Seguridad Informática – Un tema para no dejar en el olvido.
"Visión General"

Paredes Corredor, Omar Ricardo.
Universidad Piloto de Colombia, Bogotá, Colombia
omarr_p@hotmail.com

Abstract* — *Nowadays, there is a high number of ill-intentioned people who try to get unauthorised access to our computers information and the business information systems. This number is increasing and one of the possible consequences of being a victim of them is the data loss. This situation is frequent and creates many problems especially if we does not have backups. Even having them, it is not always sure that all the information could be recovered. Other of the most harmful problems is the sensitive and confidential information theft. Release the customers and goods information of a company can result in huge demands. In the case of a normal person, the email password theft can be dangerous taking into account that the email is used by most of the people to swap their personal information with others. There is not a 100% safe computer nor a red. It is not necessary set up a home computer in the same level of a company computer which has all employee's information.

Therefore, it is important understand and know that "IT Security" is the implementation of standards, policies, procedures, instructions and tools created to preserve the information's integrity, confidentiality and availability; giving to the concept properties such as authenticity, accountability, reliability and non-repudiation. The previous ensures that all the information systems and the information on it are used under the company terms and conditions and just the authorised people can access and modify it.

Resumen - Hoy en día, existen personas con malas intenciones -y que diariamente va en aumento- las cuales pretenden acceder a la información que mantenemos en nuestros computadores y a los sistemas informáticos de las empresas sin ser autorizados. Una de las posibles consecuencias de ser víctima de una intrusión, es la pérdida de datos. Este hecho es frecuente y ocasiona muchos problemas, sobre todo si no contamos con copias de respaldo. Y aun así contemos con dichas copias, no siempre se puede lograr recuperar la totalidad de los datos. Otro de los problemas más dañinos es el robo de información sensible y confidencial. La divulgación de la información que posee una empresa sobre sus clientes o sus activos puede acarrear demandas millonarias. En el caso de una persona normal, el robo de la contraseña de la cuenta de correo puede ser riesgoso debido a que por allí, la mayoría de las personas intercambiamos información importante con otros. No hay un pc 100% seguro ni tampoco una red. No es necesario tener configurado el mismo nivel de seguridad en un computador de hogar como en un computador de una empresa y que maneje la información de los empleados.

Por lo tanto, es importante entender y saber que "Seguridad Informática" es la implementación de

un conjunto de normas, medidas, procedimientos, instrucciones y herramientas, destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información y logrando darle propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. Lo anterior asegura que los sistemas de información y la información contenida allí, se utilizará de la forma como fue acordad y que solamente las personas autorizadas puedan acceder y modificar la información.

***Palabras clave* – Seguridad informática, costos, riesgo, ataques, integridad.**

I. INTRODUCCIÓN

Sin ir muy atrás, hace un poco menos de una década, era un poco extraño escuchar palabras o frases como "Intruso", "Hacker", "Vulnerabilidad", "Fuga de información", "Fraude electrónico", entre otras. Lo anterior se debe al avance agigantado que ha tenido los sistemas informáticos. Sin ir muy lejos, un teléfono celular era inicialmente un dispositivo que se utilizaba principalmente para realizar llamadas, guardar un número limitado de contactos, almacenar un par de notas cortas y precisas, y poder en un momento dado tener un momento de distracción jugando uno de los pocos juegos "sencillos" que tenía el aparato celular en su momento. Claro está que sin hablar de las pantallas que solo tenían dos colores (verde y negro ó gris y negro) y de los teclados iluminados que para poder escribir una palabra, era necesario oprimir una misma tecla varias veces.

En fin, todo en esta vida va evolucionando y como lo decía al comienzo, los sistemas no se quedaron atrás. El tema de la seguridad informática hoy en día nos afecta a todos. En la actualidad estamos rodeados de muchas "facilidades" que nos brindan las comunicaciones y la tecnología, enfocados únicamente en la información.

En este artículo quiero dar alcance a las empresas y la poca atención que le están prestando al tema de la seguridad informática, poniendo en peligro sus activos, su capital y en sí la empresa misma al no implementar el mínimo nivel de seguridad y descargando toda la responsabilidad en una fresa ya muy utilizada por todos nosotros como es: "Eso no me va a pasar a mí".

II. ES UNA RESPONSABILIDAD DE TODA EMPRESA

Empecemos por entender algunos conceptos que son muy importantes conocer y que en el transcurso del documento vamos a estar utilizando. Inicialmente, entendamos que el dato es "una representación simbólica (numérica, alfabética, algorítmica, entre otros.), un atributo o característica de una entidad. Los datos describen hechos empíricos, sucesos y entidades."[1], cabe anotar que los datos solos no ofrecen información entendible para el ser humano y no tienen valor semántico.

Entiéndase por información como "un conjunto de datos acerca de algún suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo."[2].

