Humanizando la Seguridad de la Información

González Pinzón, Nidia Nayibe. Téllez García, Leonardo
nayibeive@gmail.com,leonardotellez999@gmail.com
Universidad Piloto de Colombia

Abstract **-** This article aims to provide a general approach to the importance of Information security as from the element that we consider to be the most important in the development of Information Security Management System, human beings, who are accountable not only for the success of the system when it comes to its business implementation, but who are also key when it comes to decreasing the rate of Cyber-crime that involves children, teenagers and young people in general.

Resumen—Este artículo pretende dar un enfoque general de la importancia de la Seguridad de la información, desde el elemento que a nuestra consideración es el más importante en el desarrollo de un sistema de gestión de seguridad de la información, el ser humano, de quien no solo depende el éxito del sistema en su implementación empresarial, sino también es la clave para que los delitos informáticos en los que se ven involucrados los niños, adolescentes y jóvenes disminuyan en un gran porcentaje.

ÍNDICE DE TÉRMINOS- INGENIERÍA SOCIAL, BULLYING, CIBERESPIONAJE, PHISHING, CIBERBULLYING, TROLLING ONLINE, PHARMING

I. INTRODUCCIÓN

La seguridad informática ha sido un tema que recientemente ha cobrado importancia, entre otras razones, por escándalos internacionales sobre delitos informáticos como ciberespionaje o violaciones en la web a diferentes organizaciones. Casos como el de Edward Snowden, quien fue el hombre que reveló el espionaje que se le realizaba a miles de ciudadanos de Estados Unidos; usó correos cifrados y varias maniobras para poder mantener privada cierta información.

Colombia no se escapa de escándalos como el de Estados Unidos. Un ejemplo reciente es el del caso de *Buggly Hacker*, negocio fachada de la inteligencia militar para hacer seguimiento a objetivos que representan algún riesgo para la seguridad del Estado, y que salió a los medios de comunicación tras un supuesto desvío de su función, que habría incluido interceptaciones a los negociadores del Gobierno con las Farc.

Una de las prácticas delictivas que más afectan a los internautas es el *phising* destinado a robar los datos e identidad de las personas en internet con fines económicos. Un estudio hecho en febrero de 2013 por EMC, empresa especializada en tecnologías de la información, reveló que se presentaron 27.463 ataques de este tipo.

Si bien las personas son informadas sobre el tema, aún no se ha logrado concientizar a la población de lo importante que es proteger su información personal y privada, lo que permite a los delincuentes lograr sus objetivos delictivos, que cada vez toman mayor fuerza.

II. IMPORTANCIA DE CREAR CULTURA DE SEGURIDAD DE LA INFORMACIÓN

¿Qué es la información?

Con el fin de contextualizar un poco porqué es importante la información presentamos algunas definiciones:

Según Idalberto Chiavenato, **información** *"es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado*

contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones".[i]

Para Ferrell y Hirt, la **información** *"comprende los datos y conocimientos que se usan en la toma de decisiones"*[ii].

En el Diccionario de la Real Academia Española, se encuentran, entre varios significados, los siguientes: *(Del lat. informatĭo, -ōnis). 1. f. Acción y efecto de informar. 2. f. Oficina donde se informa sobre algo. 3. f. Averiguación jurídica y legal de un hecho o delito. 4. f. Pruebas que se hacen de la calidad y circunstancias necesarias en una persona para un empleo u honor. U. m. en pl. 5. f. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada. 6. f. Conocimientos así* comunicados o adquiridos. [6].[iii]

De acuerdo a lo anterior, podemos concluir que la información es un conjunto de datos organizados que brinda conocimiento específico sobre un tema, una persona o un hecho que puede ser comunicado y/o utilizado por quien adquiere este conocimiento.

La información dependiendo del ámbito o tema al que se refiera puede adquirir ciertas características que hacen meritorio un tratamiento particular según sea el caso. Basados nuevamente en la Real Academia de la lengua española citamos algunos ejemplos de los que se pueden denominar tipos de información según su uso:

Información (~ ad perpétuam, o ~ ad perpétuam rei memóriam):1. f. Der. La que se hace judicialmente y a prevención, para que algo conste en lo sucesivo.

Información de dominio: 1. f. Medio supletorio para inscribir el registro de bienes en el de la propiedad cuando se carece de título escrito.

Información de vita et móribus: 1. f. La que se hacía de la vida y costumbres de aquel que había de ser admitido en una comunidad o antes de obtener una dignidad o cargo.

Información en derecho: 1. f. Der. Alegato extraordinario impreso, con el cual, a veces, en apelación civil de mayor cuantía, se sustituyen los informes orales de las partes litigantes.

Información privilegiada: 1. f. La que, por referirse a hechos o circunstancias que otros desconocen, puede generar ventajas a quien dispone de ella. 2. f. Der. En el ámbito de los mercados de valores, aquella a la que se ha tenido acceso reservadamente, con ocasión del desempeño de un cargo o del ejercicio de una actividad empresarial o profesional, y que, por su relevancia para la cotización de los valores, es susceptible de ser utilizada en provecho propio o ajeno.

