Evaluación de la implementación de la norma ISO 27001 en empresas del sector privado, bajo un enfoque cultural.

Evaluation of the implementation of the ISO 27001 standard in private companies, under a cultural approach.

Juan Ignacio Cardona Fernández[1]
Raúl Augusto Restrepo Granada[2]

Resumen

Los avances tecnológicos y su aplicación en las empresas como herramienta en las funciones operativas y administrativas involucran también una gran cantidad de riesgos y amenazas. La información se convierte a su vez en el activo más importante de las compañías por lo que es vital analizar las razones por las cuales muchas de ellas carecen de políticas de seguridad apropiadas, más concretamente la norma ISO/IEC 27001:2013. El factor humano juega un papel fundamental (Hernández, 2019) y por eso se analiza la importancia de adoptar las mejores prácticas en la seguridad de la información, crear reglas y controles eficaces como también fomentar la cultura de la seguridad en las compañías. La finalidad del artículo es la generación de conciencia cultural en las empresas y el impacto y la relevancia de la implementación de la norma ISO 27001, brindando algunas técnicas y actividades que faciliten la implementación, llevando finalmente a las organizaciones a uno de sus objetivos principales, la seguridad de su información.

Palabras clave: Implementación norma ISO 27001, cultura norma ISO 27001 en Colombia, impacto norma ISO 27001, sistema de gestión.

Abstract

Technological advances and their application to enterprises - as operative and administrative tools - also carry a great deal of threats and risks. Information becomes the main asset for companies so that it is vital to analyze the reasons why so many of them show a lack of appropriate security policies, and particularly ISO/IEC 27001:2013. The human factor plays a fundamental role and for this reason the importance of adopting best security practices of information are analyzed, as well as the creation of rules and effective controls, and the promotion of the culture of security in companies.
The purpose of the article is the generation of cultural awareness in companies, and the impact and relevance of the implementation of ISO 27001, providing some techniques and activities that facilitate implementation, finally bringing organizations to one of their main objectives, the security of their information.

Keywords: Implementation of ISO 27001 standard, culture of ISO 27001 standard in Colombia, impact of ISO 27001 standard, management system.

Introducción

De acuerdo con el informe del Ministerio de Tecnologías de la Información y Comunicaciones - MINTIC, el total de suscriptores de internet viene creciendo de manera progresiva entre el último

---

[δ] Evaluación de la implementación de la norma ISO 27001 en empresas del sector privado, bajo un enfoque cultural.

[1] Ingeniero de Sistemas. Universidad de Antioquia. nachocardona@hotmail.com.

[2] Ingeniero de Sistemas. Institución Universitaria Salazar y Herrera. rarg2004@hotmail.com.

cuatrimestre del 2017 y el cuarto trimestre del 2018, como puede apreciarse en la figura 1, así mismo lo hacen los riesgos a amenazas cibernéticas según lo reporta la empresa ESET en un comparativo desde el 2017 hasta el 2018 para las empresas de Latinoamérica, tal como se presenta en la figura 2.

