "**Hackers de sombrero negro**" cuando utilizan sus conocimientos para actividades ilegales. Muchos hackers de sombrero blanco, por un tema de principios ideológicos, lo único que pretenden es dar a conocer informaciones que entienden deben ser públicas.
- **Crackers**: Son los Hackers de Sombrero Negro que hacen colapsar sistemas o roban información con el fin de obtener dinero, extorsionar o simplemente ufanarse de sus logros en las comunidades de hackers.
- **Phreakers**: Son expertos en telefonía terrestre y móvil que se dedican a vulnerar los sistemas de telecomunicaciones.
- **Newbies**: Es el "novato de red" que se inicia en la actividad de hacking.

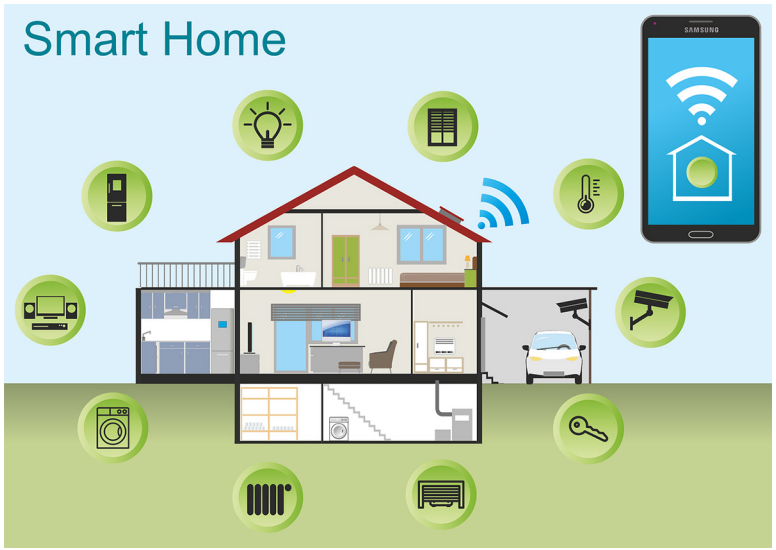
- **Script Kiddies:** Es un término moderno para describir aquellos que se encuentran en la actividad de hacking o cracking pero utilizan códigos elaborados por terceros por no tener la capacidad suficiente para crear los propios.



Conceptualización del Internet de las Cosas (elaborado por KPMG).

Seguridad de la Información y el Internet de las Cosas

La 3ra. Revolución Industrial inició con la Era de las Computadoras y llegó a su máximo esplendor con la llegada del Internet. Sin embargo, con el sostenido desarrollo tecnológico que nos trajo la Inteligencia Artificial, Machine Learning y el Internet de las Cosas (conocido como IoT por sus siglas en inglés), la 4ta. Revolución Industrial ha irrumpido de forma tal que la tecnología empieza a formar parte intrínseca de la cotidianidad de las personas. Sea a través de los teléfonos inteligentes, de los dispositivos "vestibles" o **wearables** o de la **domótica** (dispositivos en el hogar conectados a Internet), los dispositivos electrónicos conectados en línea están por doquier.



Concepto de Smart Home o Casa Inteligente (elaborado de Renovatia).

La incorporación exponencial de cada vez más dispositivos y sensores al Internet, para crear **Casas Inteligentes** (*Smart Homes*), ***Ciudades Inteligentes*** (*Smart Cities*) más el auge de la **robótica**, lo cierto es que nuestras sociedades están generando un volumen de información que está alcanzando tamaños hasta hace pocos años insospechados. Si pensamos que para el 2008 habían unos 7,000 millones de dispositivos conectados a Internet y que según las empresas CISCO y GARDNER GROUP[2] se estiman entre

2 Empresas que cuentan con divisiones de análisis y prospección tecnológica para predecir tendencias en la Era Digital.

25,000 y 50,000 millones los dispositivos que habrán conectados en el 2020, podemos imaginarnos de cómo crecerá la cantidad de datos viajando por el ciberespacio.