Fuentes de información: 1. f. pl. Confidencias, declaraciones o documentos que sirven de base para la elaboración de una noticia o reportaje periodístico. 2. f. pl. Personas que emiten esas declaraciones.

Tratamiento de la información: 1. m. Inform. Aplicación sistemática de uno o varios programas sobre un conjunto de datos para utilizar la información que contienen.

Teniendo en cuenta estos conceptos podemos intuir que información como el registro de bienes, la honra y actos de una persona es información privilegiada que solo ciertas personas pueden conocer y por tanto, merece un tratamiento adecuado.

¿Cuándo es importante la Información?

Partiendo de los conceptos anteriormente expuestos se puede afirmar que la importancia de la información es relativa para cada persona porque depende de cuánto altera de manera significativa su propia conducta o la de otros individuos; así, la importancia de la información depende de su significado y de la evaluación de las posibles consecuencias de su divulgación, de tal forma que el sujeto cambia su actitud frente a la protección o custodia de la misma.

Otra característica que pone en relieve la valoración de la importancia de la información es su vigencia

en espacio-tiempo, lo cual es difícil de evaluar, ya que las expectativas actuales frente a la información pueden cambiar con el transcurrir del tiempo y volverse más relevante.

Por otra parte, la validez de la información que es relativa al emisor o fuente permite evaluar si es fiable o no, lo que genera un valor de utilidad para los posibles receptores interesados y por ende da un mayor valor ya sea económico, de reputación o intelectual a la misma.

¿Qué es la Seguridad de la Información?

El concepto de Seguridad de la Información tomado de la NTC-ISO/IEC 27002 es: "La Seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio".

En general encontramos que: "La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma."

Ahora bien, en ambos casos se hace énfasis en la importancia de la información para empresas ya sean públicas o privadas, no se hace referencia alguna sobre la importancia de la información para la persona, olvidando que es quien la genera, la administra, la mantiene y la protege. Si bien es cierto, la información para cualquier empresa tiene un valor económico y de reputación, para el hombre como individuo, la seguridad de la información tiene un efecto de mayor valor en su vida personal.

III. ¿POR QUÉ PROTEGER LA INFORMACIÓN?

Para las empresas la utilización oportuna y eficiente de la información impacta significativamente su productividad económica, por lo que se ha convertido en un recurso estratégico y cobra valor como aspecto vital a la hora de la toma de decisiones por parte de los directivos; por ejemplo el aumento de transacciones por medios electrónicos, que van desde el pago de la nómina, hasta compras por internet y envío de información sensible por correo, determinan la necesidad de proteger la información que viaja en la nube y puede ser "escuchada" por cualquiera si ésta no se encuentra protegida.

Siendo la información de tal importancia para una entidad, se debe saber que ésta, en manos de personas inescrupulosas, pude llegar a causar daños económicos y de reputación que al final siempre serán valorados desde el punto de vista monetario, ya que se pueden llegar a efectuar: fraudes, espionaje comercial, destrucción de información vital para la organización y sus clientes, suplantaciones, entre otros, convirtiéndose de esta forma una estrategia la protección de la información.

Por otra parte las personas naturales no están exentas de ser afectadas por estos delitos, pues normalmente se dirige la atención a las pérdidas económicas que en alguna organización se pueden presentar. Pero *¿qué sucede con las personas del común, cuando entran a formar parte de lo que algunos autores denominan la diplomacia virtual?* Para ello, hay que tener en cuenta que este concepto no es más que la adjudicación de un valor geopolítico a las redes sociales (pueden ser virtuales o no), donde son más importantes las relaciones humanas que se establecen, compartiendo información y generando una identidad y reconocimiento virtual, dando a conocer información, que en muchos casos es sensitiva o intima.

¿Somos conscientes de la cantidad de información que manejamos y damos a conocer?

Es una pregunta que no solo se debe plantear para las organizaciones y sus empleados, que si bien hacen parte de una realidad importante, también aplica para la información personal y familiar se da a conocer con una facilidad aún mayor de la que se tiene conciencia.

La información personal publicada puede abrir espacios para divulgar datos de carácter sensitivo como por ejemplo: orientación sexual y creencias; de igual forma dar a conocer datos de los que no siempre queremos que todo el mundo sepa por ejemplo: saber dónde vive una persona, con quien comparte sus fines de semana, cuántos son los miembros de su familia, a qué se dedican, dónde trabajan y han trabajado. Datos que para personas interesadas en el tráfico de información o simplemente en la búsqueda de una "víctima fácil" les puede ser de gran utilidad ya sea para negociar esta información, para tratar de dañar la reputación de alguien o simplemente para generar un ambiente hostil en torno a su víctima.

