Importancia de la capacitación y concientización de los empleados respecto a la seguridad de la información como un factor clave de éxito en la prevención del fraude informático

Luceida Rendón Pinzón

Código: 2501152

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE CIENCIAS ECONÓMICAS

ESPECIALIZACIÓN EN CONTROL INTERNO

BOGOTA D.C.

2020

TABLA DE CONTENIDO

1 **INTRODUCCIÓN** 1
2 Pregunta problema 2
2.1 Objetivo general 2
2.2 Objetivos específicos 2
3 **MARCOS DE REFERENCIA** 3
3.1 **MARCO TEÓRICO** 3
3.1.2 ¿Como esta Colombia en términos de ciberseguridad? 4
3.1.3 La seguridad en términos generales 7
3.1.4 Generalidades, norma ISO 27001 8
3.1.5 Sobre la capacitación y desarrollo de personal 9
3.2 **MARCO CONCEPTUAL** 11
3.3 **MARCO LEGAL** 13
4 Importancia de la capacitación y concientización de los empleados respecto a la seguridad de la información como un factor clave de éxito en la prevención del fraude informático 14
5 **CONCLUSIONES** 25
6 **REFERENCIA BIBLIOGRÁFICA** 26

LISTA DE TABLAS

Tabla 1 Ciclo PHVA, Norma ISO 27001 8
Tabla 2 Descripción de la tipología de delitos informáticos 19
Tabla 3 Fases de la norma ISO 27001 20
Tabla 4 Modelo de plan de capacitación 23

LISTA DE FIGURAS

Figura 1 Cargos relacionados con seguridad de la información 4
Figura 2 Presupuesto invertido en seguridad de la información 5
Figura 3 Motivos más comunes por los que no se denuncia 6
Figura 4 Tipos de riesgo en la seguridad de la información 9
Figura 5 Proceso de capacitación 10
Figura 6 Principales consecuencias de los ciberataques 15
Figura 7 Principales modalidades de ciberdelitos en Colombia 16
Figura 8 Temas que debe contemplar la capacitación en seguridad de la información 22

RESUMEN

La información siempre ha sido importante para la toma de decisiones. Ya no solo quien tiene el conocimiento tiene el poder, sino además quien tiene la información. Las grandes organizaciones han entendido el valor del dato como un activo factor clave de éxito y muchas veces, clave para su permanencia en el mercado. Es así, como a finales del siglo XX surgió abundante normatividad en términos de seguridad y cumbres mundiales lideradas por Naciones Unidas que propendían por el acceso responsable a la información y la reducción de las brechas de acceso a internet como un aspecto de crecimiento y desarrollo. En países en vía de desarrollo como Colombia, la inversión en ciberseguridad es muy baja comparada con países europeos, por ejemplo, no obstante, el sector que más invierte es el sector financiero y de telecomunicaciones. En este ensayo se describen algunos de los principales ciberataques de los cuales la gran mayoría pueden ser evitados con adecuada capacitación al personal, por ello se describe la importancia de la capacitación en temas concernientes a la seguridad de la información y además se plantea la importancia de que las grandes organizaciones implementen la norma ISO 27001 como una de las formas de salvaguardar la información y prevenir los riesgos asociados a la vulnerabilidad de la misma.

PALABRAS CLAVE

Autenticación, Capacitación, Control de acceso, Ingeniería social, Información, Seguridad de la información, Riesgo, Sistemas de información, Usuarios, Virus informático, Vulnerabilidad.

ABSTRACT

Information has always been important for decision making. Not only who has the knowledge has the power, but also who has the information. Large organizations have understood the value of data as an active key factor for success and, many times, key to their permanence in the market. Thus, at the end of the 20th century, abundant regulations emerged in terms of security and world summits led by the United Nations that promoted responsible access to information and the reduction of internet access gaps as an aspect of growth and development. In developing countries like Colombia, investment in cybersecurity is very low compared to European countries, for example, however, the sector that invests the most is the financial and telecommunications sectors. This essay describes some of the main cyberattacks of which the vast majority can be avoided with adequate staff training, for this reason, the importance of training on issues concerning information security is described and also the importance of that large organizations implements the ISO 27001 standard as one of the ways to safeguard information and prevent risks associated with its vulnerability.

KEYWORDS

Authentication, Training, Access control, Social engineering, Information, Information security, Risk, Information systems, Users, Computer virus, Vulnerability.

1. INTRODUCCIÓN

Las organizaciones se enfrentan constantemente a cambios y eventos externos que ponen en riesgo su operación, su permanencia en el mercado y hasta su existencia misma. Claramente existen eventos de riesgo que posiblemente jamás serán contemplados o si están contemplados, muchas veces el impacto de los mismos está mal calculado. Por ejemplo, se podría inferir que muy pocas organizaciones habrían previsto que un enemigo invisible como lo es un virus, pondría en jaque la estabilidad económica mundial y justamente esta situación particular hizo que ahora más que nunca se generara una dependencia tecnológica en varios ámbitos: de consumo, de educación, de trabajo, de relacionamiento social entre otros, que han incrementado ostensiblemente la modalidad de riesgo de fraude informático.

Existe amplia teoría y normatividad referente a la seguridad de la información, no obstante, una de las más completas es la ISO 27001 ya que a través de las directrices que aporta, cualquier empresa puede proteger el dato, pues las personas y las empresas han comprendido la relevancia de proteger la información como uno de los activos más importantes y entienden que, a causa de la mala gestión se pierde, se altera o se vulnera su seguridad ocasionando el colapso del negocio.

En este trabajo se pretende mostrar por qué es de vital importancia la capacitación y la concientización que se haga a los empleados en cuanto a seguridad de la información se refiere, volviéndose un factor clave de éxito en la prevención de delitos de fraude informático.

2. PREGUNTA PROBLEMA

¿Por qué la falta de capacitación y concientización de los empleados respecto a la seguridad de la información es un factor clave de éxito en la prevención del fraude informático en las organizaciones?

2.1 OBJETIVO GENERAL

Analizar la incidencia que tiene la capacitación y la concientización de los empleados respecto a la seguridad de la información, como factor clave de éxito en la prevención de la modalidad de riesgo de fraude informático en las organizaciones.

2.2 OBJETIVOS ESPECÍFICOS

- Describir las principales formas en que se atenta contra la seguridad de la información y su impacto en las organizaciones.

- Considerar las prácticas propuestas en la norma ISO 27001, para crear y mantener los controles suficientes, necesarios, apropiados y proteger la información.

- Describir de qué manera la capacitación y la concientización de los empleados coadyuva en la prevención de fraude informático.

