Año 24 No.2
Número especial 2019

RVG

Año 24 No. 2
Número especial 2019

Revista Venezolana de Gerencia

Revista Venezolana de Gerencia

UNIVERSIDAD DEL ZULIA (LUZ)
Facultad de Ciencias Económicas y Sociales
Centro de Estudios de la Empresa

ISSN 1315-9984

Universidad del Zulia (LUZ)
Revista Venezolana de Gerencia (RVG)
Año 24 N° 2, Número especial 2019, 528-541
ISSN 1315-9984

Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia

Muñoz Hernández, Helmer[1]
Zapata Cantero, Laura Giseth[2]
Requena Vidal, Dina Marcela[3]
Ricardo Villadiego, Leonela[4]

Resumen

La presente investigación busca mostrar la manera en como la tecnología ha venido evolucionando gradualmente y con ella la manera de almacenar la información y la necesidad de ir aumentando cada vez más su protección en bases de datos donde se almacena virtualmente toda la información correspondiente. Se analizan diferentes situaciones de riesgo, donde se ve afectada la información y las alternativas que se toman para contrarrestar, disminuir y controlar estos tipos de situaciones, tomando como base las buenas prácticas en la aplicación de la seguridad informática en los sistemas contables. Además, se llevó a cabo una comparación de los países como España y Colombia de las medidas tomadas para capacitar, prevenir y controlar aquellos delitos

Recibido: 11-09-19 Aceptado: 18-10-19

1 Ingeniero de Sistemas de Información, Magister en Ingeniería de Control Industrial, Doctor en Gerencia, Posdoctor en Investigación, Docente Investigador Universidad del Sinù. Grupo de Investigación CUS. helmermunoz@unisinu.edu.co No. Celular 3118746734. ORDCID: 0000-0002-2445-6585

2 Estudiante Contaduría Pública, Universidad del Sinú, Joven Investigador Grupo de investigación CUS, laurazapata@unisinu.edu.co, No. Celular 3205286615. ORDCID: 0000-0002-3156-4357

3 Estudiante Contaduría Pública, Universidad del Sinú, Joven Investigador Grupo de investigación CUS, dinarequena@unisinu.edu.co, No. Celular 3137473541. ORDCID: 0000-0002-2890-0823

4 Contaduría Pública, Universidad del Sinú, Joven Investigador Grupo de investigación CUS, leonelaricardo@unisinu.edu.co. ORDCID: 0000-0002-9382-4468

informáticos que se den dentro de una organización en el ejercicio de sus procesos contables a través de sistemas digitales o computarizados (bases de datos). En vista de que los riesgos informáticos son amenazas y vulnerabilidades que afectan en todos los aspectos a la empresa, y las consecuencias pueden ser muy graves en relación a la información que se viene manejando, las personas dueñas de las empresas deben optar por estrategias que sean efectivas para disminuir o prevenir estas situaciones y que sean aplicadas de manera integral.

Palabras clave: Informática; Riesgo; seguridad; Sistema Contable.

Computer risks and alternatives for computer security in accounting systems in Colombia

Abstract

The present investigation seeks to show the way in which technology has been gradually evolving and with it the way of storing information and the need to increase its protection in databases where virtually all the corresponding information is stored, due to certain external factors that affect it; with the aim of analyzing different risk situations, where the information and alternatives that companies take to counteract, reduce and control these types of situations are affected, based on good practices in the application of computer security in systems accountants In addition, a comparison was made between countries such as Spain and Colombia of the measures taken to train, prevent and control those computer crimes that occur within an organization in the exercise of its accounting processes through digital or computerized systems (databases). In view of the fact that computer risks are threats and vulnerabilities that affect the company in all aspects, and the consequences can be very serious in relation to the information that is being handled, the owners of companies must opt for strategies that are effective to reduce or prevent these situations and to be applied comprehensively.

Keywords: Computer Science; Risk; Security; Accounting System.

1. Introducción

A lo largo del tiempo la sociedad ha venido evolucionando cada vez más en el tema de la tecnología, haciendo uso de todos los elementos que sean necesarios para ir desarrollando nuevos instrumentos que le permitan a las personas utilizarlas de manera fácil y efectiva en todos los ámbitos.