"*Si necesitas algo, sólo pídelo. El secreto del éxito de obtenerlo está en la manea de pedirlo" ANÓNIMO*

No necesariamente para cualquiera de los casos (empresarial y personal) la forma de pedir información es directa. El delincuente previamente ha realizado un estudio de su o sus víctimas; en el caso de una organización se puede contar con la mejor infraestructura tecnológica para asegurar que la información no tenga fuga alguna en medios magnéticos o electrónicos, y *¿quién asegura que el empleado tenga clara la importancia de no dejar una clave visible, o de no dejar papeles importantes con información estratégica de la compañía en sitios donde el flujo de personal ajeno a la organización es alto*?. En el caso personal, cuantas veces se han escuchado casos donde las víctimas conocían a sus atacantes e incluso les dejaron pasar el límite de su propia intimidad, en este último ejemplo se han visto involucrados con mayor regularidad los adolescentes e incluso los niños, evidenciando diversos tipos de violencia a través de la tecnología.

En ambos casos se hace necesaria la sensibilización de los adultos que son quienes trabajan en las diferentes organizaciones y que a su vez son los padres de estos adolescentes y niños que pueden caer fácilmente en las redes de personas que dedican sus talentos a desarrollar y/o efectuar los distintos tipos de delitos tecnológicos, como por ejemplo fraudes, estafas, *ciberbullying* o ciberacoso en español entre otros muchos.

IV. DATOS ESTADÍSTICOS Y COSTOS OCASIONADOS POR EL CIBERCRIMEN

Es importante tener en cuenta cómo las personas cada día van aceptando y adoptando cambios en su vida con el uso de las nuevas tecnologías, influyendo con ella las tendencias. Con respecto a este aspecto, por ejemplo, las ventas de computadores en el mundo se han reducido en un 10.9%, mientras que dispositivos como los Smartphone han aumentado en un 46.5%[iv]; ¿por qué sucede algo como esto? El día a día y la necesidad de responder a un mensaje de forma instantánea, la comunicación efectiva y las relaciones generadas en las redes sociales, con personas especiales o grupos afines a los propios gustos, hacen que el uso de un ordenador no sea tan apetecible, mientras los modernos aparatos tecnológicos, de fácil uso y portabilidad permiten el acceso a la información en tiempo real, por ende también una aceptación en una sociedad virtual.

¿Cuánto cuesta a una empresa o a una persona un incidente grave de seguridad?

Alrededor de 500.000 euros es el costo promedio en el que incurren las grandes empresas como consecuencia de un ciberataque, según datos de la Encuesta Global sobre seguridad TI corporativa – 2013, llevada a cabo por B2B Internacional junto a Kaspersky Lab y efectuada a 2.895 profesionales de TI. Estos datos corresponden a incidentes ocurridos en los últimos doce meses e incluyen dos componentes principales:

1- Pérdidas derivadas de la fuga de datos críticos, continuidad de negocio y los costos asociados con la participación de especialistas para solucionar el incidente. Que corresponden alrededor de 431.000 euros.

2- Costos no planificados, con el fin de prevenir futuros ataques similares, esto incluye el personal de contratación y formación, el

hardware, el software y otros cambios de infraestructura que suponen unos 69.000 euros.

Los daños mayores se asocian con incidentes sufridos en empresas que operan en América del Norte, con un promedio de 624.000 euros, seguido de América del Sur, con 620.000 euros. Europa Occidental registró una media más baja, pero aún considerable, de las pérdidas derivadas de ciberataques, llegando a 478.000 euros.

Symantec en su 'Reporte Norton 2013'[v] destaca los principales datos sobre el estado del cibercrimen en el mundo. Los hallazgos para Colombia son:

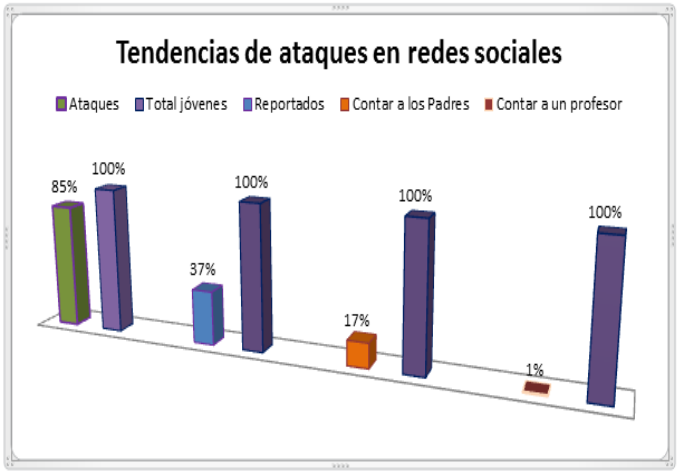
- El 64% de los usuarios adultos ha experimentado algún crimen cibernético
- El 64% de los colombianos usa sus dispositivos móviles para trabajar
- En los últimos 12 meses el costo total del crimen cibernético en el país fue de 873.466 millones de pesos
- En el último año, 6 millones de personas han sido víctimas de cibercrimen
- El 42% de los usuarios de smartphones ha experimentado algún delito cibernético en los últimos 12 meses

Si bien se muestra una tendencia a la masificación del uso de dispositivos móviles, los conocimientos de seguridad de parte de los usuarios son pocos, teniendo en cuenta que, casi la mitad de los encuestados no toman las precauciones de seguridad necesarias como el uso de contraseñas, software de protección o respaldo de los datos.