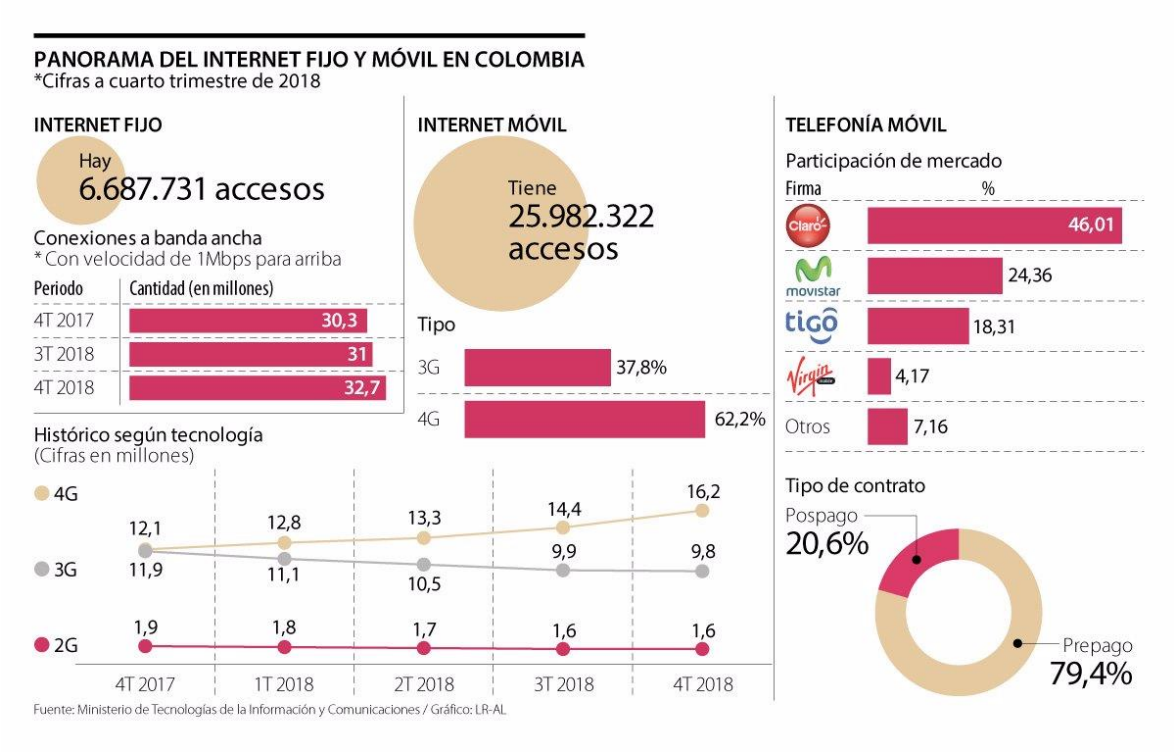

Figura 1.
Informe MINTIC Panorama uso del internet fijo y móvil en Colombia
Fuente: MINTIC (2019)

Figura 2.
Estado de la seguridad de las empresas de Latinoamérica
Fuente: ESET (2019)

Según Alberto Samuel Yohai, Presidente Ejecutivo del CCIT, el impacto que sufren las empresas colombianas luego de un ciberataque trasciende el costo económico por pérdidas de sus activos financieros y conlleva de manera colateral afectaciones a la productividad, daños reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y datos sensibles (CCIT, 2019).

Teniendo en cuenta estos antecedentes, conocer los riesgos asociados a la ciberdelincuencia y fomentar las buenas prácticas en las empresas en Colombia es un propósito que demanda esfuerzo integrado de la alta dirección, los proveedores de tecnología y hasta las autoridades responsables. ¿Por qué aún existen tantas empresas que no han implementado las políticas de seguridad? Aunque los motivos pueden ser múltiples, es precisamente la cultura organizacional el más relevante debido a que como se evidencia en el reporte de la empresa Eset (gráfica 2), el 40% de las empresas no tienen una política de seguridad definida.

La información es el activo más importante de las compañías y por ello debemos garantizar los tres pilares de la seguridad que son la integridad, la disponibilidad y la confidencialidad. Es importante entonces conocer las actividades que promuevan la conciencia sobre la seguridad de la información y cómo la norma ISO 27001 puede impactar positivamente brindando las herramientas necesarias para minimizar los riesgos del principal activo de las organizaciones, estas actividades abarcan tanto el diseño del programa de seguridad, como su implementación y mantenimiento.

La implementación de la seguridad de la información debe iniciar sin duda bajo el liderazgo de la alta dirección y proceder en orden jerárquico con la motivación cultural, lo cual depende del compromiso, de la comunicación, de la formación y capacitación de todos los integrantes frente al manejo de la seguridad de la información.

Este artículo se desarrolla de la siguiente manera, en la siguiente sección se presenta la metodología, luego se realiza un análisis del factor cultural en las organizaciones para contextualizar la importancia del factor humano en la seguridad de la información, a continuación se describen las tendencias y antecedentes en temas de seguridad, en la siguiente sección se contextualiza la relación entre la seguridad de la información y su impacto en la economía, luego se presenta un listado de actividades que pueden ayudar a promover la concienciación en la seguridad de la información, y por último, se presentan las conclusiones.

Metodología

En el presente artículo se establece la evaluación de la implementación de un sistema de gestión de seguridad de la información (SGSI) analizando la importancia que tiene el factor humano para este propósito, apoyando dicha gestión a través de actividades que sirvan como herramientas a las empresas para su implementación.

