CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Vega Lizarazo César
cesavegl@gmail.com
Universidad Piloto de Colombia

Resumen— El uso de las tecnologías de la información y las comunicaciones se constituye en uno de los pilares del mundo globalizado El crecimiento continuo de las herramientas disponibles para la administración de la información, tales como celulares, tabletas, portátiles, etc., permiten acceder a un mundo de información de diverso contenido, tales como redes sociales, correos electrónicos, fotos, chats, blogs, etc., y a su vez permite a los ciberdelincuentes ampliar su panorámica, respecto a sus objetivos, accediendo a información personal, financiera, social y demás. Éste despliegue de tecnología, y su evolución converge en riesgos en la seguridad de la información, lo cual genera la necesidad de adoptar medidas y controles efectivos que permitan resguardarse de dichas amenazas.

Este documento se enfoca en enunciar recomendaciones para crear concienciación en seguridad de la información en favor de la seguridad y así aprovechar de la mejor manera el avance tecnológico.

Abstract— The use of information and communication technologies constitutes one of the pillars of the globalized world. The continuous growth of the tools available for the administration of the information, such as cellular, tablets, laptops, etc., allow access to a wide variety of information of diverse content, such as social networks, emails, photos, chats, blogs, etc., and at the same time allows the cybercriminals to broaden their view, with respect to their objectives, accessing personal, financial, social information and other one. This deployment of technology and its evolution converges into risks in information security, which generates the need to adopt effective measures and controls to protect against such threats.

This document focuses on enunciating recommendations to create information security awareness in favor of security and thus make the best use of technological progress.

Índice de Términos—Amenazas, concienciación, controles, seguridad, sensibilización.

I. INTRODUCCIÓN

En Colombia se ha incrementado el uso de las tecnologías de la información y de las comunicaciones y por lo tanto, lo hacen en la misma medida los riesgos a amenazas cibernéticas. Los Usuarios de internet, como porcentaje de la población, muestran a Colombia con un 55.9%, por encima del porcentaje de América Latina y del Caribe quienes presentan un crecimiento del 54.46% [1].

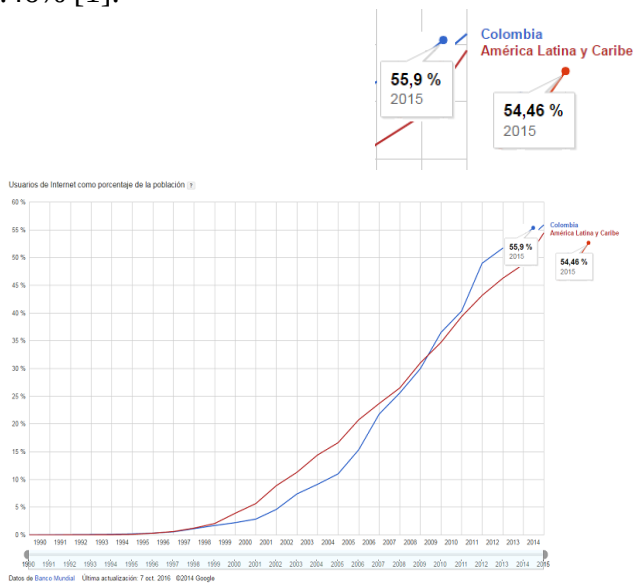

Fig. 1. Estadística de usuarios de internet como porcentaje de la población [1].

De acuerdo con el informe del Ministerio de Tecnologías de la Información y Comunicaciones - MINTIC, el total de suscriptores de internet es de 10.724.422 hasta el primer trimestre de 2015. Teniendo en cuenta que el total de la población en el 2015 era de 48.228.000 y siendo el internet móvil el de mayor uso con una diferencia de 102.204 suscriptores, podemos decir que el 22.23% de la población tiene acceso a internet entre internet fijo e internet móvil [2].

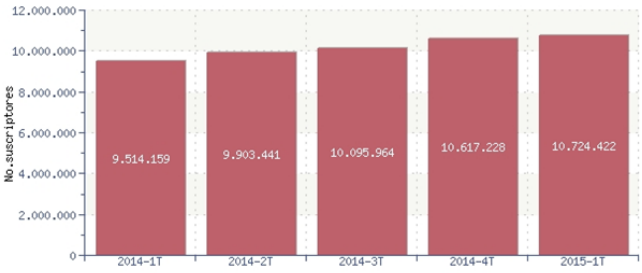

Fig. 2. Total de suscriptores de internet en Colombia [2].

II. INTERNET DE LAS COSAS (IOT)

Pero no solo los dispositivos móviles o el internet fijo acceden a la red. También lo hacen los dispositivos IoT cuya cifra es aún mayor. El término "internet de las cosas" o IoT, por sus siglas en inglés, es un concepto un poco abstracto que intenta representar cosas cotidianas que se conectan a internet [3]. En un concepto más formal, se puede decir que se trata de una red que interconecta objetos físicos valiéndose del internet.