Por otro lado, el costo del cibercrimen aumentó en un 43%, aunque el número total de víctimas disminuyó en relación al 2012 debido a que las empresas no toman las medidas necesarias para blindarse frente a los delincuentes. Por ejemplo, las empresas colombianas están perdiendo cerca de 40 millones de dólares por estos delitos 2.0 y esto no quiere decir solo invertir en tecnología, sino en sensibilización de sus propios empleados sobre el tema.

En cuanto a los abusos en las redes sociales, los adolescentes sufren en silencio siendo tan solo una tercera parte de ellos quienes se atreven a informar algún abuso como lo muestra una encuesta sobre adolescentes realizada por Knowthenet llamada Trolled Nation[vi]. El 85% de los jóvenes dijeron haber tenido alguna experiencia de bullying o trolling online pero solo el 37% de ellos lo ha reportado alguna vez en las redes sociales.

Si bien, según datos de la encuesta 2 de cada 3 adolescentes han experimentado *bullying* o *trolling*, casi ninguno recurriría a los padres (17%) o a los profesores (1%) para buscar apoyo como primera reacción, sin embargo, no se trata sólo de no haber confiado en un adulto lo que es preocupante; sino que más de la tercera parte decidieron no denunciar el incidente porque pensaron que no se iban a tomar medidas.



Fuente el autor

En la encuesta se revela otros sitios que también son foros populares para este tipo de delito: 19% Twitter, 13% BBM (BlackBerry Messenger), 9% Ask.fm, 8% Bebo, 4% Whatsapp.

En Colombia según un estudio realizado a 180 estudiantes, entre los 12 y 18 años por la universidad de la Sabana el 68% de los adolescentes se conectan a internet para socializar con sus pares y un 85% reporta haber sido testigo de un caso de intimidación virtual y temen ser víctimas de burlas, críticas, situaciones de inseguridad, chismes y pornografía. El Coronel Fredy Bautista García, jefe del Centro Cibernético de la Policía Nacional afirmo al diario EL UNIVERSAL que no es de extrañar que los adolescentes no reconozcan esta

problemática como propia porque temen ser cuestionados o simplemente tienen vergüenza.
Dentro de los costos para las personas nos permitimos referenciar dos casos publicados recientemente en un artículo del diario EL UNIVERSAL[vii]:

1- Experiencia vivida por una joven que en la actualidad tiene 20 años y afirmó que a los "16 años fue acosada por un desconocido a quien había aceptado como amigo, que le comentaba en su chat lo linda que estaba, cómo iba vestida, a qué horas salía de su casa. Lo que al principio recibió como un halago se le fue convirtiendo en pesadilla porque el delincuente la empezó a chantajear: le decía que tenía fotos de su perfil, que podía hacer montajes con estas para hacerla aparecer como "la más perra" sino hacía lo que le pedía: que se desnudara para él. La joven sospechó de un adulto al que veía merodeando por su casa y su colegio.

   Ella lo bloqueó, pero no lo denunció porque para ella no habían pruebas que la pudiesen ayudar".

2- "Otra chica también de 16 años, conoció a través de Facebook, a un supuesto joven de su misma edad, con quien, luego de tres meses de comunicaciones, se puso de acuerdo para conocerse personalmente en un concurrido centro comercial a una hora también muy concurrida.

   La joven, al parecer, al llegar al centro comercial fue drogada y terminó en Chile, siendo víctima del tráfico de personas (trata de blancas). En una ocasión, como pudo, escapó de sus captores y pudo llamar a su mamá y decirle en qué lugar se encontraba. Con la ayuda de las autoridades lograron localizarla. Hoy, ella y toda la familia viven fuera de Colombia".

V. BENEFICIOS DE CREAR CULTURA DE LA SEGURIDAD

Según informe de Norton al menos el 77% de los colombianos ha sido víctima de un delito informático y 50% de los usuarios ha sido víctima de delitos informáticos en las redes sociales. Si se crea una cultura de la seguridad donde los cibernautas reflexionen sobre sus prácticas en internet, desde el uso, cambios de contraseña, información publicada y compartida, hasta la navegación en sitios seguros estos porcentajes disminuirían en forma considerable.

Si los usuarios utilizaran contraseñas complejas y las cambiaran con frecuencia, si verificaran que el explorador tenga el símbolo de candado antes de ingresar información personal, se reduciría en al menos un 26% de usuarios afectados.

Es interesante ver cuánto invierten las compañías en seguridad. Como se mencionó anteriormente pueden llegar a un costo no planificado de unos 69.000 euros. Ahora bien, si se logra tener una cultura de seguridad se pueden evitar fraudes del tipo *phishing* o *pharming* el costo se reduciría a 45.700 euros aproximadamente.

A pesar que algunos usuarios toman precauciones básicas como borrar correos electrónicos sospechosos y no publicar contenido personal en sus redes sociales; la mayoría, en especial los adolescentes no toman las medidas necesarias para evitar ser víctima de cualquier tipo de delito informático.