Uniendo los dos conceptos y dando una relación entre ellos, se puede concluir que el dato o los datos al ser procesados se convierten en información.

Figura. 1 Ilustración del procesamiento de datos.[3]

Por otra parte, un concepto para tener en cuenta es *Tecnología de la información* (TI), que es "la utilización de tecnología – específicamente computadoras y ordenadores electrónicos - para el manejo y procesamiento de información – concretamente la captura, transformación, almacenamiento, protección, y recuperación de datos e información."[4].

Actualmente las empresas (sin importar su tamaño), requieren contar con un área de informática la cual brinde soporte a los computadores y aplicativos que tiene la compañía. Pero no es solo eso, el área de TI debe conocer a qué tipo de ataques puede estar expuesto. Entre los más comunes tenemos:

Ataques Denegación del Servicio, en sus siglas en inglés (Denial of Service)[5]. Su fin es atacar a un sistema en particular haciendo que un servicio o recurso sea inaccesible provocando pérdida de conectividad ya que el consumo de ancho de banda de la víctima es llevado al tope de su capacidad y sobrecargando los recursos computacionales como CPU, memoria o cuotas del sistema. El inconveniente está en que este tipo de ataque no es fácil de evitar ya que las peticiones son realizadas por terminales "sanas" pero en cantidades exponenciales en un periodo de tiempo específico.

Ataques de suplantación. (Spoofing)[6]. Como su nombre lo indica, consiste en utilizar técnicas de suplantación de identidad con fines maliciosos o de investigación, generalmente.

El atacante busca conseguir información de diferentes equipos tecnológicos que sean su objetivo y de esta forma pretenden hacerse pasar por una persona en nombre de otra. En otras palabras, se pretende hacer creer a la víctima que está ingresando a un sitio específico en Internet siendo que en realidad está accediendo a otro sitio de donde pueden estar obteniendo información valiosa del computador o la red de la víctima.

Ataques de Fuerza Bruta. Este ataque es una técnica enfocada a criptografía y permite probar todas las combinaciones posibles hasta poder encontrar el texto legible que fue cifrado para obtener el criptograma.[7] Entiéndase por criptografía como el arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo. Criptograma significa documento escrito en clave.

Los ataques de fuerza bruta suelen ser combinados con *ataques de diccionario* los cuales son un método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario. Este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta, ya que muchos usuarios suelen utilizar una palabra existente en su lengua como contraseña para que la clave sea fácil de recordar, lo cual no es una práctica recomendable.[8]

Ataques Dirigidos a Datos. Estos tipos de ataques son los más conocidos por los usuarios y son programas que se desarrollan con el fin de dañar un equipo de cómputo o a un sistema de información. Dichos programas son los virus, los gusanos y los troyanos, los cuales manejan por lo general código JavaScript. Para ejecutar su ataque, estos programas tiene la capacidad de permanecer ocultos y no ser percibidos por el usuario, logrando así poder causar daño al equipo donde reside y/o sustraer información valiosa.

Ataques de Ingeniería Social. Es una práctica muy usual actualmente en la que el atacante manipula y convence a la víctima para que, por medio de una llamada telefónica, un correo electrónico o por Internet, suministre información

confidencial como contraseñas o configuraciones que son utilidad al atacante para cumplir con su objetivo.

El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente.

Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas cadenas, llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, -por ejemplo proporcionando detalles financieros a un aparente funcionario de un banco- en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.[9]

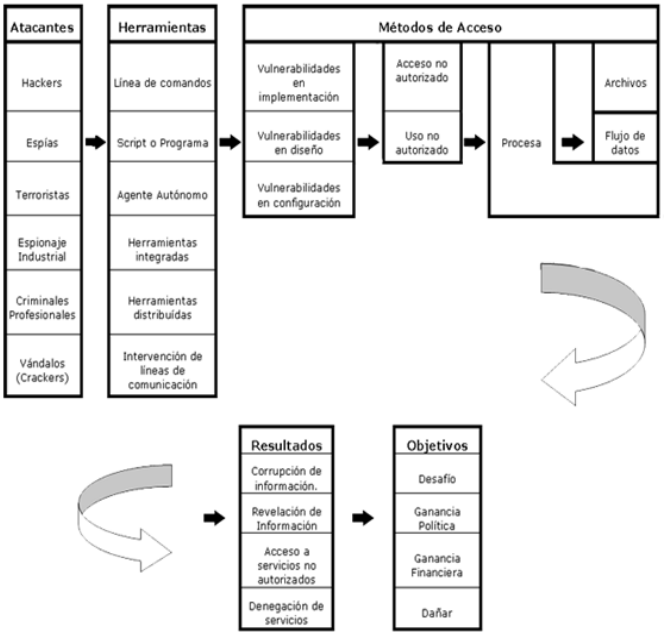

Figura 2. Esquema general de ataque informático.[10]

III. CRITERIOS DE SEGURIDAD

Como ya lo hemos mencionado anteriormente, lo que debe buscar toda empresa es proteger y conservar su información. Hoy en día la información ha tomado tanta importancia y valor que se podría decir que quien tenga la información, tiene el poder y el control. Por lo anterior, es de gran importancia conocer y tener en cuenta los siguientes criterios de seguridad, que son los pilares de la seguridad de la información y que aplicados, puede llegar a salvaguardar la información a "gran escala".