3. MARCOS DE REFERENCIA

3.1 MARCO TEÓRICO

La seguridad de la información ha sufrido profundos cambios en los últimos años, y esto se debe al crecimiento exponencial que ha tenido el uso de internet en todas las actividades cotidianas de las empresas y la sociedad en general. En los años 80 y 90 la seguridad de la información se concentraba en la protección de los equipos como tal, es decir del hardware, los ordenadores y los sistemas operativos. De otra parte, la seguridad se centraba en la protección contra los virus, algo bastante lógico si se tiene en cuenta que para esa época no se contaba con un volumen tan amplio de accesibilidad a internet, y máxime si se tiene en cuenta que la llegada del celular con datos, facilitó el acceso a la información por la enorme facilidad de tenerlo en cualquier parte.

Así mismo, acciones como las planteadas en el Artículo 2 de la Ley 1341 de 2009, en sus principios orientadores la prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones, mencionando que el Estado y en general el sector de tecnologías de la información deben "priorizar el acceso y uso a las Tecnologías de la Información y las Comunicaciones en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación, los contenidos y la competitividad". Este tipo de legislaciones ha incrementado ostensiblemente el acceso a internet de la sociedad en general, facilitando el intercambio comercial y dinamizando la economía entre otros.

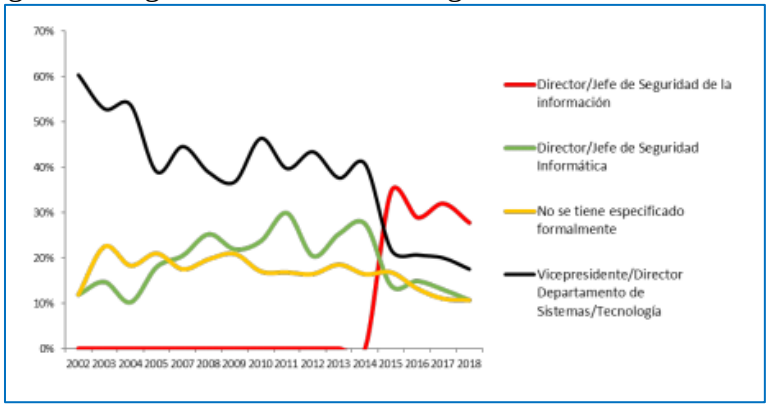
De otra parte, aunque existen variedad de soportes documentales diferentes, la dinámica de la tecnología ha modificado la manera de presentar y almacenar la información y por ello la mayoría de la información de las empresas se encuentra sistematizada a través de herramientas de tecnologías de la información.

3.1.2 ¿Como esta Colombia en términos de ciberseguridad?

De acuerdo a la Asociación Colombiana de Ingenieros de Sistemas – ACIS, entidad sin ánimo de lucro que realizo un estudio juicioso sobre la evaluación de las tendencias en lo que a seguridad de la información se refiere para establecer como las empresas han actuado frente al reto de la seguridad de la información. Para ello esta entidad elaboro una encuesta de 40 preguntas agrupadas en categorías de fallas de seguridad, herramientas y prácticas de seguridad, políticas de seguridad, presupuestos, temas emergentes y capital intelectual. Este estudio de seguimiento en el que se consolido la información de 18 años arrojo los siguientes resultados sobre la realidad de la seguridad de la información en Colombia.

La industria colombiana y la Ciberseguridad: Los sectores Financiero, Gobierno, Educación, Consultoría Especializada y las Telecomunicaciones, son los más entusiasmados en entender y adelantar acciones en materia de seguridad y control. Cargos como el de Oficial de Seguridad de la información o como el cargo de Director de Seguridad de la Información, son cargos nuevos que se han creados para hacer frente a la protección de datos. De igual forma se evidencia que en Colombia desde el año 2002 se ha hecho énfasis en cargos relacionados con seguridad informática. Como se puede apreciar en la siguiente grafica los cargos relacionados con seguridad de la información han crecido en los últimos años:

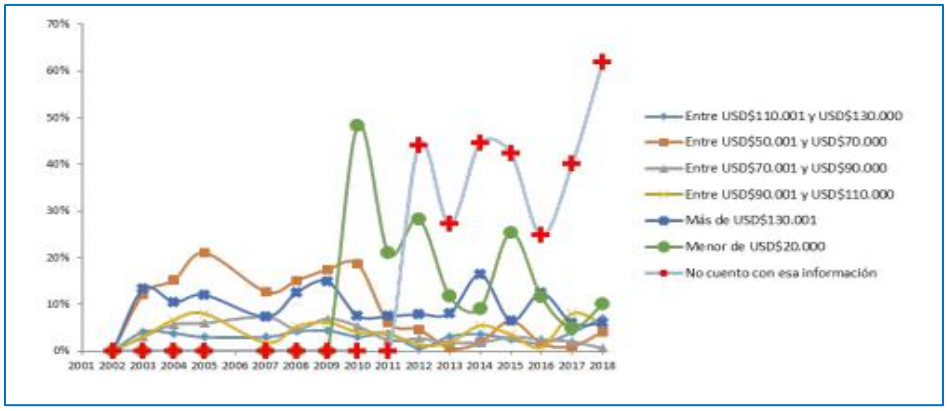
Figura 1: cargos relacionados con seguridad de la información.



Fuente: Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 – 2018.

Inversiones y Presupuestos en Ciberseguridad en Colombia: Las empresas hacen inversiones de acuerdo a su realidad, que equivale más o menos al 2% del presupuesto global, siendo el sector financiero el que más invierte en relación a la seguridad de la información, lo cual es bastante obvio ya que es el sector que más ciberataques recibe. En todo caso se observa una tendencia a seguir asignando presupuesto por este concepto se sitúa por debajo de los 50 mil dólares para las empresas medianas y para las empresas grandes se espera que sea de 100 mil dólares, ambos destinados en su mayoría a consecución y mantenimiento de las tecnologías de seguridad de la información. La siguiente grafica ilustra la inversión:

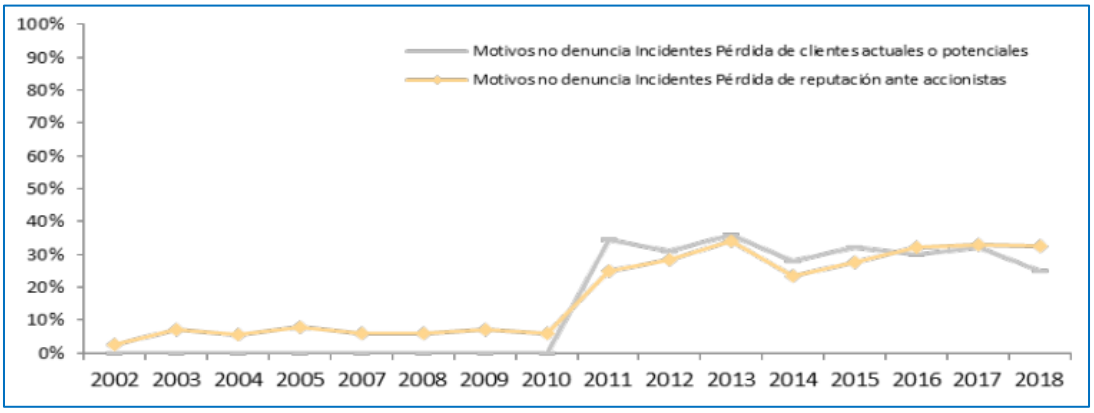
Figura 2: presupuesto invertido en seguridad de la información.