Es probable que, en algún momento, al comienzo de la historia de la humanidad, los seres primitivos sintieran la necesidad de comunicar

de forma escrita las situaciones que vivían. Entonces, el lenguaje oral estaba en ciernes, pero a su alcance tenían instrumentos y técnicas que facilitaron la tarea de plasmarlas en las paredes de las cuevas, las piedras o el suelo de barro usando como pintura sangre de los animales y jugos de algunas frutas o plantas; o, simplemente, una rama a manera de pincel (Marín Ochoa, 2012)

Al estar en constante desarrollo, la búsqueda diaria de satisfacer necesidades, ha empleado los medios informáticos para lograrlo, "al ser humano actual le ha sucedido lo mismo que a nuestros antepasados prehistóricos cuando fabricaron el primer cuchillo. Tuvo un gran alivio en sus labores diarias, se sintió cómodo, porque ya contaba con una herramienta que le ayudaría en sus tareas cotidianas de supervivencia. Pero no faltó quien usara esta herramienta con otras intenciones en contra de sus congéneres y terminara cometiendo delitos que, seguramente, en su momento no se llamaron así, aunque sí se entendían como actos en contra de la supervivencia de los demás. Con los sistemas informáticos ha ocurrido algo similar a lo observado en la historia" (Ojeda-Pérez, Rincón-Rodríguez, Arias-Flórez, & Daza-Martínez, 2010).

Para los años 50, las líneas de teléfono empezaron a extenderse a principios del siglo XX. Estos sistemas albergaban fallos que eran explotados por los intrusos que accedían a los sistemas pudiendo desviar llamadas a su antojo, escuchar conversaciones, etc. (Álvarez Marañón & Pérez García, 2004), y es en este momento donde se comienza a observar las vulnerabilidades que tenían estas herramientas de comunicación; las cuales amenazaban, ya sea a una sola persona o a un conjunto de estas (organizaciones), y donde aquellos intrusos se aprovechaban para manipular la información a la cual estaban accediendo, por el simple hecho de escuchar una conversación. Consecuentemente, en los años 70, empezó a ser pública la figura de hacker, el cual nació por "un grupo de jóvenes estudiantes del MIT expertos en manejar los sistemas mainframe de la época" (Álvarez Marañón & Pérez García, 2004)

En 1987, en la universidad de Delaware, se produce el primer incidente conocido, si bien al año siguiente se extiende por ARPANET, red precursora de Internet, un gusano creado por Robert Morris, que colapsó multitud de sistemas y está considerado como el primer incidente serio de seguridad de la red Internet (Álvarez Marañón & Pérez García, 2004). Es por ello por lo que, a partir de aquí, se empezó a presenciar las amenazas que siempre han puesto vulnerables a las empresas: los virus, los ataques cibernéticos, códigos maliciosos y entre otros, los cuales han venido evolucionado de la mano con la tecnología.

Por lo anterior, puede iniciarse un cambio en esta manipulación de la información y se logra la creencia de que el proceso de nuevos modelos y de innovación tecnológica debe comenzar de forma obligada por la investigación básica. Cuando desde la experiencia empírica existen numerosas innovaciones que pueden nacer, a través del aprovechamiento de los resultados de investigaciones aplicadas existentes. (Fereira & Torres, 2017)

Sin embargo, la gestión de riesgos no es un tema nuevo; existen diversas definiciones al respecto que se han modificado con el paso de los años y se han utilizado tanto en la academia como en la práctica profesional. Vinculando ambas perspectivas, se propone la

gestión de riesgos como una forma de gestión que va más allá de los enfoques ya conocidos. (Hernández & Dopico, 2017)

En Colombia, las estrategias empresariales han contribuido al crecimiento de las organizaciones. De acuerdo con Calderón et al, (2009, 2010), el estudio de la estrategia en Colombia es aún muy incipiente, sin embargo, las empresas locales adoptan estrategias de diferenciación por calidad y liderazgo en costos, aunque se requiere desarrollar estrategias menos reactivas y más enfocadas en el ciclo del negocio. (Díaz, Tarapuez, & Hernández, 2017)

Según el pensamiento de Buendía (2013), las empresas son mucho más atractivas para estas actividades delictivas, tanto así que existen las auditorias de seguridad: contratamos a una empresa externa especializada en seguridad informática para que revise nuestros equipos y nuestros procedimientos" en base a este pensamiento podemos evidenciar herramientas que han surgido en nuestra actualidad con el fin de garantizar seguridad y protección al activo más importante que posee la empresa; la información

Es por ello que esta investigación, se llevó a cabo por el hecho de que se siguen presenciando falencias en las empresas en varios aspectos, los cuales aprovechan los delincuentes para atacar de manera rápida y lograr su cometido; dicha investigación se apoya en las estrategias con las que cuenta Colombia, y como estas han avanzada teniendo como referencia a un País que en los últimos años ha sido experto en temas de Ciberseguridad, como lo es España, y esto debido a su desarrollo