Marco teórico

A continuación, se presentan algunas definiciones importantes relacionadas con la seguridad de la información:

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.

ISO: *International Organization for Standardization.* Entidad internacional encargada de favorecer la estandarización en el mundo.

IEC: *International Electrotechnical Commission*. La Comisión Electrotécnica Internacional es la organización líder a nivel mundial que prepara y publica estándares internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas

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.

Ingeniería Social: Tiene que ver con la manipulación psicológica de las personas para extraer información de ellas.

Phishing: 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.

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.

Amenaza: Acción o evento que puede ocasionar consecuencias adversas en los datos.

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.

Dumpster Diving: Es una técnica utilizada para extraer información que puede ser utilizada para vulnerar un equipo o un sistema de información. Alguna de esta información se extrae a través de la revisión de la basura o por medio de la ingeniería social.

CISO: (Chief Information Security Officer). Es el director de seguridad de la información. Básicamente es un rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio.

MINTIC: El Ministerio de Tecnologías de la Información y las Comunicaciones es la entidad que se encarga de diseñar planes y políticas para que la tecnología llegue a todos los departamentos y ciudades de Colombia.

DANE: El Departamento Administrativo Nacional de Estadística es la entidad responsable de la planeación, levantamiento, procesamiento, análisis y difusión de las estadísticas oficiales de Colombia.

SMARTPHONE: El término smartphone pertenece a la lengua inglesa y hace referencia a aquello que, en nuestro idioma, conocemos como teléfono inteligente. Se trata de un teléfono celular (móvil) que ofrece prestaciones similares a las que brinda una computadora (ordenador) y que se destaca por su conectividad.

STREAMING: Tecnología que permite ver y oír contenidos que se transmiten desde internet u otra red sin tener que descargar previamente los datos al dispositivo desde el que se visualiza y oye el archivo.

Factor cultural en la seguridad de la información.

El factor humano es el punto más débil en la seguridad (Hernández, 2020) y uno de los medios por donde se origina la fuga o pérdida de la información generando de esta manera eventos e incidentes de seguridad dentro de las organizaciones. A su vez las personas se convierten en el elemento de falla más común en un sistema de seguridad (Lizarazo, 2020). Sin una correcta sensibilización acerca de las buenas prácticas para la seguridad de la información, es común encontrar claves escritas en libretas, debajo de los teclados, sobre el monitor del usuario, en el email, siendo mucho más vulnerables a la materialización de una amenaza cibernética.

El fraude informático es una realidad multidimensional que afecta a todos los participantes de la sociedad (SISTEMAS, 2016). Su capacidad de adaptación y reinvención le permite asumir distintas formas y aproximaciones. El gran reto lo tiene el usuario final, pues cada vez le es más difícil identificar lo que puede ser malware o no; puede instalar por ejemplo una simple aplicación para encender la linterna, pero esta aplicación a su vez le pide permiso para acceder a los contactos del teléfono, lo cual puede es absolutamente innecesario para el objetivo que fue instalado.

Es precisamente este desconocimiento por parte de estos usuarios, que son los usuarios que utilizan la tecnología para un fin específico, pero al ignorar el alcance que puede tener una aplicación específica con los permisos adecuados podría poner en riesgo la seguridad de la información de la red en la cual se encuentre dicho dispositivo. Esta debilidad es la que se pretende abordar en el artículo a través de la concienciación para la implementación y aplicación de buenas prácticas que permitan minimizar el riesgo a ataques cibernéticos.

Tendencias y antecedentes.

En la implementación y diseño de un sistema de gestión de riesgos de la seguridad de la información, tomando como referencia el estándar internacional ISO/IEC 27001:2013, se recopila información de los entes gubernamentales como MINTIC e información estadística de la empresa de seguridad ESET con respecto a las PYMES (figuras 1 y 2), encontrando cifras acerca de las empresas que aún no cuentan con la norma e inclusive no tienen políticas de seguridad claramente definidas para luego realizar una concienciación acerca de su importancia y contribuir de esta manera a reducir las vulnerabilidades y amenazas que afectan a estas organizaciones.

De hecho, las amenazas y riesgos más representativos son el factor humano, además se hallan amenazas relacionadas con la infraestructura en las empresas y errores de programación; para reducir estas amenazas y riesgos debemos adoptar normas y políticas que permitan salvaguardar la información, además presentar una serie de procesos que permitirán minimizar el riesgo.