El principio sobre el cual funcionan es el mismo y la clave es la operación remota. Los objetos conectados a internet tienen una ip fija lo que les permite ser accedidos para recibir instrucciones. Los sectores donde hay mayor aplicabilidad son la industria de producción en masa con sus robots ensambladores, sensores de temperatura, control de producción; control de infraestructura urbana, como por ejemplo control de semáforos, puentes, vías de tren, cámaras urbanas (para foto-comparendos, control de tráfico, seguridad); control ambiental, quizás el que más aplicabilidad se le ha dado como lo es acceder desde prácticamente cualquier parte a información de sensores atmosféricos, meteorológicos, y sísmicos; sector salud, donde el personal médico puede monitorear activamente a los pacientes de una forma ambulatoria y no invasiva.

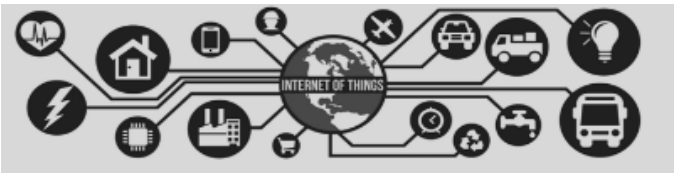

Fig. 3. Internet de las cosas [3].

Según el IBSG de Cisco de 2012, se calculó que en 2020 habrá 50.000 millones de dispositivos conectados a internet, lo que hace una media de 6,58 aparatos por persona [4]. Por ello, se estima que para 2025 todos los dispositivos que rodean el día a día estén conectados a internet.

Llega un momento en el que los datos que entran en la red dejan de ser controlables por el usuario. Por ello, uno de los principales problemas del internet de las cosas es garantizar la seguridad y confidencialidad de la información recolectada; garantizar la seguridad e integridad física del usuario.

La comunicación inalámbrica vía wifi es otro de los riesgos a los que mayor expuestos estamos, ya que generalmente no está asegurada por un buen protocolo y la clave que se tiene es la por defecto del fabricante, haciéndola más vulnerable. Por ejemplo, desde una cámara fotográfica conectada a mi red wifi puedo acceder a mis repositorios de fotos, pero también a los demás equipos de la red ya sea del hogar o bien de la empresa (si está permitido), lo cual hace del dispositivo una puerta de fácil acceso y por consiguiente haciendo la red vulnerable.

Ante este panorama, solo queda una pregunta: ¿y la seguridad a cargo de quién? Las empresas encargadas de desarrollar dispositivos inteligentes, deben incorporar desde su diseño mecanismos de privacidad y protección de datos. Estos dispositivos también deben estar alineados con los tres pilares de la seguridad como son la confidencialidad, disponibilidad e integridad. Los fabricantes deben tomar medidas como sistemas propietarios de cifrado de los datos almacenados, que por la gran variedad de algoritmos, hace que se le dificulte más al atacante el descifrado y por lo consiguiente, se les hace más costoso y abandonan la idea.

Otra medida trata de la implementación de un sistema de autenticación, como los mensajes de texto seguros por token, ipsec y otros [5].

Una tercera medida, se refiere al uso de protocolos seguros como TLS, aunque también existe los que se conoce como encriptación liviana (ligthweigth cryptographic) que hace el proceso más rápido y eficaz.

Cada vez se encuentran más problemas cuando se ingresa al mundo de la seguridad de la información tanto a nivel personal como a nivel corporativo. Las empresas, para proteger su negocio, han puesto mayor empeño en implementar medidas de seguridad y por lo tanto han implementado programas de concienciación en seguridad. Desafortunadamente no son muchas las empresas que han tomado conciencia de la necesidad de proteger su activo más valioso: la información. Las causas son diversas para la no implementación de estos programas. Se trata muchas veces de los costos inherentes y de la falta de conciencia a nivel corporativo. La alta gerencia lo ven como un "gasto injustificado", pero cuando son objeto de la materialización de algún riesgo que les afecta sus finanzas, es cuando ven la necesidad de implementar un SGSI y de crear conciencia en sus

empleados.

De otra parte, las personas en general no han creado conciencia en materia de seguridad y por lo tanto son objeto de ataques frecuentes debido a esa falta de conocimiento sobre el tema, o de que simplemente lo ignoran.

"El mercado tiene la misión de educar a la sociedad para que el internet de las cosas funcionen de una manera responsable, al igual que es importante toma conciencia del tipo de información que intercambiamos en internet para poder disfrutar de la tecnología de una forma segura" [6].

