Fundamentos sobre Seguridad de la Información

Nota 1 de 5

Jorge Alejandro Mieres

El avance tecnológico trajo aparejada la evolución de ciertos programas con características maliciosas y paralelamente a ello, la difusión de nuevas técnicas y metodologías de ataques y amenazas informáticas cada vez más sofisticadas y cada vez más eficaces. A través de éste artículo se pretende dar una noción lo suficientemente clara sobre los puntos más importantes en materia de Seguridad de la Información, los objetivos que persigue y porqué se ha convertido en una necesidad que ningún tipo de organización debería obviar.

A principios de la década del 80 empieza a ser común el uso de computadoras personales en ámbitos hogareños. Luego, durante los primeros años de la década del 90 ven la luz una serie de programas denominados virus informáticos y a partir de ese momento, se comienza a tomar conciencia del peligro que representa este tipo de códigos para cualquier sistema y equipos conectados a Internet.

Provocando el punto de partida por el cual se comenzó a valorar en su justa medida el precio de la seguridad, a tener muy en cuenta las debilidades de los sistemas informáticos y ver la importancia que tiene la información para cualquier organización.

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones, situación que inevitablemente se traduce en pérdida económica.

Por otro lado, la falta de seguridad en las redes es un problema que está en crecimiento por el sólo hecho de subestimarse las fallas que a nivel interno se producen, sobre todo teniendo en cuenta que la propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo.

Cada vez es mayor el número y tipo de nuevos ataques y día a día van adquiriendo habilidades más especializadas que les permiten obtener mayores beneficios. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas informáticos.

Al igual que en cualquier aspecto de la vida, lograr en un sistema informático un 100% de seguridad, es imposible, más allá de las discusiones que se puedan originar en torno a las distintas plataformas que existen, ya que cada uno de los componentes y piezas que conforman un sistema son susceptibles a poseer un importante margen de error debido a la naturaleza de su origen. Son creados por seres humanos, tanto en el diseño y desarrollo de una aplicación (software), implementación de un nuevo dispositivo (hardware) o en el desempeño del profesional, léase también personal de la institución, que forma parte de ese sistema informático por el sólo hecho de utilizar sus recursos.

Fundamentos sobre Seguridad de la Información

Conceptualmente hablando, se percibe una clara confusión sobre la diferencia que existe entre Seguridad Informática y Seguridad de la Información. Por ello, antes de continuar con el tema en cuestión conviene aclarar este punto.

Si bien ambas materias se complementan e interactúan constantemente en los sistemas informáticos, poseen objetivos bien diferenciados: por un lado, **Seguridad Informática (*si*)** se encarga de la protección de los sistemas informáticos, entendiéndose esto último como la conjunción de la información (software), los equipos que soportan la información (hardware) y las personas que hacen uso de la misma (usuarios); básicamente, todo lo que se encuentre en un medio informático. Mientras que, **Seguridad de la Información (*SI*)** es un proceso mucho más amplio que implica la protección no solo de la información almacenada en los sistemas informáticos sino que también pretende asegurar la información sin discriminar donde se encuentra. En otras palabras, *SI* va mucho más allá de *si*, y tiene como propósito salvaguardar la información procesada, sin importar el medio por el cual circule o el lugar en que se encuentre almacenada.

"...la falta de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de ataques y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas..."

La información es un "importante" patrimonio que puede ser guardada de diferentes formas, en diferentes medios y a través de diferentes canales, no solo puede ser almacenada digitalmente sino que también puede estar impresa, escrita en papel de puño y letra, y no se limita únicamente a estas formas sino que también puede ser encontrada en filmaciones, grabaciones, mediante el lenguaje oral (conversacional) e

incluso en la memoria de las personas. Además de poder ser transmitida a través de diferentes medios, sean éstos canales de comunicación convencional (analógica) o de última generación (digitales).