Es precisamente en las PYMES donde se presentan más deficiencias graves en sus procesos de seguridad de la información y normatividad, en un análisis de riesgos se puede notar que los controles o son deficientes o no los hay, es posible definir controles de forma apropiada para mitigar el riesgo de una forma oportuna.

Una correcta gestión del riesgo en TI y su conocimiento por parte de la alta dirección de las organizaciones pueden ayudar a generar conciencia acerca del impacto de implementar esta norma y así motivar una cultura de seguridad que iniciará desde la alta dirección y descendiendo en orden jerárquico con el fin de sensibilizar a todos los colaboradores en la aplicación y cumplimiento de las políticas de seguridad que minimicen los riesgos previamente conocidos (Vergara, 2019).

A raíz del crecimiento tecnológico, las empresas están siendo cada vez más vulnerables a ataques informáticos, la evaluación para la implementación de la norma ISO 27001 precisamente pretende ayudar a identificar y mitigar los riesgos, partiendo de un inventario de activos que deben ser protegidos precisamente a través de la definición de políticas que deben ser aprobadas por la alta dirección de las compañías, buscando siempre conocer y controlar el riesgo.

Es precisamente la evaluación y gestión del riesgo la etapa inicial de este acercamiento. La alta dirección de las compañías suele ser ajenos a este tema y desconocer algunas de las grandes consecuencias que puede llevar un ataque informático. Se hace necesario entonces generar y promover algunas actividades que permitan este acercamiento como punto de entrada con el fin de lograr la concienciación acerca de la implementación de la norma.

Los avances de la tecnología en el mundo, el uso del internet que según Global Digital (López, 2019) puede darse como un gran indicador de crecimiento en el último año. En enero de 2019 el 57% de la población tenía acceso a internet. Aunque no todos lo usan ni el acceso es similar, es destacable cómo el 67% de la población del planeta utiliza un smartphone.

Solo durante 2018 el número de usuarios de internet creció un 9,1%. A este ritmo el mundo estará completamente conectado a finales de la próxima década.

El top 5 de las búsquedas por navegador a páginas web más visitadas a nivel mundial está formado por Google, YouTube, Facebook, Baidu (el equivalente a Google en China) y Wikipedia. Curiosamente, la búsqueda por voz coincide perfectamente con esta lista, aunque posiciona a continuación un gran número de páginas chinas como QQ, Temall o Taobao. Aun así, el idioma 'oficial' de internet es el inglés (54% de las webs) y el español sólo aparece representado en el 4,9%.

Con respecto al uso que le damos a este acceso a la red, la estadística presenta una amplia mayoría utilizando el video. El 92% de los usuarios ingresan a visualizar vídeos online, el 58% reproduce TV en streaming y el 30% juega a videojuegos en red. También se chatea mucho y, si se tiene que elegir un chat a nivel mundial, este es WhatsApp (López, 2019).

Todo esto demuestra la expansión y el alto crecimiento de las tecnologías a nivel mundial en todos los sectores y lugares del mundo, por ello la seguridad y privacidad deben considerarse unos aliados en esta época y al mismo tiempo generar conciencia y cultura en la seguridad de la información en todos los niveles, lo cual permite controlar el alcance de todos los dispositivos y elementos en un mundo intercomunicado, en este sentido la seguridad informática juega un papel fundamental y por ende la implementación de la norma ISO 27001.

La seguridad de la información en todo su sentido carga con la importancia de analizar los riesgos, amenazas, normas, políticas y buenas prácticas desde los esquemas normativos, pero desde el principio de generar cultura y concientización en las personas de acatar las normas y procedimientos que permitan tener un entorno seguro en los procesos digitales que se hacen dentro de las organizaciones.

La seguridad de la información y su relación con la economía.

Según cifras del Ministerio de Comercio, Industria y Turismo, las Pyme representan el 90% de las empresas de Colombia y generan el 80% de la empleabilidad nacional, aportando un porcentaje cercano al 50 % del Producto Interno Bruto (PIB) (Castilla, 2019).
La seguridad informática en las Pymes es mucho más que tener antivirus instalados en sus dispositivos. Es necesario contar con una serie de políticas y procedimientos para controlar los riesgos y mantener la privacidad, seguridad e integridad de sus datos.