III. GUÍA PARA LA CONSTRUCCIÓN DE PROGRAMAS DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

El cibercrimen es un negocio que mueve mucho dinero y que se desarrolla en todo momento ideando nuevas formas de ataque para no ser detectados y en los que hasta el más precavido pueda caer en sus redes. Este es un fenómeno global y por lo tanto debería existir interés mundial en sensibilizar a las personas por diferentes medios para ir cerrando la brecha. Pienso que el sistema educativo formal debería implementar un programa de sensibilización en todos los grados escolares para que los jóvenes, quienes son los mayores consumidores de contenido, sean los que inicien el proceso de implementación de medidas que les permita minimizar el riesgo al conocer las amenazas y los métodos usados para materializarlas. Son ellos los que van a transmitir ese conocimiento a las nuevas generaciones haciendo de este un ciclo continuo de concienciación para que no se pierda una de las prioridades en el uso de nuevas tecnologías como lo es el del uso correcto y seguro.

A nivel corporativo se intenta crear una cultura de seguridad de la información costo-efectiva en las empresas [7]. Una iniciativa en esta materia fue desarrollada por el Instituto Nacional de Estándares y Tecnología - NIST (por sus siglas en inglés) en el mes de octubre de 2003. Se trata de una guía para la construcción de programas de seguridad de tecnologías de la información y soporte efectivos. Aunque los requerimientos fueron especificados por la Administración de Seguridad de la Información Federal (FISMA), por sus siglas en inglés, en 2002 y por la Oficina de Gestión y Presupuesto (OMB), circular A-130, appendix III., estos pueden aplicarse a cualquier tipo de entidad.

El documento generado por ellos se denomina "NIST 800-50 Construcción de un Programa de Concientización y Entrenamiento de Seguridad de Tecnologías de Información". Consta de cuatro pasos críticos en el ciclo de vida de un programa de concientización y capacitación en seguridad de TI:

1. Diseño del programa de concientización y capacitación (Sección 3).
2. Desarrollo de material de sensibilización y capacitación (Sección 4).
3. Implementación del programa (Sección 5).
4. Post-implementación (Sección 6) [8].

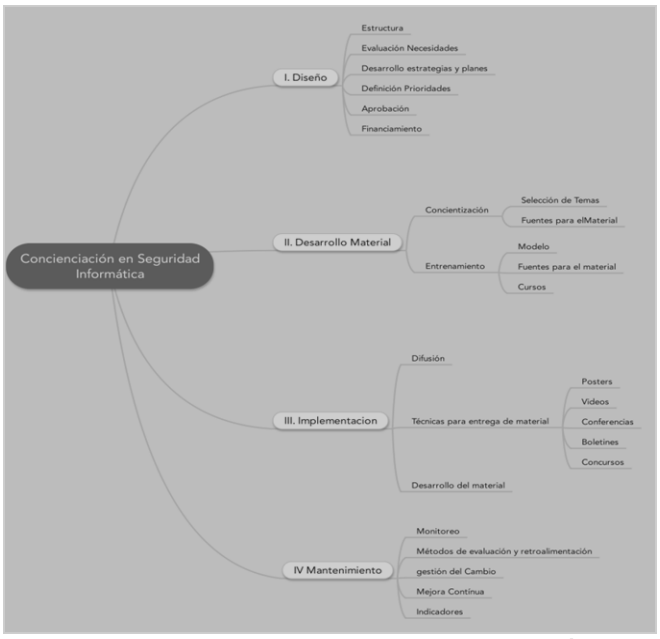

Fig. 4. Fases ciclo de vida de un programa de concientización y capacitación en seguridad de TI [7].

El documento es una publicación complementaria a la Publicación Especial NIST 800-16, Requisitos de capacitación en seguridad de las tecnologías de la información: un modelo basado en el rol y el desempeño. En un nivel estratégico superior, la SP 800-50 discute cómo construir un programa de sensibilización y capacitación en seguridad de TI, mientras que SP 800-16 se encuentra en un nivel táctico inferior, describiendo un enfoque de seguridad de TI basada en roles.

De este documento se extraen los tres componentes de un programa para desarrollar la cultura en seguridad de la información: concientización, entrenamiento y educación.

A. Concientización. Su propósito es sensibilizar

las personas en seguridad de la información para despertar su interés en dichos temas, logrando identificar inicialmente los comportamientos que se quieren reforzar, como por ejemplo, el de mantener el escritorio limpio, apropiarse de cultura de contraseñas seguras, del uso del correo corporativo cumpliendo las normas establecidas para su uso, ser partícipes de la seguridad física, identificando personal ajeno a su oficina y notificándolo a la autoridad competente, velar por el respaldo de la información corporativa almacenada en sus equipos, etc.

