PROTEGER LA INFORMACIÓN “RETO O UTOPIA”

Angel Alberto Varon Quimbayo

“Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores”

-- Kevin Mitnick

En ocasiones creemos que proteger la información puede ser una utopía, pero en realidad lo que debemos plantear es como llegar a conservar y mantener la información de forma segura donde su integridad no se vea afectada y se preserve su estructura lógica, donde únicamente puedan tener acceso a ella las personas autorizadas o los propietarios de la misma, sin embargo; el tema se complica socialmente, con el avance de internet, la aparición de las redes sociales y otras tendencias tecnológicas, ya que la mayoría de individuos no somos cautelosos cuando nos sumergimos en el mundo del ciberespacio, publicamos información personal, laboral y en ocasiones confidencial, que ha servido para que algunos malhechores saquen ventaja para cometer delitos tales como divulgación indebida de contenidos, pornografía infantil y suplantación de identidad entre otros, ultrajando el buen nombre de muchas personas y organizaciones.

Por ello es importante que toda organización cuente con herramientas que permitan monitorear y evaluar los riesgos a los cuales la información está expuesta, ya que es un recurso que como el resto de los activos, tiene valor para la sociedad y las empresas, por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión de los recursos tecnológicos.

Para que estos principios de Política de Seguridad de la Información sean efectivos, resulta necesaria la implementación de mecanismos que permitan mantener la Información de forma segura, además; es necesario que esta estrategia forme parte de la cultura organizacional, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolida-

ción y cumplimiento.

Como consecuencia de lo expuesto, se debe abocar a la tarea de implementar sus propios protocolos de seguridad, basándose en las características establecidas por los estándares internacionales, así mismo, con el propósito de que dicha implementación pueda realizarse en forma ordenada y gradual, se recomienda que cada organización tenga un Comité de Seguridad de la Información, que tenga como tarea elaborar y coordinar la ejecución de un Plan de Acción que permita tomar las medidas pertinentes.

Esto hace que la organización le apueste a tener en su nómina grandes asesores como lo son CEO y CIO.
Donde El CEO como mayor autoridad administrativa de la empresa tiene que velar por la ejecución de la estrategia y ver que se cumplan los objetivos de la organización, siendo el responsable final del desempeño, eficiencia y acciones de la empresa, mientras que el CIO gerente informático sea el encargado de la seguridad de la información, conocedor de mecanismos y procesos que le permitan hacer una planificación para la ejecución de los recursos tecnológicos, que le permitan lograr los objetivos planteados, como la administración de la información, para controlar, medir el cumplimiento de los planes y tomar medidas correctivas en casos necesarios, como el de administrar el riesgo relacionado con la perdida de información, evitando que se convierta en blanco fácil para maleantes o ciberdelincuentes conocidos como cracker, que se encargan de escudriñar todo tipo de datos con el único objeto de alterar, modificar y borrar información con el fin de obtener beneficios de dicha alteración.

Cada día esta tarea se le facilita más a la delincuencia debido a la constante evolución de las tecnologías de la información y las comunicaciones como el caso de internet, que con nuevas tendencias obliga a los mercados a optar por nuevas arquitecturas en la red, como el caso de cloud computing, conocida como computación en la nube, que hace que se convierta en un paradigma, y que permite ofrecer infinidad de servicios por medio de la red de redes más grande del mundo, por donde circulan millones de bytes de información, algo muy similar ocurre con computación grid que permite la integración y uso colectivo de ordenadores de alto rendimiento, redes y bases de datos administradas por diferentes instituciones, el constante crecimiento del comercio electrónico, que también; se fortalece alcanzando un volumen acelerado donde también fluyen grandes masas de datos, que permiten que la información se convierta en insumo relevante para la producción y comercialización de vital importancia para las empresas, pero a su vez permite que existan infinidad de riesgos.

Sin embargo, mientras las organizaciones adopten políticas y la nube traiga su propio dispositivo (BYOD) que es una tecnología integral para diseñar gestionar y controlar el acceso propio a dispositivos de red, estas tecnologías deben asegurarse de que las pólizas forenses cubran respuestas a incidentes digitales, incluyendo otras tecnologías emergentes lo que implica adicionar un mecanismo adicional de seguridad, además; los profesionales de las TI también deben de participar en sus equipos de trabajo como consultores legales o consejeros, para que las políticas realmente logren los resultados deseados y a su vez cree estrategias para evitar los no deseados.

Cuando el delito de cercenar la información se convirtió en Apología o adulación para ser justificada.