El uso de la tecnología para apropiarse del patrimonio de terceros a través de clonación de tarjetas, vulneración y alteración de los sistemas informáticos para recibir transferencias electrónicas, entre muchas otras, son conductas cada vez más utilizadas. De acuerdo con el estudio de ciberdelito desarrollado por el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), el Phishing o robo de datos personales significa pérdidas anuales por unos US$93 mil millones de

dólares, y afecta a unos 2.500 bancos que operan en la región, en tanto los robos a cuentas de clientes suman otros US$761 millones de dólares. Asimismo, según cifras del estudio de McAfee Inc. y Science Applications International Corporation, 25% de las organizaciones han sufrido la paralización o retraso de una fusión o adquisición, o bien de la implementación de un nuevo producto o solución, a causa de una filtración de datos o por una amenaza creíble de filtración de datos (PORTAFOLIO, 2016).

Dado el impacto que puede acarrear un ataque cibernético, que inclusive puede tener implicaciones legales, se hace indispensable una adecuada identificación de riesgos y la implementación de políticas de seguridad de la información donde se involucren todos los miembros de la organización.

Actividades que promueven la concienciación en la seguridad de la información.

Con el fin de promover la concienciación en la seguridad de la información, el Instituto Nacional de Estándares y Tecnología - NIST lanzó una iniciativa que consiste en una guía para la construcción de programas de seguridad de tecnologías de la información y soporte efectivos.

De esta iniciativa se extraen los tres componentes para desarrollar esta cultura de seguridad de son:

- **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 notificando a la autoridad competente, velar por el respaldo de la información corporativa almacenada en sus equipos, etc.

- **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 hasta personales.

- **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 ISO 27001, con su respectiva certificación.

Se listan algunas técnicas corporativas que pueden utilizarse para crear conciencia en los usuarios (Vega Lizarazo, 2017):

1. 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 USB infectadas (con una advertencia y un consejo).

2. 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.

3. Consejos, tests (mini auditorías).

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

5. Desarrollar trivias.

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

7. Concursos basados en pictogramas.

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

9. Encuestas.

10. 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.

11. Precaución con el correo electrónico.

    a. Realice un análisis antes de abrir algún correo.

    b. Sospeche de los mensajes no esperados. Algunas veces vienen de conocidos, por lo tanto, analice primero. Si de alguna forma usted sospecha, se aconseja llamar por teléfono al remitente para asegurarse.

    c. 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.

    d. 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 bajo el protocolo https.

    e. Analizar los adjuntos en los correos, aunque provengan de fuente conocida. Cabe la posibilidad de que sean maliciosos. Ante cualquier sospecha, llame al remitente.

    f. 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.

    g. Generales

        i. 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 puede haber documentos confidenciales que pueden ser aprovechados por los ciberdelincuentes. A esta técnica se conoce como “Dumpster Diving”.

ii. Frente a la evidencia de suplantación de identidad, denuncie y revise el perfil para minimizar el riesgo de acceso a personas desconocidas.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. Whatsapp no es totalmente segura, por lo que se aconseja no enviar información sensible por ese medio.

viii. Si desea compartir documentos, se aconseja el uso de dropbox o una plataforma similar.

ix. 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.

x. 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.

xi. 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.

xii. 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.

xiii. 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.

xiv. 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.

xv. 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.

xvi. 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 mente 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.

xvii. 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.

xviii. Los jugadores también se encuentran expuestos al spam y al phishing. 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.

Conclusiones

El crecimiento que ha tenido las TIC en Latinoamérica, especialmente en Colombia, gracias al apoyo del Ministerio de las Telecomunicaciones, donde se reconoce a las TIC como la mejor herramienta que tienen los países latinoamericanos para crear empleo y erradicar la pobreza (MINTIC, 2015), hacen indispensable la concienciación en la seguridad de la información, reconociendo el factor humano como el punto más débil en este aspecto.

La seguridad de la información es un deber de todos, tanto empresas, empleados y usuarios de cualquier dispositivo tecnológico. Es importante reconocer los riesgos involucrados en la seguridad de la información con el fin de formalizar la creación y aplicación de normas. Precisamente la norma

ISO 27001 reconoce como uno de los factores de éxito en la implementación y cumplimiento la concienciación del empleado y del usuario por la seguridad de la información.