B. Entrenamiento. Se basa en la adquisición y apropiación de habilidades y competencias de seguridad de la información con el objetivo de su aplicación en todas las actividades laborales y porque no personales.

C. *Educación.* La necesidad de capacitar personal interno en temas de seguridad a un nivel más profundo para convertirlos en especialistas de la seguridad de la información mediante una capacitación en esa materia o cursos en auditoría interna ISO27001, con su respectiva certificación [7].

IV. IMPLEMENTACIÓN

Como ejemplo de técnicas corporativas para crear concienciación, se realizan actividades como:

A. *Ataques dirigidos (simulados)* para demostrar lo expuestos que están los empleados. Por ejemplo enviarles un correo electrónico con archivo malicioso adjunto (con una advertencia y un consejo), dejar sueltos pendrives infectados (con una advertencia y un consejo).

B. *Crear una campaña con una mascota publicitaria*[1].

C. *Definir un eslogan para la campaña.* Un slogan bien estudiado, conceptualizado y construido es muchas veces un factor concluyente, que resume en pocas palabras lo que un producto, un servicio o una persona hará por las personas. Al ser de corta longitud (pocas palabras) y ser repetido constantemente en discursos o publicidad, el ser humano lo hace propio.

D. *Elaboración de materiales diversos* como pendones, posters, afiches, carteleras, protectores y fondos de pantalla, correos corporativos (con un logotipo representativo que indique la fuente), avisos en la intranet como imágenes, videos, presentaciones animadas o en la herramienta power point y documentos explicativos[2].

E. *Consejos, tests* (mini auditorias).

F. *Creación y entrega de recordatorios* como llaveros, tazas, lapiceros o tarjetas que dan una idea sobre construcción de claves seguras.

G. *Desarrollar tripticos.*

H. *Desarrollar trivias.*

I. *Elaborar juegos* como monopolio o álbum de figuras con temas relacionados por supuesto con seguridad de la información.

J. *Concursos basados en pictogramas.*

K. *Obras de teatro, stand up comedy o cuentacuentos* (relacionados con temas de seguridad de la información).

L. *Encuestas* [7].

M. *Uso de contraseñas seguras*. La cantidad mínima de caracteres a usar es 8. Entre más larga una contraseña, menos probabilidad de ser vulnerada. Se deben combinar, letras, número, símbolos (#, $, %, &, etc.), signos de puntuación. Se debe cambiar con periodicidad de 30 días y usar una diferente por cada servicio en internet.

N. *Precaución con el correo electrónico.*

1. Realice un análisis antes de abrir algún correo.
2. Sospeche de los mensajes no esperados. Algunas veces vienen de conocidos, por lo tanto analice primero. Si de alguna forma Ud. sospecha, se aconseja llamar por teléfono al remitente para asegurarse.
3. No use servicios de wifi gratuitos para acceder a sus cuentas bancarias, realizar pagos por internet, abrir correos, aplicaciones corporativas, ni escribir información sensible como la cédula, dirección de residencia o datos personales y bancarios en general, etc.

[1] Personaje que representa a una marca, creando un lazo entre el producto o servicio y el consumidor

[2] Ver ejemplos de posters en https://seguridad-de-la-informacion.blogspot.com.co/2012/02/materiales-de-concienciacion-en.html

4. Si hace uso de redes públicas:
   - Al finalizar, limpie el historial del navegador.
   - Al finalizar, limpie el cache del navegador.
   - Desactivar las opciones "autocompletar" y "recordar contraseña".
   - Debe cerrar todas las sesiones de las aplicaciones sociales que utilice, como por ejemplo, facebook, twitter, gmail, etc.
   - Siempre usar https. Los navegadores cuentan con plugins que permiten realizar dicho tipo de navegación segura "https anywhere".
5. Analizar los adjuntos en los correos aunque provengan de fuente conocida. Cabe la posibilidad de que sean maliciosos. Ante cualquier sospecha, llame al remitente.
6. Mediante el correo electrónico se hace ingeniería social. Le envían mensajes donde le ofrecen trabajo en el que "obtendrás muchos beneficios, desde casa y trabajando solo unas horas...", lo cual lo hace muy llamativo. Normalmente detrás de eso suele haber una mafia de ciberdelincuentes que bien estafan o bien incitan a cometer un delito normalmente de blanqueo de dinero.