Fuente: Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 – 2018.

Así mismo se identificó que es a los directivos a quienes se les notifica primero cuando hay un incidente de seguridad de la información y también se evidencio que muchas veces no se denuncian estos incidentes a las autoridades competentes para no incurrir en temas de mala reputación de las compañías. Otros estudios demuestran que no denuncian por la posibilidad de perder sus clientes actuales o potenciales, como lo muestra la siguiente gráfica:

Figura 3: motivos más comunes por los que no se denuncia.



Fuente: Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 – 2018.

Gobierno y Gestión de la Ciberseguridad en las empresas colombianas: La gran mayoría de las empresas colombianas tienen definidas las políticas en materia de seguridad y tienen prácticas de gestión de riesgos de seguridad con crecimiento constante.

Finalmente, el estudio realizado por la Asociación Colombiana de Ingenieros de Sistemas – ACIS, muestra que el tema de seguridad de la información en las empresas colombianas sigue siendo un tema de los niveles operativos y tácticos. Un tema que parte más del área de tecnología directamente y no desde el nivel estratégico. Así mismo el país cada vez tiene mayor regulación en términos de seguridad de la información y la alineación de las organizaciones con estas buenas prácticas de aseguramiento que sea coherente con el contexto internacional. De todos modos, es necesario desarrollar la capacidad de anticipación de nuevas amenazas digitales.

J Cano., Almanza A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 – 2018.

3.1.3 La seguridad en términos generales.

En términos generales se puede decir que la seguridad es la ausencia de riesgos frente a algo que de por si se considere confiable. Se pueden mencionar varios tipos de seguridad, como por ejemplo la seguridad ambiental, económica, sanitaria, personal, entre otras. Guerrero J. (2017). En su Manual de Políticas y Seguridad de la información menciona algunos de los principales tipos de ataques y atacantes, así:

- Phishing (Pesca): Es el acto de pescar usuarios mediante señuelos y de este modo obtener información financiera y contraseñas para intentar adquirir información confidencial de forma fraudulenta.
- Malware (Software malicioso): Es un tipo de software que tiene como objetivo infiltrarse o dañar un Pc sin el consentimiento de su dueño.
- Virus: Es un software que se copia por sí mismo, infecta un Pc, se propaga dentro de todos los archivos y luego se copia de Pc a Pc.
- Gusano: Es un software cuyo único cometido radica en pasar de Pc en Pc a través de redes informáticas en forma automática sin la intervención de ningún usuario.
- Caballo de Troya: Es un software inocente que contiene códigos escondidos que permiten la modificación no autorizada y la explotación o destrucción de la información.
- Cracker: individuos que se dedican a desproteger programas, como evitar tener que pagar las licencias de los mismos, comprar una copia y usarla en 20 puestos simultáneamente.
- Hacker: Persona que es capaz de eludir los sistemas de seguridad de un computador para acceder a la información que contiene ya sea con fines maléficos o benéficos.
- Hacktivista: Persona especialista que se moviliza con conocimientos informáticos contra la mundialización, las multinacionales y en defensa de los internautas.

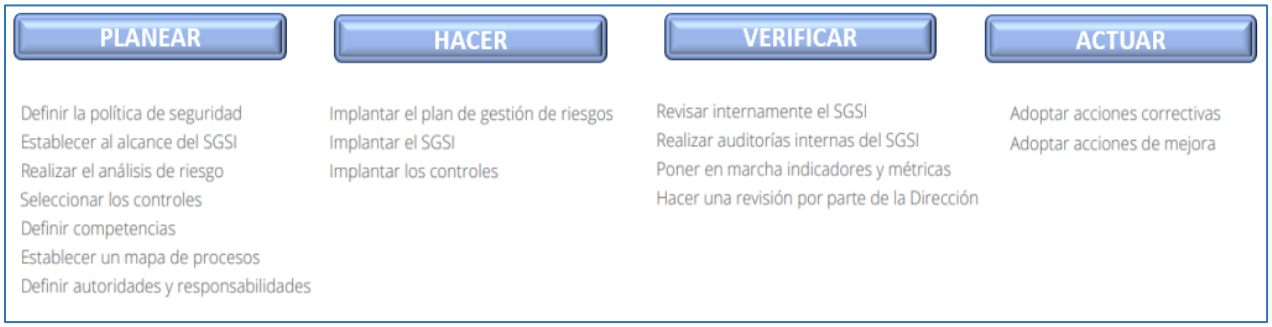
- Ankle-Biter: Son personas que indagan por la red ya sea por diversión o pasa tiempo para realizar ataques sólo para divertirse, sin importar quién los recibe.

Guerrero J. (2017). Manual de Políticas y Seguridad de la información. IDIGER.

3.1.4 Generalidades, norma ISO 27001.

El Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001, es una herramienta de mejora continua que permite evaluar todo tipo de riesgos y amenazas que pudiesen colocar en peligro la seguridad de la información de las organizaciones. Esta norma también permite generar controles y estrategias adecuadas para minimizar o eliminar dichos peligros. Además, como sucede con casi todas las normas ISO esta norma está enfocada en el ciclo de mejora continua o Deming, es decir está basado en el ciclo PHVA. Este ciclo planteado en esta norma se divide en los siguientes pasos y cada uno tiene una serie de acciones, así:

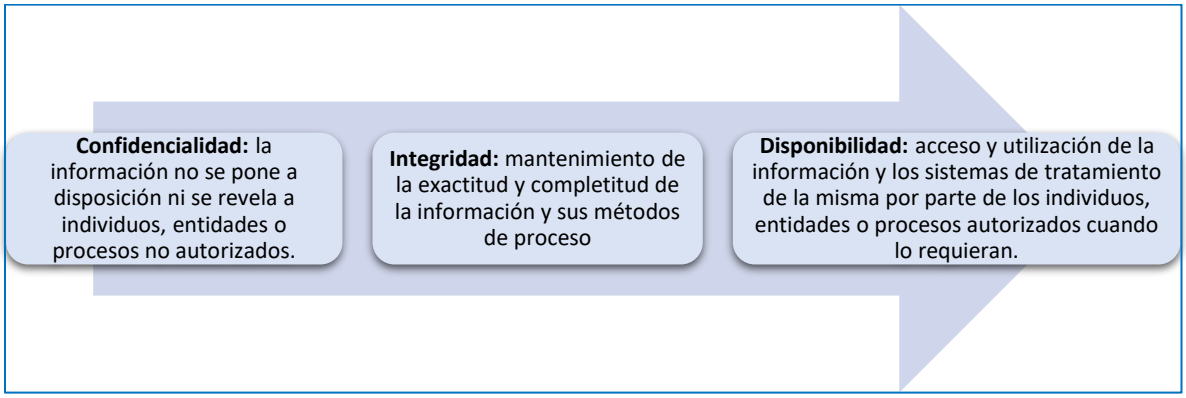
Tabla 1: Ciclo PHVA, Norma ISO 27001.



Fuente: Elaboración propia a partir de la norma ISO 27001.

Así mismo, es importante mencionar que el principal propósito de la norma es proporcionar protección a la información sensible, la cual puede ser información sobre empleados, clientes o proveedores que se puede ver afectada por tipos de riesgos que se pueden agrupar en tres categorías a saber:

Figura 4: tipos de riesgo en la seguridad de la información.



Fuente: Elaboración propia a partir de la norma ISO 27001.

La versión de la norma ISO 27001 trae un anexo SL, el cual contiene 10 cláusulas que sigue la misma estructura común que otras normas ISO, y estos no se puede cambiar, o eliminar. Además, para cumplir con sesta norma la organización debe implementar una serie de controles o dar una explicación del por qué no se implementan.

3.1.5 Sobre la capacitación y desarrollo de personal.

La capacitación entendida como un proceso esencial dentro de la administración del talento humano es de vital importancia porque siempre buscar mejorar las habilidades y ampliar los conocimientos y hasta las actitudes del personal. La capacitación y desarrollo "(…) deben concebirse precisamente como modelos de educación a través de los cuales es necesario primero, formar una cultura de identidad empresarial basada en los valores sociales de productividad y calidad en las tareas laborales" (Aguilar A., 2004, p. 16).

En tal sentido Aguilar A, también expone que la capacitación es importante para el cumplimiento de las metas de las organizaciones en tanto el modelo de educación que se diseñe este orientado a la cultura de la productividad y en la que se involucren valores de calidad, eficacia, eficacia y ahorro. Esto será logrado a treves de un plan de capacitación integral, donde

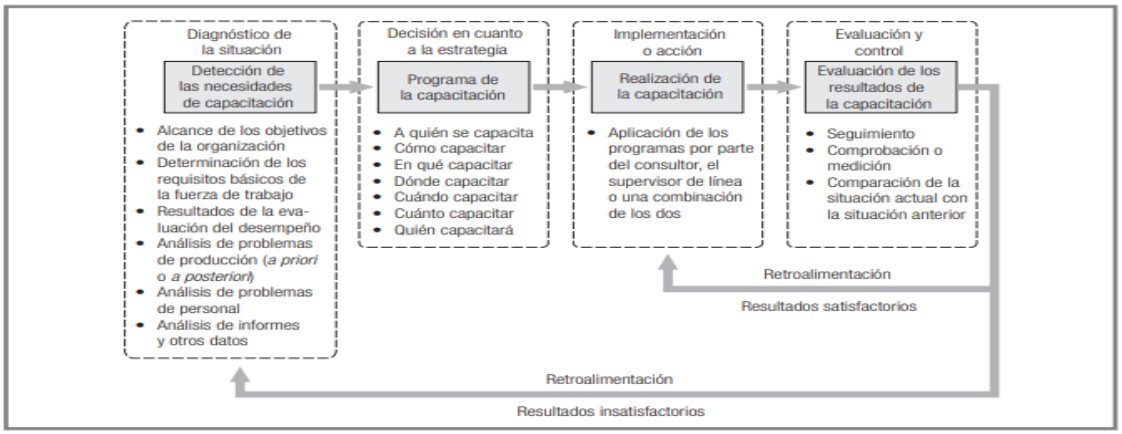
no solo se tenga en cuenta aspectos que apunten al hacer, sino además aquellos que involucren el ser, como dimensión fundamental que permite mirar el empleado holísticamente.

Vemos pues que la formación no solo redunda en beneficios para el empresario, sino que además aporta al crecimiento de los empleados, pues por un lado facilita el mejor desarrollo de sus tareas lo cual les hace sentir más tranquilos y el patrono se ve beneficiado al reducir los errores y claramente los riesgos que se deriven de estos.

De otra parte, según Chiavenato I. (2007), el contenido de la capacitación puede incluir cuatro formas de cambiar el comportamiento: 1) la transmisión de la información, como manera de brindar un conjunto de conocimientos.2) desarrollo de habilidades, sobre todo conocimientos relacionados con el desempeño del cargo. 3) desarrollo de modificación de actitudes, especialmente actitudes negativas con los compañeros de trabajo. 4) desarrollo de conceptos, para elevar el desarrollo de las ideas.

Chiavenato I. (2007) también presenta como debe ser el proceso de capacitación:

Figura 5: Proceso de capacitación.



Fuente: Chiavenato I. (2007).

Finalmente, la capacitación es una responsabilidad administrativa y esta debe estar articulada con las necesidades de la organización y apuntar a mejorar las condiciones de los empleados y debe entenderse como una inversión y no como un gasto, porque lo que el empleado aprenda redundará en beneficios para la organización y se verá traducido en un mejor hacer y mejor ser.

3.2 MARCO CONCEPTUAL

Romero M., Figueroa G., Vera D., Alava J., Parrales G., Alava C., Murillo A., Castillo M. (2018), nos dan las siguientes definiciones:

- Seguridad de la información: la seguridad informática es la disciplina encargada de planear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro confiable y sobre todo que tenga disponibilidad.
- Información: es considerada como el oro de la seguridad informática, ya que es lo que de desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo.
- Usuarios: son considerados como el eslabón más débil en la cadena, ya que las personas son imposibles de controlar. En muchos casos el sistema debe de protegerse del mismo usuario.
- Virus informático: es un programa desarrollado en un determinado lenguaje de programación con el objeto de infectar uno o varios programas informáticos.
- Vulnerabilidad: es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso.