La investigación es de tipo descriptivo, debido a que se utilizó información soportada que buscara explicar y evidenciar las causas de sucesos que involucran riesgos informáticos, vulnerabilidades, amenazas y ataques cibernéticos, en empresas, sin importar su tamaño, tomando como referencia los avances que han tenido los dos países referentes: Colombia y España, en aspectos sociales y jurídicos, debido a los ataques que siempre se evidencia en el transcurso del tiempo, la causa real del porque hacen falta estrategias que contrarresten estos sucesos que afectan en gran medida a las empresas, en la parte financiera contable, en todos los aspectos.

2. Riesgos informáticos en empresas de Montería, Colombia: evidencia en el almacenamiento y manipulación de información

Los riesgos informáticos son amenazas y vulnerabilidades que afectan en todos los aspectos a la empresa, y las consecuencias pueden ser muy graves en relación a la información que se está manejando.

Según los autores Gonzalo Álvarez y Pedro Pérez (2004:30), consideran que "Un riesgo para un sistema informático está compuesto por la terna de activo, amenaza y vulnerabilidad, relacionados según la fórmula riesgo = amenaza + vulnerabilidad", lo cual significa que las empresas como poseen un conjunto de elementos que sirven como medio para el respaldo y la conservación de la información, es decir, los activos, estos se ven a diario expuestos a unos riesgos, los cuales van ligados a unas amenazas y vulnerabilidades.

Se puede decir, que una cosa lleva

a la otra, debido a que, si un computador no tiene las protecciones mínimas que deben tener, como por ejemplo los antivirus, actualizaciones del sistema operativo, etc., es decir que ese equipo cuenta con vulnerabilidades que pueden llegar a materializarse, ocasionando el acceso no autorizado de un atacante al servidor contable de una empresa y tener así control total de la información.

Por ello, en algunas empresas, medianas o pequeñas y de varios sectores, de la Ciudad de Montería-Córdoba, Colombia, se han presentado situaciones, como: la creación, por parte de los ciberdelincuentes, de programas malware que logran entrar a las plataformas de las planillas de seguridad social de los trabajadores, que se hacen de manera virtual, a través de PSE (Pagos Seguros en línea), con el propósito de robar contraseñas, las cedulas de los afiliados, información financiera, etc.

Además las plataformas de Redeban y Credibanco, con las cuales se hace efectivo el pago de cualquier compra o transacción que se haga, también se han visto afectadas por parte de estos delincuentes, al igual que los cajeros electrónicos, utilizando códigos maliciosos y logrando hacer copias de las tarjetas que puedan ser ingresadas a estos cajeros. Además los trabajadores que desempeñan cargos administrativos tienden a estar más en el foco de los delincuentes, ya que estos son los que tienen información valiosa en sus computadores del dinero y los procesos llevados cabo en una empresa.

También se evidenciaron aspectos en donde los programas consumen muchos recursos ocasionando lentitud en el computador, problemas en el almacenamiento de las bases de datos, la inexistencia de mecanismos de protección en el acceso de información contenida en los servidores y en relación a la interrupción de los procesos, la falta de herramientas de detección de malware, la falta de conciencia en seguridad informática en los empleados, que es una de las mayores causas de incidentes informáticos que afectan significativamente en los procesos de la organización, y que si no se controlan a tiempo pueden inducir al robo o la pérdida de la información.

La administración de las copias de seguridad de los sistemas contables juega un papel fundamental en la seguridad de la información y en todo el proceso que garantice la continuidad del servicio. Los buenos procedimientos en cuanto al almacenamiento de las copias de seguridad garantizan que la empresa pueda reaccionar ante algún incidente informático relacionado con robo o eliminación de la información.

Es muy importante que la organización cuente con políticas de almacenamiento de las copias de seguridad, tan estrictas como lo crean pertinente, por ejemplo el servidor contable genera una copia de seguridad diariamente, y esa copias quedan almacenadas en el disco duro del mismo servidor contable, pero adicional se cuenta con servidor de almacenamiento en red que diariamente extrae esa copia y la guarda, hasta este punto se tiene dos puntos de respaldo, pero si se necesita un mayor respaldo ante un incidente informático o un desastre natural se debe contar con un respaldo en la nube o con una empresa que preste servicio de almacenamiento en la nube, de esta manera se garantiza la disponibilidad de la información.