O. *Generales*

1. Los ciberdelincuentes hacen uso de la técnica de ingeniería social para obtener datos que les permita vulnerar los sistemas y realizar ataques. Es muy importante en el trabajo, tener una política de escritorios limpia donde lo que se busca es no dejar "a la vista" ningún documento que incluya información sensible y que pueda ser utilizada de manera fraudulenta. La impresora debe estar limpia de documentos que hayamos impreso y contengan información confidencial. También es importante mantener limpia la papelera de reciclaje de los equipos ya que allí pueden haber documentos confidenciales que pueden ser aprovechados por los ciberdelincuentes. A esta técnica se conoce como "basureo".
2. Frente a la evidencia de suplantación de identidad, denuncie y revise el perfil para minimizar el riesgo de acceso a personas desconocidas.
3. Si requiere descargar algo, siempre revíselo y analícelo antes de proceder a su descarga. No use aplicaciones P2P. Las redes peer to peer permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados haciendo fácil inyectar malware.
4. En dispositivos móviles hay que revisar los permisos que la aplicación solicitó o está solicitando dado que puede Usted estar dando permiso para envío de mensajes de texto (sms, short message service) de manera predefinida o autorizando cargos extras o instalación de componentes de terceros que no han sido validados y pueden estar generando spam hacia su dispositivo.
5. Si viaja, no divulgue fotos ni pregone hacia dónde se dirige, con quién, cuánto tiempo durará por fuera, etc. Así evita que por ejemplo, le roben su casa o apartamento.
6. Si toma fotos, evite el geoposicionamiento de fotos o tuits (tweets, por su palabra en inglés) ya que con ello pueden ubicar su posición. Hay dispositivos que guardan metadatos (que divulgan datos como el modelo de la cámara, usuario y software utilizado, versiones, etc.) que le dan información valiosa a un atacante para acceder vía internet a la cámara y robar información o usarla como una botnet.
7. Whatsapp no es totalmente segura, por lo que se aconseja no enviar información sensible por ese medio.
8. Si desea compartir documentos, se aconseja el uso de dropbox o una plataforma similar.
9. Evite compartir información sensible en las redes sociales, dado que toda información que suba, quedará expuesta de forma permanente al público y por lo tanto, cualquiera puede copiarla y

compartirla.

10. Dejar accesible en su perfil información sensible como su dirección, teléfono, fecha de nacimiento, datos financieros, datos personales, etc. serán aprovechados por los delincuentes para acceder a su perfil y suplantar su identidad. Para este caso, se recomiendo el uso de un alias, sobrenombre, nick (en inglés), lo cual lo ayudará a proteger su identidad y privacidad.
11. No acepte peticiones de amistad de gente que no conoce. Es una técnica de ingeniería social para poder llegar a Usted o a otras personas amigas suyas las cuales poseen un perfil atractivo para el delincuente.
12. No usar la cuenta corporativa para fines personales. Esto puede estar prohibido por muchas empresas y estar explícito en su política de seguridad y en sus contratos de trabajo, lo que puede llegar a generarle problemas judiciales al divulgar información confidencial sobre su trabajo o información que pueda usar la competencia.
13. Es muy recomendable no mezclar los contactos netamente laborales con los amigos ya que no tendrá control sobre lo que puedan escribir sus amigos a cerca de Usted. Por ejemplo, una broma o comentario inadecuado podrían hacerlo quedar mal ante la empresa o ante los clientes y hasta podría perder el puesto.
14. No hay que dejar los dispositivos móviles desatendidos. Puede haber sabotaje, fraude, mail intención o simplemente bromas de sus amigos que podrían actualizar su perfil y estado con información falsa con diversas consecuencias entre legales y civiles según la falta.
15. No guarde claves en el celular ni deje sesiones abiertas. En caso de robo, pueden ingresar a su perfil de redes sociales, entidades financieras, otras.
16. Los videojuegos online están siendo aprovechados por delincuentes ya que allí se exponen datos personales y bancarios tanto por adultos como por menores. Para mucha gente es una adicción que no tiene límites. El riesgo es mayor cuando los niños se exponen a juegos con contenido sexual o de alta violencia, lo cual hace eco en la mentes de estos chicos, volviéndose asociales y violentos, imitando sus personajes favoritos en sus escuelas, donde viven, con la familia, realizando actos reprochados por la sociedad.

    Se pueden dar casos de grooming en el que un adulto se hace pasar por un niño para ganarse la confianza de otro niño, o ciberbullying que es el ciberacoso entre escolares o adolescentes. De otra parte los chats disponibles en estos juegos sirven para que gente inescrupulosa se aproveche de la inocencia de los niños para invitarlos a encuentros donde los convencen de ser "actores porno", son acosados y terminan siendo violados o asesinados.
17. Debido al costo de los juegos populares, los jugadores terminan bajando software de la red y en sitios poco confiables, lo cual los hace vulnerables a malware.
18. Los jugadores también se encuentran expuestos al spam y al pishing. Los ciberdelincuentes realizan envíos masivos a los usuarios con mensajes fraudulentos donde promocionan casinos fraudulentos e inducen al usuario a que introduzcan sus credenciales o ingresen a un sitio malicioso donde serán infectados.
19. Aquellos jugadores que prefieren juegos offline, también quedan expuestos a malware si bajan el software en sitios desconocidos y conocidos como craqueados [9]-[11].

