LA SEGURIDAD INFORMÁTICA. SEGURIDAD INFORMÁTICA APLICADA A LA DEFENSA Y SEGURIDAD BASADA EN PRINCIPIOS JURÍDICOS

COMPUTER SECURITY. COMPUTER SECURITY APPLIED TO DEFENSE AND SECURITY BASED ON LEGAL PRINCIPLES

IRENE VALENCIA BALLADARES[1], ALEX TAPIA CHICHANDE[2]

1 Universidad Católica de Santiago de Guayaquil, Ecuador. Doctorando URJC, España. *irene.valencia@cu.ucsg.edu.ec*
2 Armada del Ecuador. *aptapia@armada.mil.ec*

RESUMEN

El considerable aumento e incidencia en el uso de las tecnologías de la información y comunicación, han generado una mayor vinculación de las actividades humanas a los elementos tecnológicos. En efecto, dentro de la mayoría de actividades comunes, propias de la cotidianeidad de las personas, se verifica la presencia de herramientas tecnológicas tendientes a facilitar la ejecución de los distintos procesos, logrando prontos y mejores resultados que los conseguidos a través de la aplicación de medidas tradicionales. Sin embargo, la construcción de herramientas informáticas se ha venido desarrollando a la par de amenazas y ataques informáticos, cada vez más comunes y complejos en su detección, constituyendo un verdadero peligro para la seguridad de las personas e instituciones. En este sentido, el presente trabajo busca presentar una prospectiva de la seguridad informática, en el ámbito de la defensa y la seguridad.

PALABRAS CLAVE: Seguridad informática, seguridad de la información, ciberdefensa, ataques informáticos.

ABSTRACT

The considerable increase and incidence in the use of information and communication technologies have generated a greater link between human activities and technological elements. Indeed, within the majority of common activities, typical of people's daily lives, the presence of technological tools tending to facilitate the execution of the different processes is verified, achieving prompt and better results than those achieved through the application of traditional measures. However, the construction of computer tools has been developing alongside computer threats and attacks, which are increasingly common and complex in their detection, constituting a real danger to the security of people and institutions. In this sense, this work seeks to determine a prospective of computer and information security, in the field of defense and security.

KEYWORDS: Computer security, information security, cyber defense, computer attacks.

DOI: http://dx.doi.org/10.23878/alternativas.v21i2.335

RECIBIDO: 12/3/2020
ACEPTADO: 7/6/2020

INTRODUCCIÓN

Entre los activos inmateriales que poseen las organizaciones, el más importante está constituido por la información que se encuentra almacenada en los distintos centros de datos o servidores, a los cuales, los atacantes se dirigen con el ánimo de apoderarse de su contenido, a través de la utilización fraudulenta de diferentes medios electrónicos, que se convierten en herramientas para el cometimiento del ilícito.

Frente a tales circunstancias, la seguridad informática ha cobrado una trascendental importancia dentro del ámbito de las organizaciones, manifestado en conjunto con la seguridad de la información, como segmento que involucra tanto a los procesos, como a las personas.

Es así que, existen múltiples segmentos que se vienen desarrollando dentro de la esfera de la seguridad informática, como son: leyes y reglamentación, computación en la nube, computación forense, criptografía, entre otros, tendientes a repeler las amenazas generadas en el ambiente virtual.

En este sentido, los escenarios específicos del internet, la computación móvil y los sistemas analíticos de datos, se perfilan como retos para determinar un apropiado y seguro tratamiento de la información y la privacidad de los datos existentes; sin embargo, mientras más interconectadas se encuentren las personas, el control dirigido hacia el intercambio de información que se genera, será mucho más difícil de ejercer. No obstante, existirán mayores facilidades, productos personalizados y experiencias particulares que permitan mejorar la seguridad en la administración e intercambio de información.