Para facilitar esta concienciación se presentan unas actividades que ayudarán a los usuarios a cumplir con los estándares de seguridad, desde un punto de vista práctico, tomando algunas precauciones en el manejo de la información inclusive a nivel personal (publicación en redes sociales, información intercambiada a través del celular, entre otros). Desde el punto de vista empresarial, se sigue afianzando la transformación de paradigmas de la seguridad de la información en las organizaciones y su relación con los directivos de estas, las juntas directivas cada vez están más involucradas y participan en la toma de decisiones.

Culturalmente las organizaciones en Colombia han sido muy reactivas en temas de seguridad, tal como se evidencia en las tendencias y estadísticas de los últimos años en los sectores tecnología y seguridad de la información, donde un alto porcentaje de las empresas aún no cuentan con políticas de seguridad de la información claramente definidas, lo que significa que no han dimensionado los riesgos a las que están expuestas si se materializa una amenaza cibernética. A raíz del crecimiento de los ataques cibernéticos, las organizaciones empiezan a despertar conciencia sobre la protección de su activo más importante, la información, y por eso ahora encontramos CISO's dedicados al análisis de riesgos y su mitigación.

Es fundamental entonces, en armonía con la alta dirección, diseñar y mantener un programa de toma de conciencia que incluya actividades como campañas, folletos y boletines de noticias que fortalezcan los procesos y aporte en la planificación de los acuerdos de los roles de los empleados en la organización y donde se considere pertinente, proyectar en el tiempo y hacerlas con regularidad para que se repitan y también sean adoptadas por lo nuevos empleados y contratistas (GD Beltrán, DF Mosquera, 2016). Este programa se debe actualizar frecuentemente, de manera que siempre esté alineado con las políticas y procedimientos de la organización, construido con base a las lecciones aprendidas de incidentes de seguridad de la información propios y ajenos. Es importante que tanto los directivos como los empleados comprendan el objetivo de la seguridad de la información y el impacto potencial, positivo y negativo que tiene su propio comportamiento para la organización.

Referencias

Cámara Colombiana de Informática y Telecomunicaciones CCIT (2019). Tendencias Cibercrimen Colombia 2019-2019. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Castilla, José David. Gobierno presentará ley para proteger a las Pyme, como sucedió en Chile (2019). La República. Disponible en https://www.larepublica.co/empresas/gobierno-presentara-propuesta-para-revolucionar-el-sector-de-las-pyme-2811313

GD Beltrán Constaín, DF Mosquera Betancourt (2016). Diseño e implementación de una aplicación web orientada a generar conciencia y cultura sobre la seguridad de la información. Repositorio Institucional Universidad Piloto de Colombia. Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2708/Trabajo%20de%20grado3385.pdf?sequence=1&isAllowed=y

Hernández Otalora, Sandra Janneth (2019). Cultura en Seguridad de la Información. Repositorio Institucional Universidad Piloto de Colombia. Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6436/Art%c3%adculo_Cultura_Seguridad_de_la_Informaci%c3%b3n.pdf?sequence=1&isAllowed=y

López, Daniel (2019). ¿Cómo es el acceso a internet en el mundo?. Disponible en http://blog.orange.es/noticias/acceso-internet-mundo

MINTIC (2015). Cómo internet conecta y transforma a Colombia. Disponible en https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Blogs/9296:Como-Internet-conecta-y-transforma-a-Colombia

PORTAFOLIO. Pérdidas delitos informáticos, [Citado el 02 de Abril de 2016] Disponible en http://www.portafolio.co/economia/finanzas/perdidas-delitos-informaticos-suman-us-93-000-millones-91548

SISTEMAS. Fraude informático: viejos trucos, nuevos entornos (2016). ACIS. Disponible en https://acis.org.co/archivos/Revista/Sistemasedicion139.pdf

Vega Lizarazo, César (2017). Concienciación en Seguridad de la Información. Repositorio Institucional Universidad Piloto de Colombia. Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2667/00003624.pdf?sequence=1

Vergara Torres, O. H. (2019). Mejorando la implantación de la ISO 27001 en las organizaciones. Repositorio Institucional Universidad Piloto de Colombia. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/6178