Aunque en muchos casos se trate de implementar un sistema de seguridad para la información contable y financiera,

muchos de estos no han ayudado de manera integral debido a que la empresa deja de lado una parte importante, que son los empleados, para la obtención de conocimiento y manejo de este tipo de circunstancias en relación a su actuar, y simplemente dicha responsabilidad o carga se la delegan a los expertos que contratan.

Es por ello la importancia de generar conciencia en seguridad informática, garantizando así que se tomen los controles necesarios para la prevención de los riesgos informáticos a los que se expone la organización. Cuando se realizan jornadas de capacitación en la que intervenga todo el personal de la empresa, se estarán dando las instrucciones para poder atender, reaccionar, reducir y evitar incidentes informáticos, que comprometa la seguridad de la información.

3. Plataformas utilizadas en España y Colombia para la prevención del robo de información

Cada uno de los países presenta o integra su manera de proteger, informar o capacitar a las empresas y personas acerca de temas relacionados con los delitos informáticos, en el caso de España, este país tiene sus propias herramientas que son de gran ayuda para la minimización de casos de violación de la información que posean las empresas, al igual que Colombia también cuenta con medidas que cooperan para que las empresas y las personas (comerciantes, empresarios, etc.) estén actualizadas sobre medidas para evitar situaciones de robo de información; sin embargo, cada uno de estos países cuenta con diferentes estrategias para combatir estas situaciones, las cuales incluyen, plataformas virtuales, leyes, cartillas, casos reales, medidas de protección, capacitaciones, entre otras.

España implementa esta cultura de seguridad en todos los ámbitos a través del Instituto de Ciberseguridad de España (INCIBE), el cual es una sociedad dependiente del Ministerio de economía y empresa, que con la ayuda del Gobierno Español busca implementar la cultura de ciberseguridad a través de las investigaciones, medidas, recomendaciones y atención a las personas dueñas y empleados de empresas, lo cual conlleva a desarrollar una estructuración sistematizada de las acciones que se deben hacer y las medidas que se deben tomar en situaciones donde se vea en riesgo la información contable-financiera de las empresas.

INCIBE es una plataforma que integra unas herramientas de información, actualmente cuenta con *Avisos de seguridad* el cual contiene información acerca de fraudes que se pueden dar en áreas de las empresas, las actualizaciones que ofrecen para los programas que tienen los dispositivos electrónicos y documentación de prevención acerca de situaciones que podrían presentarse; el *Reglamento General de Protección de datos RGPD para pymes* que no solo busca la actualización y protección de datos personales de cada uno de los ciudadanos sino de reforzar la seguridad de la información y así garantizar que las personas y empresas tengan el control de sus datos, además esto es fundamental a la hora de hablar de la competitividad en el mercado, debido a que se puede filtrar información que provoque desventaja en el mercado frente a otras personas o empresas;

información acerca de la *Protección de la información, del puesto de trabajo y en movilidad y conexiones inalámbricas* las cuales incorporan datos importantes sobre la necesidad de proteger las áreas en general que se encuentran en las organizaciones por ejemplo, la cartera, las cuentas bancarias, los clientes, la gerencia, el área financiera, contable y softwares contables, documentos de nómina, transacciones, estrategias de negocios, entre otras; cabe resaltar que estas prevenciones comienzan desde las medidas y comportamientos tomados por las personas, ya que al momento de incorporar un empleado nuevo a la organización se le debe presentar unas pautas específicas sobre la protección de la documentación que va a tener en sus manos, esto se hace efectivo siempre y cuando la empresa tenga una estructura organizativa y técnica para la formación de sus empleados.

España cuenta con informes acerca de las *Buenas prácticas en el área de informática* "con el objeto de dar a conocer cómo tratar los riesgos que suponen estas amenazas, se especifican un conjunto de buenas prácticas para la gestión de activos de información, la seguridad en las operaciones y la gestión de incidentes" (INCIBE, 2014), esto ayuda de manera gradual a las organizaciones para tener unas buenas políticas de copias de seguridad en caso tal que se presenten incidentes y así poder recuperar la información sin que se filtre, al igual que la parte de la accesibilidad que tienen los empleados en relación a las cuentas que le son creadas, las cuales introducen en los computadores, ya que en las entidades donde se pueda presentar una alta rotación de personal se tiene que tomar la precaución de restringir de manera inmediata el acceso a la información para evitar problemas, una vez desvinculado de la empresa.