ANÁLISIS

PRINCIPIOS RECTORES DE LA SEGURIDAD DE LA INFORMACIÓN

Al respecto, es menester indicar que tanto los principios que guían la protección de la información, así como los diversos procedimientos que se construyen alrededor de estos, se encuentran destinados hacia una disminución de los riegos que afrontan las múltiples interacciones humanas desarrolladas a través de los elementos informáticos; por lo tanto, resultaría utópico hablar de una seguridad o herramienta de protección absoluta para la plena conservación de la actividad virtual. Dicho esto, la actividad de seguridad y defensa de la información se rigen, básicamente, a través de los siguientes principios concretos:

- Principio de Confidencialidad

Este principio presupone el resguardo apropiado de la información, sin que terceros no autorizados tengan acceso al contenido de los datos almacenados, conservando la seguridad de los mismos.

- Principio de Integridad

En virtud de este principio, la información almacenada se encuentra resguardada en cuanto a la exactitud y totalidad de datos que contiene; ello, involucre también a las diferentes técnicas de procesamiento.

- Principio de Disponibilidad

Propugna un acceso libre y absoluto a la información, por parte de las personas autorizadas para su manejo y configuración, evitando peligros paralelos al momento de su revisión.

LEYES Y REGLAMENTACIÓN

Para denominar de manera global a estas conductas, a lo largo del amplio marco de legislaciones en el mundo, los ordenamientos jurídicos de algunos países, han acogido el término de delito "informático", en otros se lo ha denominado "cibernético" o "telemático". Sin embargo, en algunos Estados, aún no se ha legislado de manera concreta alrededor de estos temas, empleándose instituciones jurídicas aproximadas, generalmente de tipo civil y penal, bajo el eminente riesgo de que las causas no prosperen en los tribunales de justicia, por falta de sustento legal que justifiquen la activación de la potestad jurisdiccional (tipicidad de acciones e infracciones).

Efectivamente, a través del empleo de las nuevas tecnologías de la información y comunicación (NTIC), se pueden apreciar diversas conductas delictuales, concretamente definidas. De este modo, algunos autores analizan esta temática, bajo el nombre de "criminología virtual", y otros, a través de la etiqueta de "ciberdelincuencia": es así que, los delitos tradicionales de estafa, chantaje, extorsión, perpetrados en la sociedad virtual mediante las NTIC y otras formas contemporáneas, se llevan a cabo desde la red y terminan materializando una agresión en contra de la confidencialidad, integridad y disponibilidad de la información. En virtud de lo dicho, se puede hacer referencia a delitos relativos a datos personales, ciberterrorismo, ciberataques, delitos económicos, delitos de pederastia, delitos contra los derechos de autores de software y música, delitos contra la

propiedad intelectual, entre otros actos ilícitos de relevancia jurídica.

Evidentemente, los países que han emprendido la tarea legislativa de penalizar los delitos informáticos, han logrado dar un paso significativo en la lucha contra su impunidad; sin embargo, existen diversos inconvenientes, principalmente evidenciados en cuanto a su prosecución, tal como se destaca a continuación:

> Con la llegada de Internet, las grandes redes de telecomunicaciones y la información digital, las fronteras entre naciones se han difuminado. Así como consumimos servicios alojados en otros países, guardamos nuestra información en "la nube" o enviamos información que viaja a través de redes internacionales, cuando se trata de un delito informático (o incluso evidencia digital) la investigación generalmente trasciende el territorio de una nación. Esto resulta un tanto complejo a nivel legislativo, especialmente si las leyes de los países involucrados no están alineadas (Pastorino, 2017).

En efecto, a nivel regional y mundial, todavía no existe un acuerdo internacional ratificado por la mayoría de naciones. De tal modo que, aún se encuentra pendiente la producción de esfuerzos serios y destinación de recursos, de manera mancomunada, que permitan garantizar la seguridad en el almacenamiento y transmisión de la información, a través de herramientas con valor jurídico, de aplicación directa en el marco de los distintos ordenamientos, respondiendo eficazmente a las dificultades propias reportadas en las actividades de seguimiento de los ilícitos informáticos.

Gráfico 1: Dominios de la Norma ISO 27001

Sin embargo, encontrándose justificada la existencia de normas de carácter internacional, emitidas con la consigna de mejorar la seguridad de la información, se han empezado a emprender gestiones para su regulación; muestra de ello, es la norma ISO 27001, la cual abarca varios dominios de trabajo. Ver Gráfico No 1.