Los cracker en muchas ocasiones han demostrado que el nivel de seguridad de la información se encuentra en entre dicho, ya que han sido capaces de escudriñar bases de datos de entes gubernamentales que se creían invulnerables, como el caso más sonado en los últimos tiempos, el de WikiLeaks y la casa blanca incluyendo otros entes estatales del gobierno de Obama, que desenmascaró la hegemonía política que ejercen sobre algunos países subdesarrollados y el afán de someter a gobiernos y poblaciones por medio de espionaje, saboteando, manoseando y vulnerando la integridad y el respeto de sus homólogos, que sin lugar a dudas se convierte en un caso de apología que lo justifican con una breve disculpa a través de los medios de comunicación por parte del presidente Obama ya que él es líder del imperio Yankee.

Todo esto se dio a conocer debido a que Julian Assange (Fundador de Wikileaks), que recibe la información generalmente por medio de la web, mediante el uso de mensajes encriptados y filtrados por personas interesadas en que estos casos salgan a la luz pública, otro caso bastante sonado es el del espía norteamericano y ex agente de la CIA Edward Snouden, que destapó los masivos programas de espionaje del Gobierno Estadounidense, publicado por el semanario Alemán Der Spiegel que hizo la siguiente publicación: La Agencia Nacional de Seguridad (NSA) de EEUU capta información de transacciones bancarias y pagos con tarjetas de crédito de todo el mundo, además; remite documentos del ex analista de la CIA Edward Snowden, que según la fuente el espionaje americano había creado un banco de datos para este cometido, concentrado en el flujo de información de todo tipo de operaciones, ya sea a través de bancos o de tarjetas, especialmente las Visa.

Casos como el del DAS en Colombia que manejaba un archivo detallado con la vida de los magistrados de la corte suprema de justicia donde llevaban notas con las posibles debilidades de cada uno de ellos, con expedientes similares a los que se llevan para las organizaciones criminales, según informes adelantados por la fiscalía general de la nación en el interior de la policía secreta luego de que estallara el escándalo de las chuzadas, se determina que uno de los investigadores del D.A.S identificado como Fabián Eliecer Gaitán Arias, adscrito a la subdirección de contra inteligencia, tenía en su lugar de trabajo las hojas de vida con algunas anotaciones de algunos magistrados de la corte suprema de justicia, este es otro caso que sin lugar a dudas ira a sumarse a miles de casos de impunidad.

Contexto de los Delitos Informáticos

La ingeniería Social se ha convertido en una de las tendencias más apetecidas por los criminales del ciberespacio, ya que se convirtió en la práctica de obtener información confidencial que se enfoca como un arte para manipular personas con el objeto de vulnerar sistemas de seguridad, obteniendo información de los usuarios por medio de teléfono, contacto directo, correo electrónico o correo tradicional, acercándose a las personas de una forma muy persuasiva aprovechándose de la inocencia de los usuarios, esta técnica suele utilizar personajes tales como investigadores privados, criminales o delincuentes que suelen hacerse pasar por compañeros de trabajo, un técnico un administrador, con el único objeto de tener información de acceso o privilegios de los sistemas de información, que les permita realizar algún acto para perjudicar y exponer a la persona o a la organización a riesgos inclusive a abusos.

Estos son algunos de los delitos informáticos registrados por la policía nacional de Colombia:

Claves programáticas espías: son conocidas como troyanos, o software espías, utilizadas para sustraer información en forma remota y física, preferiblemente aquella que le permita al delincuente validarse en el sistema bancario, suplantando a la víctima.

Estafas a través de subastas en línea: se presentan en el servicio de venta de productos, generalmente ilícitos, en línea o en la red; se pueden encontrar celulares hurtados, software de aplicaciones ilegales, además puede ser una vía de estafa ya que suelen incumplir reglas de envío y de calidad de los productos solicitados.

Divulgación indebida de contenidos: son conductas originadas en el anonimato ofrecido el internet y el acceso público sin control es decir desde ciber cafés; entre ellas se encuentra el envío de correos electrónicos anónimos, con fines injuriosos o calumnias, amenazas y extorsiones.

Pornografía Infantil en Internet: a través de foros, chats, comunidades, virtuales, transferencia de archivos, entre otras modalidades, los delincuentes comercializan material pornográfico que involucra menores de edad.

Violación a los derechos de autor: utilizando reproductores en serie, los delincuentes realizan múltiples copias de obras musicales, video gramas y software.

Piratería en internet: implica la utilización de internet para vender o distribuir programas informáticos, protegidos por las leyes de la propiedad intelectual. Aquí encontramos la utilización de tecnología par a par, correos electrónicos, grupos de noticias, chat por relay de internet, orden postal o sitios de subastas, protocolos de transferencia de archivos, los phishing que son técnicas que hacen que el usuario muerda el anzuelo, utilizan la manipulación del correo electrónico para lograr que en el enlace aparezca una ruta legitima de la organización, por la cual se hace pasar el impostor manipulando las URL un ejemplo es la utilización de páginas bancarias en la cual la vista mostrada en pantalla no corresponde a la dirección real, o la utilización de direcciones que contenga el carácter @ ya que por medio de este pregunta el nombre de usuario y contraseña.