Independientemente del carácter que adopte la información, se acopie o se disemine, debe estar protegida adecuadamente a fin de garantizar en todo momento la confidencialidad, integridad y disponibilidad de los datos *(CID)*.

Por ello, el principal objetivo en Seguridad de la Información es justamente ese, proteger de una manera adecuada la información, preservando una serie de parámetros fundamentales para que los activos (todo aquello que puede ser medido a través de un costo) puedan considerarse protegidos y seguros, reduciendo al máximo posible los daños ocasionados por alguna eventualidad que impida el normal funcionamiento de la organización, sea esta comercial o militar.

Este objetivo se logra a través de un conjunto de metodologías, prácticas y procedimientos que tienden a proteger la información de cualquier tipo y en cualquier momento y lugar.

Parámetros básicos de Seguridad de la Información

Habitualmente, al abordar la problemática sobre Seguridad de la Información, se tiende a analizar sólo los aspectos relativos a los medios informáticos (copias de seguridad, mantenimiento de las computadoras, servidores, redes, etc.), todos ellos orientados a la disponibilidad de la información, olvidando otras características que se deben atender y que guardan el mismo nivel de criticidad como lo son la confidencialidad y la integridad de los datos y servicios.

El exceso de confianza y la falta de concientización son los principales problemas, ya que son los responsables de dejar que la seguridad descanse en su totalidad sobre lo tecnológico (herramientas antivirus, firewall, IDS, etc.) logrando con ello una falsa sensación de seguridad.

Es importante tener en cuenta que el factor humano cubre casi el 99% de la seguridad y que sólo el 1% esta constituido por el aspecto tecnológico.

Mantener la información debidamente protegida es equivalente a mantenerla segura ante amenazas que puedan afectar la funcionalidad, ya sea corrompiéndola, accediendo a ella en forma indebida, eliminándola e incluso robándola.

> **"Seguridad de la Información tiene como propósito salvaguardar la información procesada, sin importar el medio por el cual circule o el lugar en donde se encuentre almacenada."**

Por lo tanto, Seguridad de la información tiene como objetivo proteger la información de la organización preservando tres parámetros básicos conocidos como CID: confidencialidad, integridad y disponibilidad.

Confidencialidad de la información.
Garantiza que únicamente personal autorizado tendrá acceso a la información, es decir, la información posee un grado de privacidad que se debe respetar y preservar para que personas sin autorización no puedan acceder a ella. Si la información es

confidencial no debe ser divulgada ya que la pérdida de confidencialidad equivale a la pérdida del secreto. Además, cuanto más valiosa es la información mayor debe ser su grado de confidencialidad, y cuanto mayor sea el grado de confidencialidad mayor será el nivel de seguridad que deberemos implementar.

Integridad de la información.
Garantiza que la información no será alterada, eliminada o destruida por entidades no autorizadas, preservando la exactitud y completitud de la misma y de los métodos utilizados para su procesamiento, es decir, la información es recibida como fue enviada, por lo tanto es íntegra. Esto significa que se encuentra en su estado original. Si llegase a sufrir alteraciones entonces pierde integridad.

Disponibilidad de la información.
Permite asegurar que los usuarios autorizados tendrán acceso a la información y sus medios asociados cada vez que lo requieran, es decir, la disponibilidad no sólo involucra la información sino que también toda la estructura física y tecnológica que permite el acceso, el tránsito y el almacenamiento garantizando que la misma llegue en el momento oportuno.

Estos tres parámetros forman la columna principal de la Seguridad de la Información, constituyendo los mecanismos esenciales y pilares básicos para lograr la generación de confianza. Contar con una buena implementación de estos tres principios básicos es la situación deseable para cualquier organización, ya sean instituciones de gobierno, educativas, militares, etc., por lo que siempre deben estar presentes para garantizar un adecuado nivel de seguridad.