Esta norma, entre otros motivos, se destaca por lo siguiente:

> La norma define de manera genérica, independientemente de los factores ambientales de organización (entorno, contexto, activos de las TIC, información, cultura organizacional, etc.) —tanto internos como externos a la misma— y de los activos de los procesos de la organización (políticas, procedimientos, procesos, etc.), cómo se planifica, implanta, verifica y controla un Sistema de Gestión de Seguridad de la Información (SGSI), a partir de la realización de un análisis de riesgos y de la planificación e implantación de la respuesta a los mismos para su mitigación. Es decir, cualquier empresa u organización puede desplegar un SGSI siguiendo este estándar (Universidad Internacional de La Rioja, 2019).

En igual sentido, surge el Convenio sobre Ciberdelincuencia o simplemente Convenio de Budapest, aprobado por el Comité de Ministros del Consejo de Europa, el 8 de noviembre de 2001, el cual constituye el primer instrumento internacional promulgado a modo de respuesta defensiva a los delitos informáticos y cualquier tipo de infracciones cometidas a través del uso de medios electrónicos. Entre las diversas problemáticas que busca enfrentar para lograr su cometido fundamental, se encuentra sin lugar a dudas, el propugnar por una armonización de las distintas legislaciones, entendiendo que el crimen informático trasciende las fronteras territoriales de los países; así mismo, busca incentivar una mayor cooperación por parte de los Estados suscriptores y la adherencia de más naciones, abriéndose a la firma en Budapest, el 23 de noviembre de 2001, dentro del contexto de la Conferencia Internacional sobre la ciberdelincuencia.

COMPUTACIÓN EN LA NUBE

En cierto sentido, no se posee una definición generalmente acordada; sin embargo, existen diversos organismos de carácter internacional, cuyos objetivos se circunscriben a la estandarización de Tecnologías de la Información y, en forma concreta, de Cloud Computing.

Efectivamente, entre las organizaciones de mayor relevancia a nivel internacional, se encuentra el National Institute of Standards and Technology (NIST) y su Information Technology Laboratory, los mismos que extienden y analizan la siguiente definición:

> La nube es un conjunto de hardware y software, almacenamiento, servicios e interfaces que facilitan la entrada de la información como un servicio. El mundo de la nube tiene un gran número de actores o participantes. Los grupos de intereses del mundo de la computación en nube son: los vendedores o proveedores: proporcionan las aplicaciones y facilitan las tecnologías, infraestructura, plataformas y la información correspondiente; los socios de los proveedores: crean servicios para la nube, ofreciendo servicios a los clientes; los líderes de negocios: evalúan los servicios de la nube para implantarlos en sus organizaciones y empresas; los usuarios finales utilizan los servicios de la nube, gratuitamente o con una tarifa (Joyanes, 2012).

De esta manera, la nube se plantea como una nueva dinámica que supera las tradicionales interacciones presentes en el Internet; busca, entre otras cosas, que los procesos sean más agiles y seguros, reduciendo el tiempo en su ejecución y logrando conectar a las personas de una forma ágil e inmediata. Todo ello, dentro de un marco de automatización de procedimientos, en los que se reducen los costos de interacción, circunscrito en el medio virtual, con diferentes fines (sociales, comerciales, laborales, entre otros).

De esta manera, se espera que para los años venideros, la computación en nube se convierta en una estrategia consolidada de interconexión, siendo incorporadas de esta manera, las gestiones propias de diversos tipos de actividades, a arquitecturas que no dependan de un hardware o software en específico; fenómeno que será capaz de vincular tanto los entornos propios de la actividad privada, como pública.

Consecuentemente, el ofrecimiento material que brinda la computación en nube, viene dado por la manera en que reforma los paradigmas para la construcción de software. Lo dicho, teniendo presente que tanto los administradores de TI, como los distintos desarrolladores, detentan la capacidad de crear auténticos núcleos sobre los cuales se construye una verdadera infraestructura de centros de datos virtuales, donde los recursos se encuentren virtualmente conectados a través de las nubes y locales, y los desarrolladores puedan tener acceso a las API de servicios en las aplicaciones y middleware de diferentes proveedores.