Es importante invertir en tecnología que cubra o proteja la información, solo que esta inversión no sirve de nada si el usuario final, ya sea desde su puesto de trabajo o en su propia casa continúa exponiendo la información. Esto incluye el manejo de los nuevos dispositivos móviles donde se encuentran configuradas las cuentas personales y las del trabajo, que ocasionalmente son usados por sus

hijos adolescentes para conectarse a redes sociales o simplemente descargar un juego online.
A continuación presentamos los riesgos de ataques minimizados al tener presentes buenas prácticas como:

- ***Verificar la información recibida***. Ayuda a minimizar el riesgo de virus ocultos que en algunos casos estos pueden redireccionar a páginas no seguras.

- ***Tener un adecuado cuidado con las contraseñas y claves*** pues pueden ser reveladas en sitios no oficiales y a personas no autorizadas.
- ***Verificar el sitio web***, en este caso que la barra de dirección tenga un candado, asegura que la información que se suministre tendrá el tratamiento estipulado en el contrato establecido con la entidad bancaria acordado por la ley.

- ***Una buena comunicación con los miembros de la familia***, puede prevenir el hecho de ser víctimas de *bullying*, y en caso dado de ser víctimas de esto, ayuda a tomar las medidas necesarias para frenar los ataques.

Evadir la configuración de privacidad de redes sociales como *Facebook, Twitter, Instagram* o la cámara de *smartphones* con sistema *android* puede hacer que las personas sean víctimas, de robos o secuestros.

El mundo globalizado presenta un sinfín de herramientas y puertas abiertas para el acceso a la información, y son las personas las que permiten que esa información circule o continúe circulando en la red. Si como individuos nos alejamos de nuestra responsabilidad frente a la divulgación de información y la depositamos solo en la tecnología (software y hardware) nos veremos envueltos en crímenes que en el peor de los casos ni siquiera somos capaces de denunciar, permitiendo así la impunidad y el crecimiento delincuencial, que día a día se transforma.

VI. ¿CÓMO SENSIBILIZAR EN SEGURIDAD DE LA INFORMACIÓN A LAS PERSONAS?

Formas de aprendizaje

Es importante analizar las formas de aprendizaje del ser humano, así como el contraste del enfoque didáctico utilizado para brindar conocimiento, las herramientas de aprendizaje y su aplicación en la sensibilización de un tema como el de la seguridad de la información, las evaluaciones alternativas, la utilización de estrategias didácticas y la búsqueda de apoyos y materiales diseñados a partir del enfoque del aprendizaje; sin dejar de analizar la efectividad de los métodos para alcanzar aprendizaje de alto nivel en las personas con el fin de ayudar al desarrollo del ser humano.

Cuando las personas desean aprender algo utilizan su propio método o conjunto de estrategias y habilidades para procesar, aprender y entender la información. Para lo cual como individuos usamos y nos apoyamos en diferentes factores que intervienen en cada uno de nosotros, los cuales se pueden agrupar de acuerdo a nuestras semejanzas: la edad, el género, el idioma, la cultura, la religión, los valores, la situación socio-económica, la situación geográfica, entre otros; y las diferencias: el desarrollo o formación del sujeto, el flujo de las emociones, la creatividad, la intuición, los mecanismos de interacción, los patrones de organización, la reflexión y la motivación.

Al combinar y analizar estas diferencias y semejanzas se pueden evidenciar diferentes métodos de aprendizaje, así como, las modalidades sensoriales de cada uno de los individuos:

Los individuos visuales: los cuales aprenden mirando. Ellos van a imágenes del pasado cuando tratan de recordar y además dibujan la forma de las cosas en su mente.

Los individuos auditivos: que tienden a deletrear fonéticamente (sonidos.) Estas personas aprenden escuchando y recuerdan los hechos cuando éstos son presentados en forma de poemas, cantos o melodías.

Los individuos kinestésicos o manipuladores: (que tocan las cosas) aprenden mejor moviendo, experimentando y manipulando. Les gusta descubrir cómo funcionan las cosas y muchas veces son exitosos en artes prácticas como carpintería o diseño.

Este concepto de los métodos de aprendizaje está directamente relacionado con la concepción del aprendizaje como un proceso activo; refleja la forma que respondemos al ambiente, a los estímulos sociales, emocionales y físicos, para entender la nueva información de tal manera, que cada individuo centra el aprendizaje en sus fortalezas y no en sus debilidades.
Es importante resaltar que un individuo puede desarrollar más de un estilo de aprendizaje diferente, esto se puede dar con base en sus habilidades, estrategias, disposición y preferencia.

Hay que recordar que la estructura de la enseñanza sigue siendo la del aprendizaje memorístico, es decir, la teoría del conductismo, que para efecto de la sensibilización no ha dado los resultados esperados; olvidamos que quienes están frente a nosotros son personas con formas de aprendizajes diferentes y se les debe brindar la información con metodologías de educación creativa, participativa, de aprendizaje significativo y orientado por una epistemología constructiva.

Posibles aplicaciones para los métodos de sensibilización

Como ya se mencionó, los métodos de aprendizaje son la manera en la que cada uno de nosotros captamos la información y la procesamos, sí, el éxito de la sensibilización depende de los mecanismos utilizados para no solo hacer llegar la información a la persona sino generar una cultura de la importancia de esta información y la gran responsabilidad que tiene el sujeto frente a su protección y reserva.