V. GLOSARIO DE TÉRMINOS

- *Activos de información*. Todos los componentes de información que tienen valor para la organización, todo lo que es posible realizar, concluir, visualizar y procesar de la información.
- *Amenaza*. Acción o evento que puede ocasionar consecuencias adversas en los datos.
- *Ataque.* Tipo y naturaleza de inestabilidad en

la seguridad.

- *Autenticidad.* Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quien los envió y cuando fueron enviados y recibidos.
- *Blanqueo de dinero.* El lavado de dinero (también conocido como lavado de capitales, lavado de activos, blanqueo de capitales u operaciones con recursos de procedencia ilícita o legitimación de capitales) es una operación que consiste en hacer que los fondos o activos obtenidos a través de actividades ilícitas aparezcan como el fruto de actividades legales y circulen sin problema en el sistema financiero.
- *Botnet.* Red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.
- *Ciberbullying.* También conocido como ciberacoso en español. Son amenazas, hostigamiento, humillación u otro tipo de molestias realizadas por un adulto contra otro adulto por medio de tecnologías telemáticas de comunicación, es decir: internet, telefonía móvil, videoconsolas en línea, etc.
- *Ciberdelincuente.* Persona que realizan actividades delictivas en internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.
- *Confidencialidad*. Propiedad de prevenir la divulgación de información a sistemas o personas no autorizados.
- *Crackear.* En español craquear. Desactivar la protección de los programas para no tener que insertar el disco original cada vez que se ejecute la aplicación o el juego, o para seguir utilizándolo pasado el período de evaluación. Es un asunto ilegal que vulnera los derechos de autor cuando la copia no tiene el destino autorizado.
- *Disponibilidad.* Característica de la información de encontrarse siempre a disposición del solicitante que debe acceder a ella, sea persona, proceso o sistema.
- *Dropbox.* Es un servicio de alojamiento de archivos multiplataforma en la nube, operado por la compañía Dropbox, Inc. El servicio permite a los usuarios almacenar y sincronizar archivos en línea y entre ordenadores y compartir archivos y carpetas con otros usuarios y con tabletas y móviles [19].
- *Grooming.* Es una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él.
- *Hardware.* Término en inglés que hace referencia a cualquier componente físico tecnológico, que interactúa de algún modo con un sistema computacional.
- *ISO. International Organization for Standardization.* Entidad internacional encargada de favorecer la estandarización en el mundo.
- *Incidente.* Se define como un evento que sucede de manera inesperada y que puede afectar la confidencialidad, integridad, disponibilidad de la información y además de esto los recursos tecnológicos.
- *Información.* Conjunto de datos que toman sentido al integrarse con características comunes.
- *Informática.* La informática es la ciencia que tiene como objetivo estudiar el tratamiento automático de la información a través de la computadora.
- *Ingeniería Social.* Tiene que ver con la manipulación psicológica de las personas para extraer información de ellas [12].
- *Integridad*. Propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- *Malware.* Abreviatura de “malicius software” (software malicioso), término que engloba a todo tipo de programa o código de computador cuya función es dañar un sistema o causar un mal funcionamiento. Este grupo podemos encontrar términos como: virus, troyanos (trojans), gusanos (worm), dialers, spyware, adware, hijackers, keyloggers, fakeavs, rootkits, bootkits y rogues, etc.
- *Metadatos*. Son datos altamente estructurados que describen información, el contenido, la calidad, la condición y otras características de

los datos. Es "información sobre información" o "datos sobre los datos".