Asimismo, además de implementar los mecanismos necesarios que posibiliten garantizar los tres aspectos antes mencionados, se deberían tener presentes otras características adicionales que en un segundo plano apoyarán y ayudarán al fortalecimiento de toda la estructura del ambiente informático y a la protección de la información. Estas características que integrarán la segunda columna como aspectos secundarios podrán estar constituidas por las siguientes:

Control: consiste en controlar quien utiliza el sistema (o cualquiera de los recursos que ofrece) y cómo lo hace.

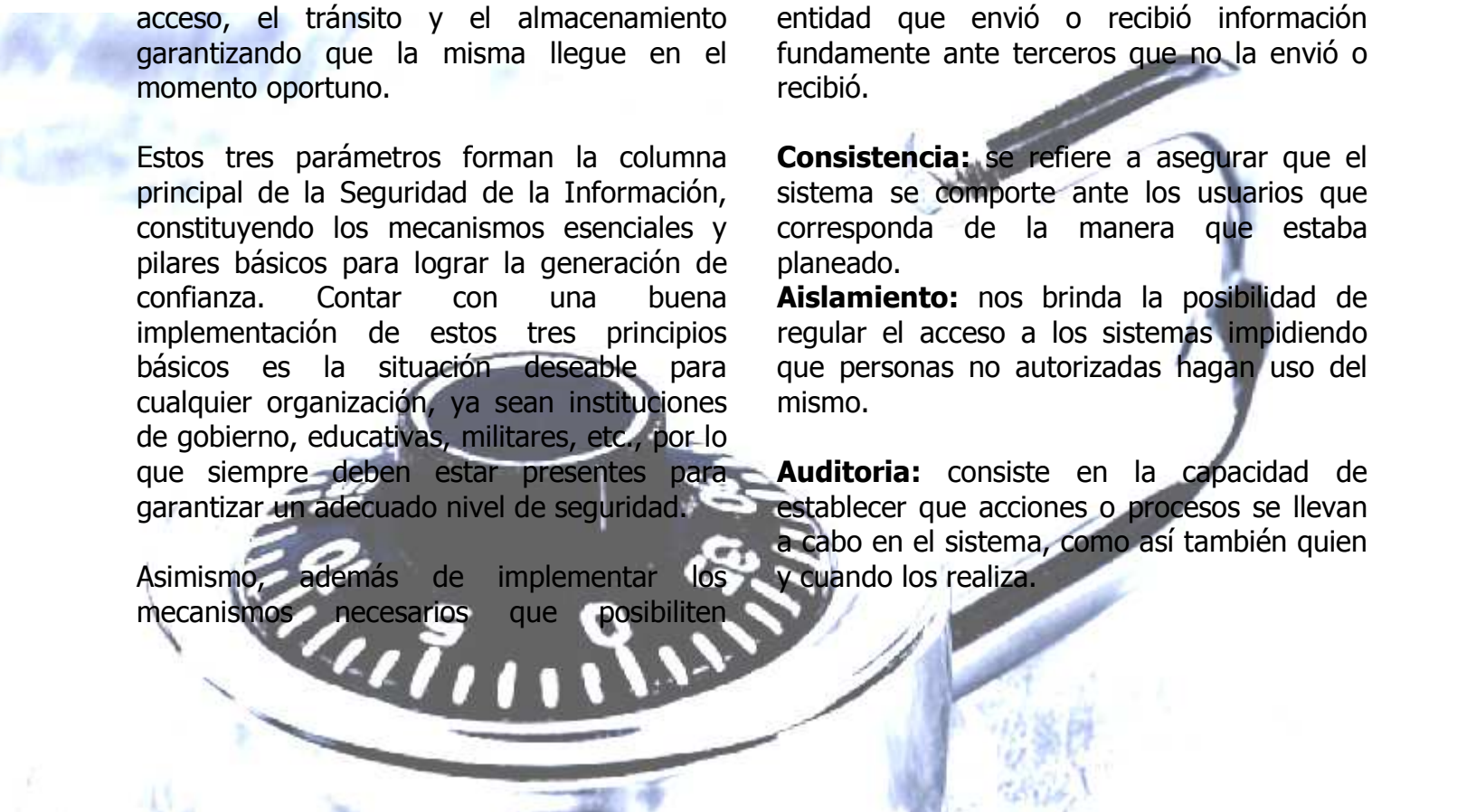
Autenticidad: garantiza que quien dice ser "x" es realmente "x", implementando mecanismos para verificar quien está enviando la información. En otras palabras, el objetivo de este proceso es asegurar la identificación de una persona o cosa.