Normalmente en una clase magistral, se toman decisiones como, qué método usar para que los estudiantes asimilen el conocimiento, esto se hace por medio de un análisis del grupo que permita definir o determinar una metodología. Para el caso de sensibilización existen manuales y normas que explican o sugieren como realizar este entrenamiento, como por ejemplo la norma "*NIST 800-50 Construcción de un programa de Concientización y Entrenamiento de Seguridad de Tecnologías de Información*".

Más allá de implementar una u otra metodología la sugerencia es: conozca la organización o el grupo al que va a sensibilizar, si es necesario haga un análisis senillo de los conocimientos básicos que tiene sobre el tema, y saque todos los recursos necesarios para que la interiorización sobre seguridad, sea real y vivencial; es decir, utilice medios visuales, ejemplos que sean reales y adaptados a la situación psicosocial o psicoafectiva, del público receptor.

No se case con una sola metodología, investigue nuevos métodos y realice esta sensibilización con actividades lúdicas; cuando el cerebro se encuentra en un estado de relax, es mucho más receptivo que en medio de presiones ya sean de tiempo, espacio o simplemente disponibilidad.

VII. MEDIOS Y METODOS APLICABLES DE SENSIBILIZACIÓN

Como ya se mencionó la "*NIST 800-50 Construcción de un programa de Concientización y Entrenamiento de Seguridad de Tecnologías de Información*", proporciona una guía para la construcción de programas de seguridad de tecnologías de información y soporte efectivos que pueden aplicarse a cualquier tipo de entidad.

En el mencionado documento se establecen los tres componentes clave para el desarrollo de una cultura en seguridad de la información:

Concientización: Su objetivo es lograr que las personas reconozcan los comportamientos que se deben reforzar en materia de seguridad de la información, por ejemplo, mantener el escritorio limpio, tener copias de respaldo, usar el correo responsablemente, el uso adecuado de contraseñas, cuidados especiales con dispositivos móviles, etc.

Entrenamiento: Este es un ciclo de aprendizaje continuo que busca generar habilidades y competencias en las personas con el fin de que estas las apliquen en su cotidiano vivir.

Educación: Se basa en la formación de expertos en seguridad, por ejemplo la capacitación en sistemas de seguridad de la información o en auditoría interna ISO27001.

Dentro de las fases mencionadas en el programa Conciencia y Entrenamiento se encentran:

1- **Fase de diseño:** En esta fase se define la estructura del programa, la evaluación de las necesidades, el desarrollo de las estrategias y planes, la definición de las prioridades, la aprobación y el financiamiento.

2- **Fase del desarrollo del material:** Esta fase está dividida en el material utilizado para la concientización y el utilizado para el entrenamiento. Aquí se seleccionan los temas, fuentes a utilizar, definición de los modelos del programa de concientización y cursos de entrenamiento.

3- **Implementación del programa:** se realiza primero por medio de una difusión que permite dar a conocer el programa y pretende generar expectativas dentro de la organización; luego por medio de diferentes técnicas o metodologías de sensibilización, se difunde el material didáctico o de formación que se ha planteado utilizar para este fin, por ejemplo: posters, videos, conferencias, boletines, concursos etc.; por último se desarrollan las actividades utilizando las diferentes técnicas establecidas.

4- **Mantenimiento:** Se debe realizar un monitoreo del programa, evaluarlo para ser retroalimentado, gestionar cambios de ser necesario, medir a través de indicadores.

Todo esto se debe realizar con el aval de la gerencia, la alta dirección, la rectoría de cualquier institución según sea el ámbito donde se realice la sensibilización.

Dentro de todo el desarrollo de una sensibilización no se deben descuidar a las personas, pues el verdadero éxito de esta propuesta radica, en la forma como es asimilado el concepto de seguridad y como es interiorizado por el personal sensibilizado.

De la misma forma se pueden dar herramientas que ayuden a quienes son padres de familia en la orientación a sus hijos sobre el tema de seguridad. Más allá de pretender generar malestar o paranoia frente al tema, se debe tratar de forma clara, permitiendo que los niños, adolescentes y jóvenes puedan sacar sus propias conclusiones y expresar su propia opinión sobre el tema.

Los métodos que se encuentran en la actualidad están referidos netamente al desarrollo de sensibilización en las organizaciones, esta sensibilización a nivel familiar, corresponde a los padres y en ocasiones a los maestros que tratan el tema de los diferentes delitos informáticos. Si bien es cierto para muchos de los jóvenes y adolescentes, los adultos no tienen mucho que aportar frente a temas de tecnología no debemos dejar de lado el concepto de información que no necesariamente esta almacenada de forma electrónica, pero si masificada actualmente.

Sentarse a dialogar con ellos, a investigar juntos y a educar, no solo en valores sino en conciencia y responsabilidad de su propia vida puede hacer la diferencia pues aprenden juntos y al mismo tiempo se brindan la posibilidad de compartir y reconocerse como seres humanos que merecen respeto y que se permiten ser escuchados.