- *P2P*. Una red peer-to-peer, red de pares, red entre iguales o red entre pares (P2P, por sus siglas en inglés) es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.
- *Pendrive*. La memoria USB (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información. Se le denomina también lápiz de memoria, lápiz USB, memoria externa.
- *Pictograma.* Es un signo claro y esquemático que representa un objeto real, figura o concepto. Sintetiza un mensaje que puede señalar o informar sobrepasando la barrera de las lenguas [20].
- *Pishing*. Es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.
- *Plugin*. Es aquella aplicación que, en un programa informático, añade una funcionalidad adicional o una nueva característica al software. En español puede nombrarse al plugin como un complemento.
- *Políticas*. Actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. Acción elegida como guía en el proceso de toma de decisiones al poner en práctica o ejecutar las estrategias, programas y proyectos específicos del nivel institucional.
- *Red*. Es una serie de computadores o dispositivos que se encuentran conectados entre sí, por un medio físico (cable) o de manera inalámbrica donde se comparte información, recursos y los servicios.
- *Riesgo*. La probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o un grupo de activos, generando pérdidas o daños.
- *SGSI*. Sistema de gestión de la seguridad de la información.
- *Seguridad*. Puede afirmarse que este concepto que proviene del latín “securitas” que hace referencia a la cualidad peligro, daño o riesgo. Algo seguro es algo cierto, firme e indubitable. La seguridad, por lo tanto, es una certeza.
- *Spam*. Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.
- *Trípticos*. Es un folleto informativo doblado en tres partes, por lo regular es del tamaño de una hoja de papel tamaño carta.
- *Trivia*. Es un juego de habilidad donde el jugador debe contestar preguntas sobre conocimientos generales. Cada pregunta tiene un valor en puntos dependiendo de su dificultad, con distintas opciones para elegir como respuesta y debe hacerlo dentro de un determinado tiempo.
- *Vulnerabilidad.* Es una debilidad en los procedimientos de seguridad, diseño, implementación o control interno que podría ser explotada (accidental o intencionalmente) y que resulta en una brecha de seguridad o una violación de la política de seguridad de sistemas.

VI. CONCLUSIONES

Colombia ha crecido en mayor medida que el resto del continente. Una de los motivos es el impulso dado por el Ministerio de las Telecomunicaciones a través del plan vive digital cuyo objetivo principal se refiere a que “las TIC son la mejor herramienta que tienen los países latinoamericanos para crear empleo y erradicar la pobreza”. [13]

El Ministro Molano Vega compartió un video con los principales logros del plan vive digital 2010-2014 que incluyen que Colombia será el primer país de Latinoamérica que tendrá este año internet de alta velocidad en todos sus municipios, el crecimiento exponencial de conexiones en hogares y mipymes[3], la vinculación del campo y sus habitantes con la tecnología, los avances en gobierno en línea, el desarrollo de la industria TI en el país, entre otros [13].

Otro de los objetivos principales son “…convertir

[3] Micro, pequeña y mediana empresa.

a Colombia en líder mundial de desarrollo de aplicaciones dirigidas a los más pobres y que el gobierno de Colombia sea el más transparente y eficiente gracias a las TIC" [13]. Todo esto en colaboración de la OEA quienes desde su interior impulsan la regulación tecnológica para mejorar la cobertura y servicios en el continente de América.

La Comisión Interamericana de Telecomunicaciones (CITEL) de la OEA han realizados gestiones para que los ciudadanos que hacen uso del servicio celular puedan comunicarse entre ellos. Desafortunadamente esta iniciativa no tuvo en cuenta la concienciación en seguridad de la información, ya que se debió realizar una campaña de sensibilización a medida que se iba ampliando el grupo de usuarios que acceden a la tecnología para comunicarse y hacer negocios, entretenimiento, vida social, grupos de interés científico, cultural, musical, etc.

Algunos países como España han estado regulando el mercado mediante normas y leyes que les permiten estar a la vanguardia a nivel de los países de habla hispana, en las iniciativas que sobre este tema de la sensibilización se han estado dando, como es el caso del Instituto Nacional de Seguridad (INCIBE), con su kit de concienciación a nivel pymes [14].

Las personas son el punto más débil en el entorno de la seguridad de la información, a su vez se convierten en el elemento de falla más común en un sistema de seguridad. Sin un programa de concientización, es muy común encontrar que la gente tiene claves escritas en libretas de notas, debajo de los teclados, sobre el monitor del usuario, en el correo, respaldos de información inexistentes o incompletos, errores de configuración en equipos, etc., que los hacen aún más vulnerables y susceptibles de materialización de amenazas [15].

Un ejemplo de cómo realizar la concienciación en las empresas se da para el caso del Ministerio de Ambiente y Desarrollo Sostenible, con un enfoque preventivo en el que se desarrolló un lema, una mascota, se alineó con el SGSI de la entidad cumpliendo con el Marco legal de Seguridad de la Información en Colombia [16]-[18].

La seguridad de la información es un deber de todos, tanto empresas, sistemas educativos y usuarios de los dispositivos IoT.

Se debe tomar conciencia del rol desempeñado, acatando las recomendaciones y cumpliendo con las normas que se establezcan para ello dentro del marco legal de seguridad de la información en Colombia. En la norma ISO27000 se haya que uno de los factores de éxito para su implementación y cumplimiento y por tanto la mejora continua es la concienciación del empleado y del usuario por la seguridad.

REFERENCIAS

[1] Banco Mundial. (2016). *http://datos.bancomundial.org*. Retrieved 11 14, 2016, from http://datos.bancomundial.org/indicador/IT.NET.USER.P2?contextual=min&end=2015&locations=CO-ZJ&name_desc=true&start=1990&view=chart.