- Ingeniería social: es cualquier acto que induce a una persona a realizar una acción que puede, o no, ser de su mejor interés.
- Riesgo: es la posibilidad de ocurrencia de un daño. Está compuesto por amenazas y vulnerabilidades.

Así mismo en la norma ISO 27001, encontramos otras definiciones importantes en materia de seguridad de la información:

- Autenticación: Garantía de que una característica reivindicada de una entidad es correcta. Es un proceso que garantiza y confirma la identidad de un usuario.
- Gobernanza de seguridad de la información: Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas.
- Sistemas de información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.
- Control de acceso: medios para garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.

Finalmente, Chiavenato I. (2007), nos refiere las siguientes definiciones:

- Capacitación: entraña la transmisión de conocimientos específicos relativos al trabajo, actitudes frente a aspectos de la organización, de la tarea y del ambiente, así como desarrollo de habilidades y competencias.

3.3 MARCO LEGAL

- Congreso de la Republica (05-enero-2009). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos”.

- Congreso de la Republica (30-julio-2009) Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Artículo 4.

- Congreso de la Republica. (17-octubre-2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

4. Importancia de la capacitación y concientización de los empleados respecto a la seguridad de la información como un factor clave de éxito en la prevención del fraude informático

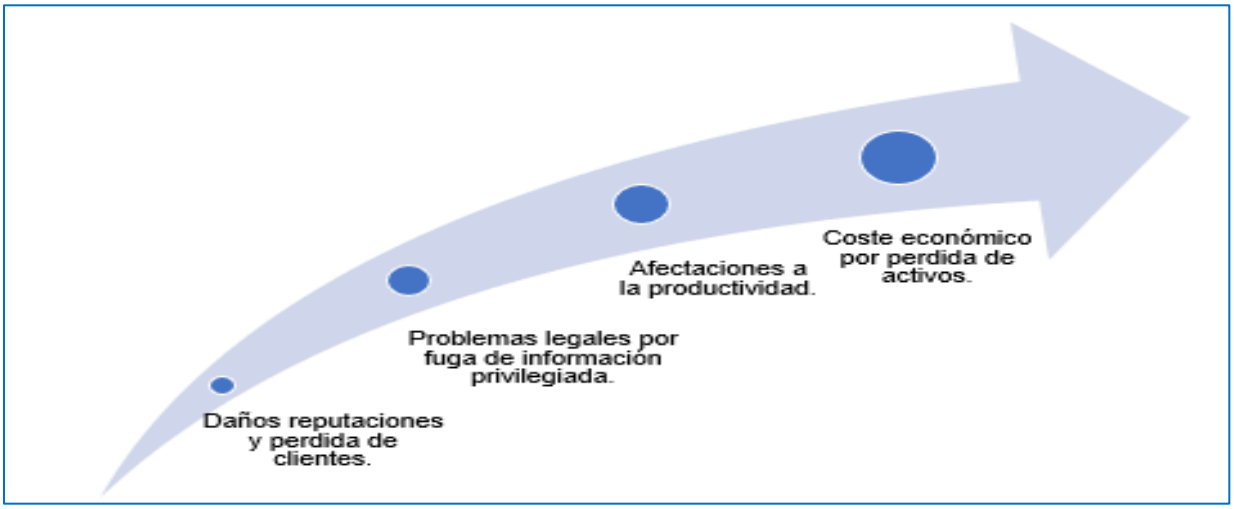
La seguridad de la información ha cobrado una importancia preponderante, debido a la facilidad de producir datos en masa, como resultado del alto nivel de conectividad, tanto que la seguridad de la información en muchos países se ha vuelto un tema nacional. En la era de la información digital las grandes esferas del poder saben que "quien tiene la información tiene el poder" el gran dilema es ¿cómo librar la información valiosa para que no caiga en manos maliciosas? Para ello es clave guna adecuada gestión de riesgos inherentes a la administración de la información. La sociedad de la información está evolucionando estratosféricamente y esto ha modificado la manera de trabajar en las organizaciones, no solo por el volumen de información, sino que además se ha convertido en un gran desafío asegurar la gestión de la información.

De otra parte, es importe entender cuando se atenta contra la seguridad de la información, ¿cuál es su impacto en las organizaciones? Las empresas guardan registros de las transacciones financieras, de los proyectos importantes, información confidencial de los clientes e información importante relativa al core del negocio. En cualquier caso, si esta información cae en manos indebidas puede generar problemas de gran alcance. Por ejemplo, si grandes volúmenes de información de clientes caen en manos de la competencia esta puede utilizarla para determinar patrones de consumo, frecuencia de compra y robar los clientes más determinantes para la sostenibilidad de la empresa. Así mismo si se fuga la información de las transacciones bancarias pueden hurtar dinero de las cuentas de la empresa y de los clientes incluso. Por motivos como estos es que el robo de la información de las empresas se ha convertido en un negocio inmensamente lucrativo. Una de las mayores consecuencias son las pérdidas financieras que

muchas veces se traducen en la desaparición de las empresas. Un virus por ejemplo como el ransomware que se instala en la red interna de las empresas, explora donde hay falta de seguridad y descifra todos los archivos posibles, para luego hacer un secuestro de información por el que exigen para su devolución. Cuando los ataques son muy grandes las empresas pueden perder acceso a todos los sistemas, lo que genera una parálisis literal en la operación y si a ello se suma que no hayan backups de información ni reglas claras de continuidad del negocio, pues el trauma es mayor debido a que puede ser muy demorado el restablecimiento de los sistemas de información. Los datos de las empresas son indispensables para la ejecución de las operaciones lo que muchas veces deriva en grandes pérdidas financieras e incluso reputacional, o acaso ¿qué cliente va a seguir vinculado a una empresa donde se evidencia perdidas de algún tipo como consecuencia de la falta de cuidado y protección de la información?