VIII. CONSEJOS PRÁCTICOS PARA TODO PÚBLICO

Frente a esta problemática pretendemos mostrar algunas buenas prácticas que se pueden implementar:

- No reenviar cadenas de correos electrónicos
- Al hacer una transacción por internet asegurarse de digitar correctamente la página.

- Con el fin de garantizar la seguridad de una transacción verifique que en la página de internet dónde se esté realizando la transacción, tengan al inicio de la dirección, las siglas **https** y no solamente **http**.

- Para evitar suplantaciones o accesos a información confidencial a través de los teléfonos inteligentes no usar redes wi-fi desconocidas.

- Es importante revisar las condiciones de privacidad en todas las redes sociales, y estar atentos a no publicar o revelar información que permita la identificación de datos como: nuestro lugar de residencia, a donde hemos ido de vacaciones, así como la cantidad de adquisiciones en un tiempo de terminado.

Dime qué publicas y te diré quién eres.

Al tener una cuenta en cualquier Social Media, eres considerado un ciudadano digital, que para la buena suerte puedes tener una imagen intachable y perfecta; o por el contrario, ridícula y negativa.

Se debe tener en cuenta que es el mismo usuario quien puede crearse mala fama, al convertirse en amo de lo que publica, es exclusivamente él dueño de lo que dice y cómo lo dice, entonces a partir de allí su círculo social online construye en su imaginario una idea de quién es. De esa manera, nuestra personalidad online estará directamente relacionada con el potencial que mostremos en cada uno de esos escenarios. No se trata solo de las capacidades cognitivas y los aspectos físicos, también se trata de establecer los límites de nuestra intimidad y privacidad; y qué es lo que deseamos que nuestros contactos conozcan y sepan acerca de nosotros.

De acuerdo a la "*Guía para usuarios: identidad digital y reputación online*" algunos de los determinantes de la reputación online son:

- El contenido generado por nosotros mismos.

- El contenido sobre nosotros generado por terceros.

- El contenido generado en el marco de las relaciones con los demás.

Igualmente, se pueden observar algunas recomendaciones para la correcta gestión de la identidad online, así como las reacciones frente a casos especiales:

- Creación responsable de perfiles.

- Configuración adecuada de la privacidad y seguridad.

- Participación respetuosa en la red.

- Aplicación de medidas y hábitos de seguridad en la navegación.

- Revisión periódica de la identidad.

Qué hacer en caso de sentir vulnerada su identidad:

Cuando una persona sea víctima de cualquier tipo de ataque debe realizar las siguientes acciones

- Denuncia interna a proveedores de servicios.

- Denuncia judicial frente a atentados contra la reputación

- Denuncia de posibles delitos informáticos. (Ver página de la policía, Delitos Informáticos)

Finalmente, la popularidad o reconocimiento en las redes sociales está determinada por cómo nos mostramos y vendemos en ellas, somos nosotros mismos exclusivamente los dueños de lo que publicamos, (a menos que seamos víctimas de robo de identidad o hackeo de nuestras cuentas).

Tips de Knowthenet.org.uk para combatir el trolling:

Para los adolescentes:

1- No "alimentar" a los trolls. Ellos se alimentan de las respuestas, entonces, hagas lo que hagas, nunca contestes.

2- No dudes en informar dile a un compañero, profesor, padre o alguien en quien confíes sobre lo que sucede lo más pronto que puedas.

   Pide ayuda para poder juntar evidencia de rastros sobre algún email o mensaje en caso de que se vuelva más grave.

Para los padres:

1- Escuche a su hijo y dialogue con él sobre el problema que está teniendo, no lo juzgue, no lo culpe, acompáñelo y juntos adopten medidas para evitar entrar en contacto nuevamente.

2- Ayude a su hijo con los elementos prácticos de recolección de evidencia, pero sea respetuoso de su privacidad. Por eso, pregúntele antes de leer sus mensajes.

3- Apoye a su hijo a reportar el abuso en la red social, el servicio de mensajería online, o incluso las autoridades y siga de cerca la situación de manera regular.

4- Establezca límites en la forma y en las horas que se ocupa el computador y se consume Internet.

5- Use controles en los distintos dispositivos electrónicos que tenga en casa. Algunos de ellos son: *Qustodio, K9 Web Protection, Avira Social Network Protection, Kids Place Parental Control, Norton Family*.

6- Respete e invite a sus hijos a respetar los límites de edad de las redes sociales. La mayoría de ellas piden que los usuarios sean mayores de 13 años.

7- Los chats no son recomendables para los más pequeños. En caso de aceptar el uso de estos, procure supervisar sus comunicaciones y con quienes las tienen.

8- Enseñe la importancia de no compartir información privada en sus conversaciones digitales (su nombre completo, dirección de la casa, edad, entre otros).

9- Si son pequeños, es recomendable que no tengan una dirección de correo propia, sino que usen una familiar.

10- En caso de querer crear una cuenta de correo, háganlo juntos.

11- Decir a los niños que no respondan correos o mensajes de personas que no conocen, ya que pueden ser víctimas de '*grooming*' u otro delito informático.