En el mundo virtual los delitos informáticos están aumentando, en el 2009 fueron cerca de 700 casos denunciados, por ejemplo los fraudes a través de banca virtual, amenazas, calumnias, injurias por medio de correos electrónicos, la pornografía infantil también

es un delito que viene en crecimiento, otro de los delitos informáticos que más se ve en las empresas es la suplantación de Identidad para realizar los fraudes bancarios, donde se identifican desfalcos desde menos de un millón de pesos hasta equivalentes a mil millones de pesos en un solo fraude, sin embargo; no solo a través de la informática forense se puede contrarrestar la delincuencia en internet, en el caso de la pornografía infantil los jóvenes pueden evitar ser víctimas de este delito, alguno de los consejos prácticos es que en las redes sociales solo tengan a personas conocidas, como compañeros de colegio, escuela, grupos de estudio o grupos deportivos, a sus familiares, además; no deben darle la clave a nadie, no publicar fotografías, ni fijar citas con alguien que no se conozca y mucho menos solos, además tratar siempre de proteger la información para no ser víctimas de los ciberdelincuentes.

No debemos olvidar que los criminales en internet pueden ser perseguidos, procesados y analizados, no hay ninguna prueba que se pueda ocultar desde que se cometa el delito en el ciberespacio, solo hay que denunciar a la policía nacional.

En la página www.internetsano.gov.co se han denunciado cerca de 7100 páginas web, que tienen como característica promover la pornografía infantil o promover hechos violentos que atentan contra la integridad de las personas, debido al incremento de estos delitos los investigadores se valen de la computación forense o de informática forense, ya que la policía nacional cuenta con laboratorios modernos en la dirección de investigación criminal, donde se analizan todos los dispositivos de tipo digital como discos duros, Sim card, memorias USB, entre otros.

Algunos mecanismos de defensa contra los delitos informáticos.

Computación Forense

Se entiende como la ciencia de la aplicación de técnicas científicas que permiten la identificación, recopilación, exámenes y análisis de datos, mientras que la preservación de la integridad de la información y el mantenimiento de una estricta cadena de custodia de los datos que hacen parte de un proceso legal, la meta del análisis forense es obtener una mejor comprensión de un evento de interés por la búsqueda y el análisis de los hechos relacionados con ese evento forense, pueden ser necesarios en muchas situaciones diferentes, tales como la recopilación de pruebas para los procedimientos judiciales y las acciones disciplinarias internas, y el manejo de incidentes de malware y problemas operativos inusuales (Kent, Chevalier, Grance y Dang, 2006).

De acuerdo con la guía NIST de la Orientación Autenticación Electrónica, la autenticación es un proceso de establecimiento de la confianza en la identidad de los usuarios o sistemas de información.

El protocolo de autenticación es una secuencia definida de mensajes entre un demandante y un verificador, que demuestra que la demanda

tiene posesión y el control de un token válido para establecer su identidad, y opcionalmente, demuestra a la demanda de que él o ella se está comunicando con el verificador previsto. El proceso de autorización es diferente del proceso de autenticación. Con la autenticación, el sistema de prueba que usted es quien dice ser. Sin embargo, con la autorización, el sistema verifica que tiene derecho a hacer lo que se quiere hacer.

La Esteganografía

Es conocida como el arte y la ciencia de ocultar información, es una de las ramas de la criptologia cuya presencia no puede ser detectada. Esta técnica consiste en el ocultamiento de información, dentro de un archivo gráfico, de audio o video, inclusive algunos programas permiten ocultar otros tipos de archivos, ficheros PDF, el texto puede ser manipulado en el tamaño de letra, espaciado, tipo y otras características para ocultar un mensaje, asegurados con una clave de acceso conocida por la persona que creo el archivo, quien será el encargado de hacerla saber a quién tenga que descubrir el contenido,

La esteganografía ha evolucionado con la aparición de los computadores, para estos propósitos no sólo podemos incluir un mensaje, también podemos cifrar su contenido de forma sencilla. Con esto conseguimos dos mecanismos de seguridad. Por un lado ocultamos la existencia del mensaje y por otro, en caso de ser descubiertos, el cifrado complicará su lectura en función del algoritmo empleado y la complejidad de la clave utilizada. La esteganografía es razonablemente segura para intercambiar información en la red, ya que oculta el mensaje en los bits menos significativos, ahora no es necesario incluir en el “punto” de una “i” un microfilm, como llegó a hacerse.

Un mensaje original inalterado se llama “texto cubierto” el emisor trata de ocultar un mensaje agregado, transformando el texto cubierto utilizando una clave secreta, el mensaje resultante se llama “estegotexto” y es enviado al receptor. Similar a la criptografía, asume que el adversario tiene completo conocimiento sobre el sistema excepto por la clave secreta que comparten receptor y emisor, que garantizan la seguridad.