Algunas de las principales consecuencias de los ciberataques en los que se vulnera la información la encontramos en la siguiente imagen:

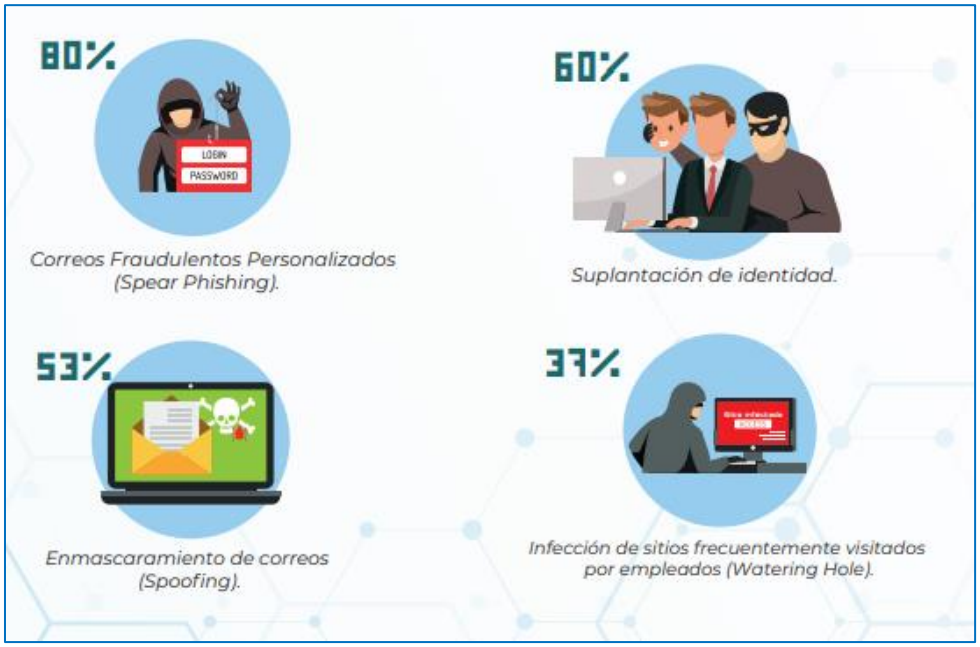
Figura 6: principales consecuencias de los ciberataques.



Fuente: Elaboración Propia.

Un informe sobre Tendencias Cibercrimen Colombia 2019-2020 presentado por el Tanque de Análisis y Creatividad de las TIC - TicTac de la CCIT y su programa SAFE en asocio con la Policía Nacional - Centro Cibernético Policial, presento algunas de las siguientes cifras y modalidades de los ciberdelitos en Colombia. Este estudio se hizo a partir de 15.948 denuncias al Centro Cibernético Policial CECIP y como se aprecia en el siguiente gráfico, muchos de estos tipos de engaños se pueden prevenir con una adecuada gestión de usuarios y accesos.

Figura 7: principales modalidades de ciberdelitos en Colombia.



Fuente: Tendencia cibercrimen Colombia 2019-2020.

No basta con conocer las modalidades de cibercrimen si no se busca la forma adecuada de contrarrestarlo y para ello es de vital importancia que los empleados tengan buenas prácticas en el manejo de la información sensible. Como se puede ver apreciar la modalidad de correo fraudulentos representa el 80% y prevenir esta modalidad de ataque es posible si se hace un adecuado entrenamiento y capacitación a los empleados para que aprendan a identificar correos

de dudosa procedencia. Respecto a la suplantación de identidad es necesario tener cuidado de no revelar las claves de accesos ni los usuarios incluso a personas de la misma empresa.

En muchas ocasiones el fraude en las empresas surge por la falta de cuidado en la manipulación de la información, ya que son los mismos usuarios quienes por desconocimiento o falta de cautela “abren la puerta” al delito informático. Martha R., Figueroa G., Vera D., Álava J., Parrales G. Álava C., Murillo L., Castillo M. (2018), mencionan respecto que los usuarios que “Son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de contralar, un usuario puede un día cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo” (p. 14).

En efecto, los usuarios deben ser considerados como la parte más frágil ya que todas las actividades realizadas por personas son susceptibles de errores, y si bien es cierto hay muchas actividades que tienden a desaparecer porque están siendo realizadas por maquinas, lo cierto es que la sistematización misma es controlada por humanos y el riesgo de error siempre estará presente.

Para ilustrar un poco más la importancia de la protección de la información, se revisará el caso de lo ocurrido a mediados de 2014 en la empresa WXYZ, donde ocurrió un desangre pensional por cerca de 5 mil millones de pesos, el equivalente a la pensión de aproximadamente cinco mil pensiones con salario mínimo. Todo ocurrió por un descuido en el que una trabajadora prestó su computador a una compañera de trabajo para que esta redactara su carta de renuncia a la empresa WXYZ y no se percató de cerrar los programas con los que se administraban las historias laborales, que son la base para el reconocimiento pensional. Entonces la funcionaria que estaba redactando la carta aprovecho para cambiar la fecha de ingreso a laborar de una persona lo cual le implico ganarse tres años de ahorro pensional. Esa simple acción logro poner al

descubierto una gran modalidad de fraude que se producía por varias personas dentro de la empresa. Con el tiempo la Unidad de Delitos Informáticos recolecto información suficiente que termino con la captura de 11 contratistas que habían beneficiado alrededor de 174 personas a quienes se les otorgo pensión sin cumplir con el requisito de las semanas cotizadas. Estas personas eran extrabajadores de otra empresa de pensiones quienes ya contaban con el conocimiento suficiente en temas de reconocimiento pensional lo cual fue aprovechado por la empresa WXYZ. Esta red delincuencial cobraba entre 10 y 100 millones de pesos por modificar las historias laborales de los afiliados. En casos tan descarados acreditaban 20 años laborados (1.100 semanas), a personas que nunca en su vida habían cotizado a sistema de pensiones. Finalmente, "el ente acusador les imputó los delitos de estafa agravada, acceso abusivo a un sistema informático, falsedad material en documento público, fraude procesal, violación de los datos personales y concierto para delinquir. Acusaciones aceptadas por dos de los sindicados". (Revista Semana, 6/8/2017).

El caso anterior tiene dos componentes: uno es el uso indebido de la información concerniente a las claves y accesos a los aplicativos que contienen información sensible y de alto valor. El otro refleja el caso de problemas en la infraestructura en términos de seguridad tanto de las personas que ingresan como de la vulnerabilidad misma de los sistemas de información.

De otro lado las imputaciones realizadas se encuentran reglamentadas en la Ley 1273 de 2009, que menciona en su Capítulos 1 y 2, de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y de los atentados informáticos y otras infracciones, lo siguiente:

Tabla 2: descripción de la tipología de delitos informáticos.

Delito	Descripcion
Acceso abusivo a un sistema informático	El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo
Daño Informático.	El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos
Violación de datos personales.	El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes
Hurto por medios informáticos y semejantes	El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos

Fuente: Elaboración propia.

De la misma manera, la Ley 1581 de 2012 en el Articulo 4, sobre los Principios para el tratamiento de datos personales, trata del principio de seguridad como se administrar los datos “con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento” y respecto el principio de confidencialidad indicando que “todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento”. Por tanto, en el caso que se expuso de la empresa WXYZ se evidencia la falta grave en el manejo de la información, ya que el desconocimiento o falta de prevención de la persona que prestó la clave del computador, por partir de la buena fe, no la exonera de la culpa ante la ley.