12- Invite a sus hijos a recurrir a usted y su pareja o a otro adulto en caso de encontrarse en una situación incómoda en la red.

13- *WOT* (*Web of Trust*) es una herramienta de navegación segura que indica qué sitios web son confiables, permite realizar búsquedas, transacciones y compras con tranquilidad.

14- *KidZui* es un navegador diseñado especialmente para que sea usado por niños y niñas entre los 3 y 12 años.

15- Telefónica Movistar trajo a Colombia la aplicación 'Te Protejo' para equipos móviles con sistemas operativos *iOS*, *Android* y *Blackberry*. A través de ella se pueden denunciar contenidos relacionados con pornografía infantil.

Todos seguros con el internet

Estas son algunas páginas para visitar y conocer las ventajas y los riesgos en la red:

www.enticconfio.gov.co
www.teprotejo.org
www.pantallasamigas.net
www.ciberfamilias.com
www.tus10comportamientosdigitales.com

CONCLUSIONES

Concientizar a las personas de que son el eslabón más importante en materia de la Seguridad de la Información, es un reto para todas las organizaciones y para la sociedad en general ya que la información cuando cae en manos equivocadas por exceso de confianza de los usuarios o por falta de información para ser protegida correctamente, se convierte en el mejor insumo para realizar fraudes, suplantaciones y otros delitos informáticos

Generar en las empresas la conciencia que invertir en la sensibilización de las personas es una de las mejores estrategias adoptadas por una organización en el tema de protección de la información sensible de la misma.

Se debe tener en cuenta que quienes permiten que la seguridad informática sea violentada son los empleados de las organizaciones, por descuidos tal vez involuntarios, y estos a su vez son los mismos padres de adolescentes que no se percatan de la información que rota por el ciberespacio.

Es importante la inversión que las compañías realizan en tema de seguridad, pero es más importante aún que los usuarios de nuevas tecnologías cibernéticas que crecen día a día tomen conciencia de capacitarse, para prevenir robos de información y que tomen conciencia que la confianza no siempre es la mejor herramienta de navegación, de lo contrario todo el dinero invertido por las organizaciones en cuanto a tecnología no será fructífero.

IX. REFERENCIAS

[1] Introducción a la Teoría General de la Administración, Séptima Edición, de Chiavenato Idalberto, McGraw-Hill Interamericana, 2006, Pág. 110, México.

[2] Introducción a los Negocios en un Mundo Cambiante, Cuarta Edición, de Ferrell O. C. y Hirt Geoffrey, McGraw-Hill Interamericana, 2004, Pág. 121, México.

[3] Colaboradores de Wikipedia. Información [en línea]. Wikipedia, La enciclopedia libre, 2014 [fecha de consulta: 1 de Abril de 2014]. http://es.wikipedia.org/wiki/Informaci%C3%B3n.

[4] Diccionario de la Real Academia Española. Información [en línea]. 2014 [fecha de consulta: 1 de Abril del 2014]. Disponible en: http://lema.rae.es/drae/?val=informaci%C3%B3n.

[5] Diario el Espectador en su versión Online http://www.elespectador.com/print/442538

[6] Revista online Knowthenet Power by nominet http://www.knowthenet.org.uk/articles/nineteen-year-old-males-revealed-top-trolling-target

[7] Globak Corporate IT Security Risks: 2012 Kaspersky lab Mayo de 2013

[8] Reporte de Norton 2013 Symantec Contacto de RP Heidi Cortés, Symantec heidi_cortes@symantec.com

[9] ¿Ha sido víctima de algún delito informático? Revista Online Colombia Digital, Corporacón Colombia Digital @colombiafdigital 28 de enero de 2013

[10] Recomiendan configurar la privacidad de las redes sociales, Alejandra Galicia/SPSE Cancún

Revista Online Novedades QUINTANA ROO, abril 6 de 2014.

[11] Jugando a crear cultura de seguridad de la información – De la teoría a la práctica Carlos Villamizar R. CISA, CISM, CGEIT, CRISC, CobiT Foundation Certificate e ISO27001 LA • 30/08/2013

Autores

Nidia Nayibe González Pinzón
Ing. de Sistemas
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia

Leonardo Téllez García
Ing. de Sistemas
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia

---

[i] Introducción a la Teoría General de la Administración, Séptima Edición, de Chiavenato Idalberto, McGraw-Hill Interamericana, 2006, Pág. 110, México.

[ii] Introducción a los Negocios en un Mundo Cambiante, Cuarta Edición, de Ferrell O. C. y Hirt Geoffrey, McGraw-Hill Interamericana, 2004, Pág. 121, México

[iii] http://lema.rae.es/drae/?val=informaci%C3%B3n

[iv] Gartner. Datos segundo trimestre de 2012

[v] http://www.symantec.com/es/mx/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

[vi] En terminología de internet, el trolling es la acción de publicar comentarios en foros, chats, grupos de noticias o blogs, que son despectivos o incendiarios para que otros usuarios reaccionen.

[vii] Artículo del 24 de Marzo de 2014 "Adolescentes de cabeza en Internet"