[2] Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). Retrieved 11 14, 2016, from http://estrategiaticolombia.co/estadisticas/stats.php?id=34&pres=content&jer=7.

[3] Hipertextual. (2014, 10 20). hipertextual.com. Retrieved 11 14, 2016, from https://hipertextual.com/archivo/2014/10/internet-cosas/.

[4] Cisco. (2011, 04). *www.cisco.com*. Retrieved 11 14, 2016, from www.cisco.com: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[5] Telefónica. (2015, 06 17). *aunclicdelastic.blogthinkbig.com*. Retrieved 11 14, 2016, from aunclicdelastic.blogthinkbig.com: http://aunclicdelastic.blogthinkbig.com/seguridad-y-privacidad-en-iot-estamos-a-tiempo/.

[6] Ropero, C. (31 de 05 de 2016). *secmotic.com*. Recuperado el 14 de 11 de 2016, de secmotic.com: https://secmotic.com/blog/internet-de-las-cosas-seguridad/.

[7] HYPERLINK "http://www.magazcitum.com.mx/?author=44" \o "Posts by Carlos Villamizar R. CISA, CISM, CGEIT, CRISC, CobiT Foundation Certificate e ISO27001 LA" C. Villamizar. Jugando a crear cultura de seguridad de la información – De la teoría a la práctica (Agosto 2013). http://www.magazcitum.com.mx/?p=2361#.WCXtEvnhBaQ.

[8] Hash, W. M. (2016). *https://dl.acm.org*. Recuperado el 14 de 11 de 2016, de https://dl.acm.org: https://dl.acm.org/citation.cfm?id=2206263.

[9] ABC Tecnología. (2014, 08 25). *www.abc.es*. Retrieved 11 14, 2016, from www.abc.es: http://www.abc.es/tecnologia/consultorio/20140823/abci-facebook-perfiles-falsos-spam-peligros-201408221245.html.

[10] Wikipedia. (2016, 11 10). *https://es.wikipedia.org*. Retrieved 11 14, 2016, from https://es.wikipedia.org: https://es.wikipedia.org/wiki/Peer-to-peer.

[11] CSIRT-CV. (2016). *www.csirtcv.gva.es*. Recuperado el 14 de 11 de 2016, de www.csirtcv.gva.es: http://www.csirtcv.gva.es/es/paginas/este-veranorefresca-tu-seguridad.html.

[12] Gerardo Ayala, J. G. (2011). *repositorio.utp.edu.co*. Retrieved 11 14, 2016, from http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2514/0058A973.pdf?sequence=1.

[13] Ministerio de la Telecomunicaciones. (2014, 07 24). *mintic.gov.co*. Retrieved 11 14, 2016, from http://www.mintic.gov.co/portal/604/w3-article-6623.html.

[14] INCIBE. (2016). *www.incibe.es*. Recuperado el 14 de 11 de 2016, de https://www.incibe.es/protege-tu-empresa/kit-concienciacion.

[15] Secure Information Technologies - Secureit. (2015). *Secureit*. Retrieved 11 14, 2014, from http://secureit.com.mx/concientizacion-en-seguridad-de-la-informacion/.

[16] Camelo, L. (2010, 02 23). Blog sobre Seguridad de la Información en Colombia. Retrieved 11 14, 2016, from https://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html.

[17] Contreras, O. (2013, 05 08). prezi.com. Retrieved 11 14, 2016, from https://prezi.com/rdx0g-zitcgh/marco-legal-sgsi/.

[18] Ministerio de Ambiente y Desarrollo Sostenible. (2013, 09 01). *minambiente*. Retrieved 11 14, 2016, from http://www.minambiente.gov.co/images/tecnologias-de-la-informacion-y-comunicacion/pdf/PlanDeSensibilizaci%C3%B3nen_Seguridad_de_la_Informacion.pdf.

[19] Google Search. (14 de 11 de 2016). *www.google.com.co*. Recuperado el 14 de 11 de 2016, de https://www.google.com.co/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=""+definicion.

[20] Logopedia del Ponce de León. (2016). *www.ponceleon.org*. Recuperado el 14 de 11 de 2016, de www.ponceleon.org: http://www.ponceleon.org/logopedia/index.php?option=com_content&view=article&id=110&Itemid=96.

Autor

César Vega. Ingeniero de Sistemas de la Universidad Piloto de Colombia, año 1988, con especialización en Construcción de Software de la Universidad de los Andes, año 2001, Ha sido desarrollador de software haciendo uso de diferentes lenguajes de programación en diversas plataformas, destacándose en la investigación e implementación de nuevas tecnologías. También se ha desempeñado como líder técnico, supervisor, auditor de calidad. Estudiante de Especialización en Seguridad Informática en la Universidad Piloto de Colombia, año 2016.