Del caso anterior queda la gran importancia que tiene la correcta gestión de privilegios, en términos de seguridad de la información y sobre este aspecto Martha R., Figueroa G., Vera D., Álava J., Parrales G. Álava C., Murillo L., Castillo M. (2018). comenta que “cada individuo y cada herramienta debe acceder solo a aquello imprescindible para el desempeño de sus

funciones". De igual manera indica que "al implementar cualquier sistema organizativo, de reparto de tareas y responsabilidades se debe tener claro no todo el mundo tiene por qué acceder a todos los recursos de la organización". Claramente el tema de la correcta administración de los usuarios y privilegios, fue la piedra angular en el caso real de lo ocurrido en la empresa WXYZ, pero también fue la pieza clave para poner al descubierto esta modalidad de fraude pensional y para prevenir este tipo riesgos en la gestión de la información las organizaciones se pueden apoyar en la implementación de la ISO 27001. Esta macro actividad está recomendada para las grandes organizaciones que pueden implementar las buenas prácticas contenidas en esta norma ISO ya que gestiona la calidad de los servicios de Tecnologías de la Información. Es muy completa ya que contempla todos los escenarios en distintas fases como se observa a continuación:

Tabla 3: fases de la norma ISO 27001.

1. Análisis y evaluación de riesgos. 2. Implementación de controles 3. Definición de un plan de tratamiento de los riesgos o esquema de mejora. 4. Alcance de la gestión 5. Contexto de organización 6. Partes interesadas 7. Fijación y medición de objetivos 8. Proceso documental 9. Auditorías internas y externas

Fuente: Elaboración propia a partir de la Norma ISO 27001.

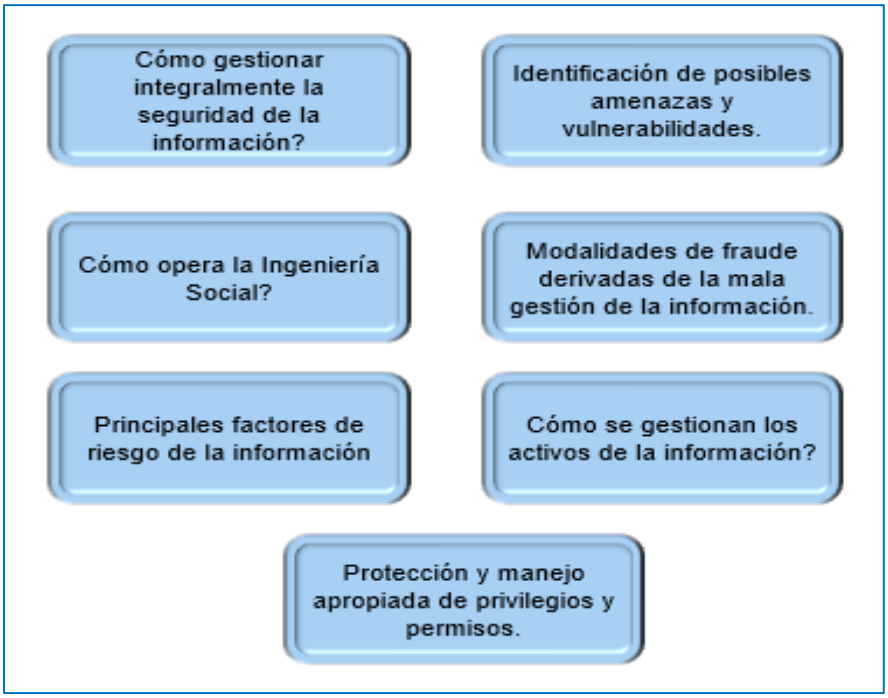
En el análisis y evaluación de riesgos se deben identificar los riesgos y principales amenazas de que pueden atentar contra la seguridad de la información, analizando el impacto en la organización que ponga en riesgo la confidencialidad, integridad o disponibilidad de la información. Teniendo en cuenta que los dueños de los riesgos son las personas, los riesgos o amenazas se deben asociar a cada proceso y a cada responsable. Para esto también es indispensable la implementación de controles y al respecto la norma ISO 27001:2013 describe

114 puntos de control. No obstante, dentro de los controles se propone implementar la capacitación a los usuarios como factor clave de éxito en la prevención de riesgos frente a la seguridad de la información (en este punto se hará énfasis más adelante). Esta norma también define un plan de tratamiento de los riesgos que se identifiquen y su forma de afrontarlos lo cual es de gran relevancia porque pasa a menudo que se identifican los riesgos, pero las organizaciones fallan respecto a la manera de tratarlos. También cobra bastante importancia el hecho de entender el contexto de la organización, como forma de prevención y anticipación de los riesgos sobre los que no se tienen control. Riesgos de tipo político, económicos, sociales, tecnológicos y ambientales que si no se contemplan literalmente pueden terminar con una organización. Existen variedad de herramientas de diagnóstico que permiten anticiparse y por lo menos pueden paliar estos eventos, si no logran ser eludidos. Además, otra parte clave contenida en esta norma es la auditoría interna y la revisión por la dirección, esto con el fin de hacer seguimiento al estado del sistema, estas auditorías internas se basan en la supervisión del liderazgo y el entorno y en la auditoria de los 114 controles propuestos por la norma.

Dentro de la implementación de la norma se definen una serie de controles para proteger y gestionar adecuadamente la información y dentro de estos controles es preciso implementar esquemas de capacitación al personal de las organizaciones, no solamente los que por la naturaleza de sus funciones tengan relación directa con información sensible que pueda comprometer la estabilidad de la organización, sino todos los empleados en general, como lo son el personal de servicios generales y el mismo personal de vigilancia. ¿Han notado que muchas veces las personas más informadas de los movimientos de la empresa son los vigilantes y las señoras cafetería? Pues bueno, esto se debe a que son las personas que tienen la visión general del movimiento de los demás empleados, los horarios y hasta saben dónde está ubicada la

información importante porque normalmente tienen acceso irrestricto a todos los lugares de la empresa y es allí cuando los delincuentes detectan cualquier espacio desprotegido e ingresan para obtener información. Por lo anteriormente expuesto, un factor clave de éxito para combatir los riesgos derivados de deficiencia en la gestión de la información es levantar un plan de capacitación para todos los colaboradores de la organización en el cual se contemplen al menos los siguientes temas:

Figura 8: temas que debe contemplar la capacitación en seguridad de la información.



Fuente: Elaboración propia.

El plan de capacitación debe reunir al menos las siguientes condiciones para que sea efectivo:

- Estar incluido en el plan de capacitación anual de la organización y estos deben responder a las necesidades y requerimientos de las dependencias.
- Tener definido un alcance y estar acorde con las funciones, responsabilidades y roles de los empleados.