Evidentemente, este prometedor mercado se enfrenta a muchos desafíos y oportunidades. A pesar de ser diversas las amenazas a las que se somete todo tipo de información almacenada en la nube, cada vez son mayores los datos contenidos en ella, principalmente en las gestiones privadas de amplios sectores comerciales, motivado, como ya ha sido destacado, por la practicidad que esta dinámica reporta, en cuanto a la forma de visualizar la información y administrarla.

Esto nos lleva a pensar en sistemas de defensa que exploten las ventajas de los servicios en la nube de manera segura; generalmente, en el ámbito de las interacciones personales, se suelen implementar herramientas relacionadas con la determinación de claves o encriptación de los datos almacenados. Sin embargo, dentro del contexto de las organizaciones, los desafíos de seguridad aumentan exponencialmente, debido de manera principal, por el acceso masivo que tienen los trabajadores o funcionarios, a la información almacenada; he ahí que surge la necesidad de implementar herramientas y recursos mediante los cuales se pueda, entre otras cosas, determinar la identidad de las personas que están accediendo a los datos en la nube.

COMPUTACIÓN FORENSE

La Informática forense, entre otras consideraciones, es la "ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en soportes informáticos" (Fernández, 2018). En otras palabras, constituye una disciplina que involucra a diversas técnicas de investigación, identificación, extracción, conservación, exploración y análisis de información almacenada en soportes digitales; esta actividad, en efecto, tiene su ámbito específico de desarrollo, dentro

de un esquema legal de investigación, por el presunto cometimiento de ilícitos.

En efecto, la Informática forense se desarrolla en el ámbito legal, obedeciendo a una gestión probatoria destinada a recabar información suficiente que sirvan de soporte objetivo para su valoración y consecuente construcción de una decisión judicial; "la evidencia puede ser cualquier tipo de dato almacenado en un dispositivo informático que los peritos deben recoger en la escena del crimen digital" (Presman, 2016).

Lógicamente, para el óptimo desarrollo y ejercicio de esta práctica forense, se requiere contar con profesionales que posean sólidos conocimientos, tanto de carácter técnicos como jurídicos, y que evidentemente cuenten con instrumentos de software y hardware, necesarios para el cumplimiento de sus gestiones investigadoras.

En este sentido, resulta meritorio resaltar que, de la encuesta Global de Análisis Forense de Datos 2016 de EY[1], se destacaron los siguientes aspectos:

- La alta gerencia encuentra la necesidad de implementar herramientas de Análisis Forense de Datos, FDA para tratar los principales riesgos del negocio.
- Existe un aumento considerable de empresas que utilizan herramientas de Análisis Forense.
- El 56% de las empresas que han implementado herramientas FDA, han obtenido resultados positivos.

Esta información nos lleva a considerar que las metodologías de análisis forense de datos crecerá en las diferentes entidades y organizaciones.

CRIPTOGRAFÍA

Según el Diccionario de la Real Academia de la Lengua, la palabra criptografía proviene de las raíces griegas "kriptos" que significa oculto, y "graphos", que significa escritura, que al unirse darían como resultado: "escritura oculta" y, que en la actualidad puede traducirse como el arte de la escritura de mensajes en clave o en secreto. Sin embargo, una definición más completa sería la siguiente:

> "Rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves" (Iglesias, 2017).

Por consiguiente, como resultado del vertiginoso desarrollo de las NTIC, en conjunto con la prolífera implementación de las comunicaciones digitales, se ha generado un número creciente de problemáticas alrededor de la seguridad, motivo por el cual, el objetivo central de la criptografía ha sido necesariamente ampliado, con la finalidad de estudiar las técnicas destinadas a dotar de seguridad a la información, pudiendo clasificar los criptosistemas, de la siguiente manera: criptografía simétrica y criptografía asimétrica

Por lo tanto, la criptografía simétrica se emplea para poder cifrar de manera masiva, grandes cantidades de información, de una forma más ágil; se encuentra técnicamente integrada por un conjunto de algoritmos que tanto el emisor como el receptor utilizan en sus interacciones, mediante una sola llave, denominada clave privada, con la función fundamental de cifrar y descifrar el mensaje secreto, quedando condicionada la seguridad en la clave y no en el algoritmo usado.