Protección a réplica: se basa en asegurar que una transacción sólo sea realizada una vez, a menos que se defina lo contrario.

No Repudio: trata de asegurar que cualquier entidad que envió o recibió información fundamente ante terceros que no la envió o recibió.

Consistencia: se refiere a asegurar que el sistema se comporte ante los usuarios que corresponda de la manera que estaba planeado.
Aislamiento: nos brinda la posibilidad de regular el acceso a los sistemas impidiendo que personas no autorizadas hagan uso del mismo.

Auditoria: consiste en la capacidad de establecer que acciones o procesos se llevan a cabo en el sistema, como así también quien y cuando los realiza.



Entonces, en base a todo lo expuesto y siguiendo los lineamientos tipificados en la norma ISO/IEC 27002:2005 (ex ISO/IEC 17799:2005) "la seguridad de la información se logra implementando un conjunto adecuado de controles que abarcan políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software a partir de los que se trata de preservar los activos de información."

Todas estas implementaciones deben presentar un balance entre un uso transparente para los usuarios y la máxima seguridad, todo a un costo razonable.

Por otro lado, parte de nuestro trabajo como profesionales en Seguridad de la Información será hacer recomendaciones y tomar acciones para minimizar los riesgos y exposición de la información. Estas actividades no son sencillas pero hay que tener en cuenta que son necesarias para mantener la información dentro de niveles razonables de protección.

Una apropiada gestión de la Seguridad de la Información permite garantizar los adecuados niveles de seguridad exigibles para cualquier tipo de Organización.

Sobre todo asumiendo que el objetivo no es eliminar los riesgos sino gestionarlos, y que la seguridad no es un producto sino que es un proceso.

Glosario

Ataque: Acción de vulnerar la seguridad explotando algún tipo de bug o problema en el software o hardware del sistema.

Amenaza: Agentes capaces de explotar los fallos de seguridad o debilidades de un sistema informático.

Activo: En Seguridad de la Información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma.

Bug (bicho, error): Error persistente en un software o hardware.

Dato: Unidad mínima que compone cualquier información.

Firewall (cortafuego): Sistema que se coloca entre una red local (LAN) e Internet permitiendo asegurar las comunicaciones entre dicha red e Internet.

Hardware (soporte físico): Conjunto de elementos materiales que componen una computadora.

IDS (Sistema de Detección de Intrusos): Programa capaz de detectar accesos no autorizados a un sistema o a una red.

Información: Conjunto de datos que al ser unidos tienen un significado especifico más allá de cada uno de estos. 2, 0, 0, 7 son datos, 2007 es información.

Riesgo: Probabilidad de que un ataque se consuma explotando una vulnerabilidad.

Software: Conjunto de programas que pueden ser ejecutados por el hardware para realizar tares solicitadas por los usuarios.

Virus Informático: Archivo o porción de código ejecutable capaz de reproducirse, auto-ejecutarse y ocultarse.

Vulnerabilidad: Debilidad en la Seguridad de la Información de una Organización que potencialmente permite que una amenaza afecte los activos.

Bibliografía.
CISSP All-In-One. Third Edition. Shon Harris. 2003 (Certified Information Systems Security Professional).
Norma ISO/IEC 27002:2005, Código de Prácticas para la Gestión de la Seguridad de la Información.
Security in Computing, Fourth Edition. Prentice. 2006.