- Tener destinado un presupuesto específico para cubrir locación, capacitadores y refrigerios.
- Estar alineado con los objetivos de la organización o al menos algunos de ellos.
- Permitir evaluar el contenido impartido de las capacitaciones en materia de seguridad de la información.

La capacitación implica las siguientes etapas básicas:

- ✓ Levantamiento de necesidades en las distintas áreas de la organización.
- ✓ Elaboración de un plan de capacitación que sea coherente con las necesidades detectadas.
- ✓ Desarrollo del plan de capacitación.
- ✓ Evaluación de los resultados.

Así mismo, a continuación, se presenta un modelo de planeación de capacitaciones:

Tabla 4: modelo de plan de capacitación.

CRONOGRAMA DE CAPACITACIONES 2021

Empresa WXYZ

N° de capacitacion	Dirigida a:	Responsable	Tema de la capacitacion	Contenido	ene-21	feb-21	mar-21	abr-21	may-21	jun-21	jul-21	ago-21	sep-21	oct-21	nov-21	dic-21
	1			1- 2- 3-												
	2															
	3															

Fuente: Elaboración propia.

La capacitación que se brinde a los empleados en términos de ciberseguridad y seguridad de la información, la empresa debe asumirla como inversión porque como hemos visto anteriormente, los costos derivados de los ataques y diferentes vulnerabilidades de la información le sale muy costoso a las organizaciones, no solo en términos financieros, sino que, además, afecta gravemente su reputación y por ende genera pérdida de clientes. La capacitación

de los empleados, por tanto, resulta de vital importancia, ya que gran parte de los delitos de seguridad informática son consecuencia de la falta de conocimiento, poca cautela y en otros casos un manejo irresponsable de la información vital para la empresa. Ahora, todo esto se puede prevenir en gran medida con adecuados planes de capacitación que contemple al menos los siete temerá mencionados en la figura N°9.

El caso puntual que se planteó de la empresa WXYZ es un caso real, donde hubo un acto netamente de imprudencia por parte de la empleada. Claramente esto se hubiese podido evitar si la empleada hubiera tenido una conducta menos confiada, y si además hubiese sido informada de los posibles riesgos que tiene en uso indebido de sus usuarios y claves de acceso. Estamos en una era donde ahora más que nunca el rey es el dato. La hiper conectividad ha hecho que sea muy compleja la gestión de la información y lidiar con ciber atacantes está a la orden del día. Así mismo, es una gran oportunidad desde control interno para coadyuvar en que la información sea efectiva, confiable, relevante, entendible y cuente con medios de seguridad, entre otras características, que permitirá tener una adecuada gestión de riesgos de la información para facilitar la toma de decisiones y alcanzar los planes de la organización.

5. CONCLUSIONES

La dinámica de las organizaciones y la sociedad en general ha cambiado con la denominada sociedad del conocimiento, propiciada por el gran intercambio de información gracias a las inmensas posibilidades que brindan las tecnologías de la información y las comunicaciones. Los avances tecnológicos han traído consigo grandes ventajas para la economía porque no solo se han acortado distancias, sino que además se ha ampliado la oferta y variedad de productos a los que se puede acceder desde cualquier parte del mundo. No obstante, también las organizaciones han enfrentado grandes desafíos respecto a la manera de administrar monumentales volúmenes de información, los sistemas de información mismos y los riesgos nuevos derivados de fallas humanas, hurto o fallas cibernéticas. En este escenario no solo es importante contar con herramientas eficientes, mejores políticas de acceso, copias de seguridad, potentes firewall y antivirus etc., sino que además es un factor clave de éxito frente al fraude derivado de la deficiencia en la gestión de la información, contar con personal capacitado que incorpore buenas prácticas tendientes a proteger la información de la empresa como uno de los activos más preciados. Por ello, como una medida de mitigar y prevenir los ataques informáticos y preservar información crítica, se recomienda a las organizaciones incluir dentro del plan de capacitaciones temas concernientes a la seguridad de la información y además que implementen la norma ISO 27001 ya que es una norma bastante completa cuyo fuerte son los controles.

Finalmente, desde nuestra competencia como especialistas en control interno estamos llamados a coadyuvar en la protección del dato como activo empresarial, brindar asesoría, vigilar y controlar el quehacer en las distintas dependencias y sobre todo acompañando a los empleados que son el centro del quehacer de la organización.

6. REFERENCIAS BIBLIOGRAFICAS

Aguilar A. (2004). Capacitación y desarrollo de personal. México D.F. Editorial Limusa S.A.

Antiveros E., López S.V. (2007). Economía de los datos. Riqueza 4.0. Telefónica fundación. Ariel.S.A. Barcelona.

Chiavenato I. (2007). Administración de recursos humanos. El capital humano de las organizaciones. Interamericana editores S.A. México.

Ceballos A., Bautista F., Mesa L., Argaez C., Duran A., Miranda F., Acevedo R., Prada W., Ruíz J., Santos H., (2019). Tendencia cibercrimen Colombia 2019-2020. Bogotá D.C. Recuperado de: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Congreso de la Republica (05-enero-2009) Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos". Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la Republica (30-julio-2009). Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Artículo 4. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

Congreso de la Republica. (17-octubre-2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Fraude a Colpensiones: van tras la pista de 1.000 casos más (06-08-2017). Revista Semana. Bogotá D.C. Recuperado de: https://www.semana.com/on-line/nacion/articulo/fraude-a-colpensiones-capturan-a-11-contratistas/527960.

Guerrero J. (2017). Manual de Políticas y Seguridad de la información. IDIGER. Recuperado: https://www.idiger.gov.co/documents/20182/200680/VERSION+FINAL-+ya+corregida-+julio+18.pdf/ce505c53-95b7-494c-ad41-8a91259dc2ee

ISO 27001:2013. Guía de implantación para la seguridad de la información. Recuperado de file:///C:/Users/lucei/Downloads/NQA-ISO-27001-Guia-de-implantacion.pdf

J Cano., Almanza A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 – 2018. Revista Ibérica de Sistemas y Tecnologías de la información. RISTI. ISSN: 1646-989. Recuperado de: file:///C:/Users/lucei/OneDrive/Escritorio/ESP%20CONTROL%20INTERNO/TRAB%20FINAL/Manual-de-citacio%CC%81n-APA-v7%20u%20externado.pdf

Martha R., Figueroa G., Vera D., Álava J., Parrales G. Álava C., Murillo L., Castillo M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Área de innovación y desarrollo. Alicante España.

Sofistic Cibersecurity (2019). La breve historia de la ciberseguridad. Recuperado de: https://www.sofistic.com