- **Confidencialidad**. Es una propiedad de la información mediante la cual se garantizará el acceso a la misma solo por parte de las personas que estén autorizadas. Es de alguna manera lo que se dice o hace en confianza y con seguridad recíproca entre dos o más individuos. Lo anterior implica que la información clasificada como confidencial no puede ser distribuida, ni publicada ni ser transferida a terceros. Por lo cual se postula a hacer la información más codiciada por la competencia.[11]

- **Integridad**. Es una cualidad de la información la cual indica que la información no ha sido borrada, copiada o modificada, desde su origen hacia su destino. Uno de los mecanismos más utilizados para asegurar la integridad de la información es a través de la firma digital.

- **Disponibilidad**. Este concepto se utiliza en diversos ámbitos y esferas para hacer referencia a la posibilidad de que un servicio, producto o activo, esté disponible de ser utilizado. La disponibilidad significa que ese servicio, está disponible para ser

usado en cualquier momento o cuando el usuario lo requiera.

- **No repudio**. Es la capacidad de afirmar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o creación. Entre sus principales características está comprobar la creación y origen de los contenidos y poseer documentos que acrediten el envío o recepción de mensajes, entre otros.

Figura 3. Pilares de la seguridad de la información.[12]

IV. MECANISMOS DE SEGURIDAD

Se dice que el mecanismo de seguridad se asemeja a cada uno de los eslabones que componen una cadena. Su nivel de seguridad se mide por la seguridad efectiva que presente su eslabón más débil. A continuación se enumeran los más importantes mecanismos de seguridad que se deben básicamente tener en cuenta en una organización.

Autenticación. Es la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

Normalmente para entrar en un sistema informático se utiliza un nombre de usuario y una contraseña. Pero, Es posible autenticarse de tres maneras diferentes que pueden ser combinadas dependiendo la infraestructura con que cuenta la empresa y el nivel de seguridad que se quiera implementar. Estas son:

- Por lo que uno sabe (una contraseña)
- Por lo que uno tiene (una tarjeta magnética o token)
- Por lo que uno es (las huellas digitales o su usuario de red)

La contraseña será mejor o peor dependiendo de las características de la contraseña. En la medida que la contraseña sea más grande y compleja para ser adivinada, más difícil será burlar esta técnica. La contraseña debe ser confidencial. Para que la contraseña sea difícil de adivinar debe tener un conjunto de caracteres amplio y variado (con minúsculas, mayúsculas y números).[13]

Autorización. Es el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización. El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización. Es necesario que dicha autorización siempre quede registrada para ser controlada posteriormente. En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos. Por otra parte, solo se debe dar autorización a acceder a un recurso a aquellos usuarios que lo necesiten para hacer su trabajo, y si no se le negará.

Administración. Es la que establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema. Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema. La administración de la seguridad informática dentro

de la organización es una tarea en continuo cambio y evolución ya que las tecnologías utilizadas cambian muy rápidamente y con ellas los riesgos. Normalmente todos los sistemas operativos que se precian disponen de módulos específicos de administración de seguridad. Y también existe software externo y específico que se puede utilizar en cada situación.

Auditoria. Es la continua vigilancia de los servicios en producción y para ello se revisa información y se analiza. Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización. Pero auditar no tiene sentido sino va acompañado de un estudio posterior en el que se analice la información revisada. Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos, y con una periodicidad que dependerá de lo crítica que sea la información protegida y del nivel de riesgo.

Mantenimiento. Es el conjunto de procedimientos establecidos por la empresa para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada. Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos están: uso de antivirus, encriptación y funciones 'hash'.

V. COSTOS Vs NO IMPLEMENTAR SEGURIDAD

Los costos en los que incurre una empresa deben son por lo general en proporción a los riesgos de pérdidas a las cuales se ve enfrentada.

No es fácil ponerle valor a la información debido a su intangibilidad y todas las medidas de seguridad que se relacionen con su entorno, no afectan la productividad del sistema y es por esto que la alta gerencia es reacia a invertir dinero a este rubro. La forma más sencilla de tratar este tema es cuantificando los daños que pueden causar cada una de las vulnerabilidades que tiene la empresa en caso de que ocurran.