Por su parte, la criptografía asimétrica se encuentra compuesta por un conglomerado de algoritmos, que tanto el emisor como el receptor ejecutan, a través de dos llaves diferentes, con la premisa de cifrar y descifrar el mensaje secreto contenido; como característica específica, la llave para cifrar mensajes se denomina "clave pública" y puede ser conocida por todos, mientras que por su parte, la llave para descifrar mensajes se llama "clave privada" y sólo llega a ser conocida por un usuario, debiendo mantenerla en secreto, con lo cual el número de claves que emplea este criptosistema, se encuentra directamente determinado por la cantidad de usuarios intervinientes.

En resumidas palabras, este tipo de criptografía contempla una variada cantidad de técnicas destinadas a establecer una comunicación segura entre el emisor y el receptor, empleando una clave secreta compartida, que puede ser usada como llave para cifrar y descifrar mensajes empleando métodos de criptografía simétrica.

[1] Encuesta realizada por la empresa Ernst & Young, líder mundial en servicios de auditoría, entre junio y septiembre del 2015 a 665 ejecutivos de empresas de 17 países a nivel mundial.

De este modo, se espera que en un futuro próximo, cuando se construya una computadora cuántica, los principios de la criptografía moderna se desmoronarán, debido a que la mayor parte de los sistemas criptográficos actuales dependen de la complejidad matemática para factorizar números grandes, dado que no existe un algoritmo capaz de factorizarlo en un tiempo polinomial con las computadoras actuales.

CONCLUSIONES

1. El uso masivo de las tecnologías de la información y comunicación, han ocasionado que se multipliquen las amenazas que afrontan los sistemas informáticos; es por ello que se requiere mejorar los sistemas de seguridad informática y los procesos de la seguridad de la información.
2. La tendencia regional y mundial se encuentra decantada hacia la promulgación de nuevas leyes, a la par de la determinación de nuevos estándares que permitan asumir la tarea de defensa y seguridad de la información en las organizaciones.
3. Sin lugar a dudas, las áreas de trabajo circunscritas al ámbito de la seguridad informática, cada día experimentan adelantos científicos que permiten mejorar las capacidades de almacenamiento y procesamiento de la información.

REFERENCIAS BIBLIOGRÁFICAS

Fernández, P. (24 de noviembre de 2018). Qué es la informática forense y cómo se usa para resolver casos policiales o judiciales. Obtenido de https://www.europapress.es/portaltic/sector/noticia-informatica-forense-usa-resolver-casos-policiales-judiciales-20181124112932.html

Iglesias, I. (26 de enero de 2017). Introducción a la Seguridad Informática. Obtenido de https://silo.tips/download/capitulo-3-introduccion-a-la-seguridad-informatica#:~:text=La%20criptograf%C3%ADa%20es%20aquella%20rama,usando%20una%20o%20m%C3%A1s%20claves.

Joyanes, L. (2012). Computación en la Nube: Notas para una estrategia española en Cloud Computing. Obtenido de Dialnet-ComputacionEnLaNube-4098278_1.pdf

Pastorino, C. (6 de diciembre de 2017). Convenio de Budapest: beneficios e implicaciones para la seguridad informática. Obtenido de https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/

Presman, G. (10 de mayo de 2016). Desafíos de la Informática Forense. Obtenido de http://web9.unl.edu.ar/noticias/news/view/desaf%C3%ADos_de_la_inform%C3%A1tica_forense_1#.YBCdR15KhH0

Universidad Internacional de La Rioja. (11 de diciembre de 2019). ¿Qué es la certificación ISO 27001 y para qué sirve? Obtenido de https://www.unir.net/ingenieria/revista/iso-27001/