Casos donde se utilizó esteganografía

- Durante la segunda guerra mundial, agentes de espionaje usaban micro-puntos para mandar información, los puntos eran extremadamente pequeños comparados con los de una letra de una máquina de escribir, por lo que en un punto se podía incluir todo un mensaje.

- Mensajes escritos en un cinturón enrollado en un bastón, de forma que sólo el diámetro adecuado revela el mensaje.

- Mensajes escritos en el cuero cabelludo, que tras crecer el pelo de nuevo, oculta el mensaje.

Encriptación: la seguridad en la transferencia de información cada día se vuelve más crítica, por lo que las técnicas de encriptación deben de ser más Sofisticadas, lo que obliga a utilizar la encriptación de la información que consiste en volver ilegible la información, utilizando una serie de fórmulas matemáticas y para desencriptar se usan claves como parámetros para esas fórmulas.

Llave murciélago: esta técnica consiste en sustituir las letras del abecedario por las letras de la palabra llave, en este caso murciélagos. Donde la primera letra la m sustituye la a, la letra u sustituye la b y así sucesivamente, después de la letra s colocamos una letra que no aparezca en la letra llave Ejemplo:

E s t u d i a n t e C u n i s t a
f k l b c e M f d b e k l m
murcielagos

Firewall o cortafuegos: es un dispositivo electrónico que hace las veces de policía o guardián y funciona como cortafuego entre redes, ya que se encarga de permitir o denegar transmisiones de una red a otra, la técnica más común es ubicarlo entre una intranet o red local y la red de internet, para evitar que los intrusos tengan acceso a información confidencial, ya que sirve como filtro de comunicación examinando la información entrante o saliente y el tipo de servicio al que corresponde puede ser web, el correo o IRC para permitirlo, un firewall puede ser un dispositivo o un software que se instala en el modem que nos conecta a la web, inclusive hoy día se instalan computadores o servidores con aplicaciones específicas para el monitoreo de redes de comunicaciones.

Los Antivirus: son programas que cuyo objetivo es contrarrestar, prevenir u evitar la activación de los virus, así como el contagio, la propagación de los mismos, estos programas cuenta además; con ciclos o rutinas de detección, eliminación, reconstrucción de archivos y áreas afectadas en el sistema, un buen antivirus debe contar con tres componentes fundamentales, que son los que le permiten cumplir con el objeto por el cual fueron creados.
Vacuna: que es un programa que instalado reside en la memoria y actúa como filtro de los programas cuando son ejecutados, para ser leídos o copiados en tiempo real.

Detector: este programa examina todos los archivos existentes en el disco duro a los que se les indique en una determinada ruta o PATH. Tiene instrucciones de control y reconocimiento exacto de los códigos virales, que permiten capturar sus pares debidamente registrados y de forma acelerada permiten destruir su estructura.

El eliminador como su nombre lo indica, después de destruir la estructura del virus se encarga de eliminarlo inmediatamente y posteriormente se dirige a reparar o reconstruir las áreas y archivos afectados.

Cabe aclarar que un antivirus es un programa informático que sirve como herramienta para el usuario y no es eficaz para el 100% de los casos, y además aclaro que nunca será la protección total y definitiva.

Cabe concluir que uno de los retos es convencer a la clase dirigente de las organizaciones sobre la importancia de invertir para crear una cultura direccionada a fortalecer y a aplicar los mecanismos necesarios para proteger un insumo tan relevante como es la información, además; debemos resaltar la importancia de crear un vínculo directo entre el gerente administrativo y el gerente informático, para que con el direccionamiento de ambos se pueda lograr un fortalecimiento institucional para el logro de sus objetivos, incluyendo la protección de los medios informáticos y el flujo de la información ya que existe el apoyo del estado y una serie de elementos que hace posible que podamos dar un buen paso frente a este flagelo.
Queda abierto el debate si la seguridad de la información es un reto o posiblemente una utopía, ya que debido al gran flujo de información, los ciberdelincuentes han logrado un incremento importante en la cuantificación de delitos, además; es sano resaltar que los entes gubernamentales a nivel mundial son los llamados a dar ejemplo y que no debemos olvidar que por no existe motivo para ser partícipes en estos crímenes y menos justificar la razón de estos con una simple disculpa, ya que es como darle una bofetada a la moral institucional.
También podemos clarificar que existe un alto índice de desconocimiento sobre los mecanismos y delitos que los malhechores pueden ocasionar por medio de la web, la verdad en Colombia existe un sitio web denominado www.internetsano.gov.co pero la verdad es poco visitado debido a que la mayoría de los colombianos desconocen la existencia de estos sitios.