Los costos se pueden clasificar en seis grandes grupos que son:

- Costos de personal
- Costos tecnológicos
- Costos ocultos
- Costos de cumplimiento a la legalidad
- Costos de cumplimiento de políticas y normativas
- Costos en seguros[14]

Punto de equilibrio. Una vez evaluados los riesgos y los costos en los que se está dispuesto a incurrir y decidido el nivel de seguridad a adoptar, podrá obtenerse un punto de equilibrio entre estas magnitudes: Costo / Seguridad / Riesgo.[15]

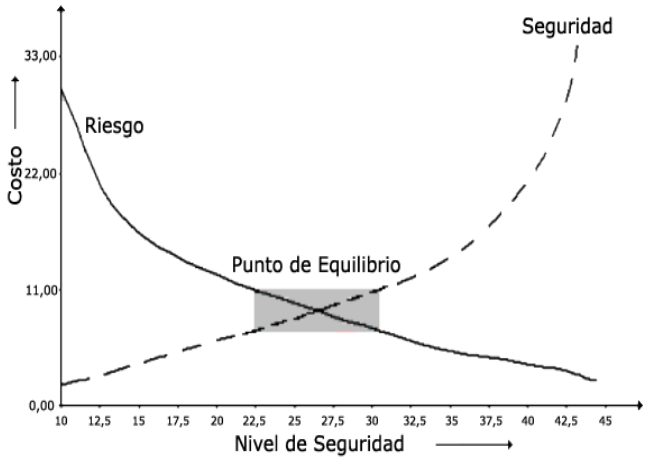

Figura 4. Gráfico punto de equilibrio.[16]

Como puede apreciarse los riesgos disminuyen al aumentar la seguridad (y los costos en los que incurre) pero como ya se sabe los costos tenderán al infinito sin lograr el 100% de seguridad y por supuesto nunca se logrará no correr algún tipo de riesgo. Lo importante es lograr conocer cuan

seguro se estará conociendo los costos y los riesgos que se corren (Punto de Equilibrio).

VI. CONCLUSIONES

Con lo expuesto anteriormente se pretende que el lector logre tener una visión y un conocimiento general sobre lo que es la seguridad informática a nivel de tecnología, buenas prácticas y costos.

No implementar seguridad en la empresa es asumir un riesgo muy alto teniendo en cuenta todo lo que se ha hablado anteriormente. Esperar a que llegue a suceder algo y luego tratar de recuperarse sin tener algún soporte o mecanismo establecido, podrá muy seguramente generar gastos económicos incalculables que no es concebible que una compañía asuma de forma consiente. La seguridad debe ser un tema que forme parte de toda la compañía sin importar su área, funciones o responsabilidades.

Mantener una plataforma de seguridad informática no es fácil y es algo que periódicamente requiere ser analizado, actualizado y monitoreado para lograr mantener un nivel "controlado" ya que nadie ni nada puede asegurar el 100% de seguridad.

Es importante que la empresa involucre a todo su personal en el tema de la seguridad por medio de capacitaciones, avisos, concursos, campañas de tal forma que todos se vean comprometidos y apliquen siempre lo aprendido.

REFERENCIAS

[1] (2014) Sitio web Bligoo.com. Disponible: http://alfabetizacioninformatica-computacional.bligoo.com.ar/concepto-de-datos-informacion-informatica-telematica-ofimactica-burocratica-domotica-orgware#.U88Sd7FnaSo

[2] (2014) Sitio web Promonegocios.net. Disponible: http://www.promonegocios.net/mercadotecnia/que-es-informacion.html

[3] Figura. 1 Ilustración del procesamiento de datos. http://bricogeek.es/dato-proceso-e-informacion/

[4] (2001-2014) Sitio web Degerencia.com. Disponible: http://www.degerencia.com/tema/tecnologia_de_informacion

[5] , [6], [7] (2014) Sitio web Kiokea.net. Disponible: http://es.kioskea.net/contents/22-ataque-por-denegacion-de-servicio

[8] Sitio web Redinfocol.org disponible: http://www.redinfocol.org/atacando-por-fuerza-bruta-bruteforce-1/

[9] (2014) Sitio web wikipedia.org Disponible: http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)

[10] Figura 2. Esquema general de ataque informático. http://bienvenidos-comunicaciones.blogspot.com/2012/04/ataques-informaticos.html

[11] Sitio web Definicionabc.com Disponible: http://www.definicionabc.com

[12] Figura 3. Pilares de la seguridad de la información. http://www.inteco.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/preocupas_seguridad_informacion_empresa

[13] Sitio web recursostic.educacion.es Disponible: http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

[14] Sitio web dma.eui.upm.es Disponible: http://www.dma.eui.upm.es/conferencias/contenido/seguridad_infor.pdf

[15], [16] Sitio web segu-info.com.ar Disponible: http://www.seguinfo.com.ar/politicas/costos.htm