Eso significa que, si no se mejoran los protocolos de seguridad de la información y se dimensionan a los volúmenes proyectados, seremos más vulnerables. Por el Internet estará viajando abundante información personal relacionada con los lugares en que visitamos, las rutas que seguimos, la ropa que vestimos, si estamos estresados o cansados, qué comemos, etc. Estamos hablando de un paraíso de información para los hackers y crackers salir de pesca.

Una de las soluciones planteadas por los expertos es la incorporación de mecanismos físicos de encriptación incorporados a los múltiples sensores y dispositivos dotados con conectividad que proliferarán en el próximo lustro. El problema es que la mayoría de esos sensores son tan diminutos que físicamente se hace muy difícil incorporar estos mecanismos. Esto podría inducir a los fabricantes de esos sensores a incorporar mecanismos de encriptación relativamente sencillos que podrían dar pie a, por ejemplo, ataques de denegación de servicio[3] . Solo imaginémonos la posibilidad de que, en el contexto de una Ciudad Inteligente, un hacker ataque con el fin de producir tapones haciendo mal funcionar a los semáforos o los sensores de tráfico, o de que puedan entrar a nuestra red WiFi hogareña a través la televisión Smart o el monitor de bebé que tenemos instalado en casa.

En igual medida, según crezca el nivel de automatización y digitalización de las operaciones en el sector público y privado, especialmente en aquellas entidades que operen infraestructuras críticas, la seguridad de la información involucra a los organismos de defensa e inteligencia. Porque si ya el Internet es un terreno donde se practica la delincuencia, el terrorismo, el espionaje y toda clase de amenazas contra el Estado, empresas y ciudadanos, en un contexto de IoTel ciberespacio se convierte obligatoriamente en una de las más importantes líneas de defensa de la seguridad pública y hasta de la propia soberanía.

Conclusión

Ante el crecimiento exponencial de los datos que son diariamente procesados por dispositivos electrónicos, la industria TIC está actualmente abocada a fortalecer los protocolos de comunicación de los más de 20,000 millones de dispositivos electrónicos con conectividad a Internet que saldrán al mercado en los próximos 2 o 3 años.

Por supuesto, no cabe la menor duda de que así será, porque desde la invención de la primera computadora nació la necesidad de asegurar la información que esta genera, almacena y transmite. Y así seguirá siendo cuando todas las cosas que nos rodean estén conectadas entre sí para hacer de nuestra vida más productiva y placentera.

Y es que se vislumbra que, al igual que lo es el Derecho a la Libertad de Expresión, de Tránsito, a la Educación, Salud, Acceso a la Información Pública, etc., el Derecho a la Protección de los Datos Personales, en el marco de la Seguridad de la Información, se convertirá en un derecho fundamental del ciudadano de la Era Digital.

3 Un tipo de ataque cibernético que consiste en hacer colapsar a un servidor para que no pueda atender solicitudes de servicio legítimas mediante el bombardeo de múltiples solicitudes falsas de servicio para lograr su saturación.

Es por tal razón que garantizar esos nuevos derechos que genera la Sociedad de la Información y el Conocimiento deben ser prioridad para los estados modernos a través de estrategias concretas de Ciberseguridad, que protejan al Estado, a las organizaciones y a los ciudadanos de los peligros que los amenazan constantemente a través de este nuevo frente que los nuevos tiempos han abierto.

Porque es la información, y no el oro ni el petróleo, el bien más valioso en la Era Digital.

Referencias Bibliográficas:

Bishop, M. (2003). *What is Computer Security?*, IEEE Security and Privacy Magazine 1(1):67 – 69, 2003. Doi: 10.1109/MSECP.2003.1176998.

CISCO (2016). *Internet of Things. At-a-glance*. CISCO: San José, CA.

Ferreiro, M.A. (2018). Los primeros métodos de encriptación de la Antigüedad. El Reto Histórico. Revista Digital. Recuperado de https://elretohistorico.com/encriptacion-mensajes-secretos-espias-antiguedad-criptologia/ el 28 de octubre de 2018.

Hung, M. (2017). *Leading the IoT. Gartner*, Inc.: Stamford, CT.

Shimeall, T. y Spring, J. (2014). *Introduction to Information Security*: A Strategic-Based Approach. Elsevier.