La formación del personal por medio de la *capacitación*, es también otra medida que incorpora España, esto se logra por medio de expertos en el área con el propósito de preparar al personal para cualquier eventualidad, partiendo del que tiene un alto cargo hasta el más bajo cargo según el organigrama empresarial. De igual forma, la gestión adecuada de los activos que posee la empresa, como computadores, memorias USB, dispositivos móviles, impresoras, los servidores, los softwares, entre otros.

Analizando la estructuración en el desarrollo que ha tenido España en el tema de la ciberseguridad ha evolucionado notablemente puesto que anteriormente solo se veía focalizada en temas relacionados con el desarrollo de proyectos de innovación en las TIC (Tecnologías de la información y la comunicación), algo muy general y no estaba focalizada en un aspecto en específico, sin embargo con el cambio de visión hacia la ciberseguridad, debido a las ciberamenazas que enfrentan las personas y empresas, le ha dado la oportunidad al país de reducir casos que pueden ser lamentables.

Este país ha tomado medidas muy estratégicas, que benefician a todas las personas en general (empresas, niños, jóvenes, adultos, profesionales), en el uso del internet y dispositivos tecnológicos, teniendo siempre presente el triángulo de la seguridad CID, el cual trata de la Confidencialidad en el ámbito de que la información y los datos son netamente privados y solo se les puede mostrar a un grupo reducido de personas, la Integridad refiriéndose a que la información puede ser modificada por personal autorizado y la Disponibilidad,

que toda la documentación está disponible cuando se necesite y haya un acceso efectivo.

Partiendo de esto, Colombia en comparación con España, ha instaurado, a través de la Policía Nacional de Colombia, el *Centro Cibernético Policial de la Dijín,* el cual es un centro policial de denuncia virtual que busca brindar toda la información que sea necesaria para mantener en conocimiento a las empresas, personas y profesionales de informes sobre las modalidades más frecuentadas por los ciberdelincuentes, como medio de precaución y prevención para que se tome como referencia las actuaciones que toman para delinquir virtualmente.

Incorpora un sistema de visualización en tiempo real, **"***Ciberincidentes"*, de los casos que se han presentado, dando la oportunidad de ver el tiempo en el que se evidenciaron, el tipo de robo de información o modalidad, el lugar y si fue a una persona o a una empresa, en este las personas se pueden dar cuenta que en años anteriores y actualmente en el país se evidenciaron muchos casos de vulnerabilidad y amenaza de la información. También ofrecen dos Apps que son muy fáciles de descargar y eficientes a la hora de denunciar y hacer efectivo procesos que disminuyen estos delitos, como *Polis*, que está conectada directamente con la línea de emergencias de la Policía Nacional de Colombia 123, y *A Denunciar*, un sistema nacional de denuncia virtual, la cual brinda procesos agiles para denunciar ataques cibernéticos.

Al igual que INCIBE, el Centro Cibernético Policial de la Dijín en Colombia ofrece *un mural de cibercrimen*, el cual brinda información acerca de modalidades que se vienen presentando como el Phishing, Malware, La carta Nigeriana, La Estafa y Smishing, dentro de las cuales muestran ejemplos con imágenes de las estrategias que utilizan los delincuentes para obtener información de otras personas. Además cuentan con un *observatorio cibercrimen*, donde se puede observar boletines, acerca de falsas cadenas de empleos, correos spam, suplantación de Sim Card, falsas publicaciones en internet, etc.; guías ciberseguridad, acerca de las modalidades delictivas del Smishing y Vishing, guía ransomware, guía de seguridad de información en WhatsApp, etc.; y análisis del cibercrimen, otorgando reportes anuales del cibercrimen junto con los costos que generaron para las personas y organizaciones afectadas.

La dirección de investigación criminal e INTERPOL (DIJIN) junto con otros organismos de otros países han desmantelado bandas de ciberdelincuentes en el país, dando a conocer todos los aspectos que estos utilizaban para lograr un robo de cantidades de dinero significativas a través de la información que obtenían, esto también puede ser visible en la plataforma del centro cibernético policial de la DIJIN, a través de los casos operativos.

4. Seguridad informática en Colombia y España: Avances

A lo largo de los años, España y Colombia han venido incorporando cierto desarrollo en el tema de la seguridad informática en las empresas, y esto se ve reflejado en el aspecto jurídico, el cual incluye leyes que de alguna u otra forma establecen el respaldo, que las empresas y las personas, necesitan para minimizar la presencia de situaciones que incorporen robo de información

financiera y contable.

En relación con España se logra evidenciar que el Consejo de Seguridad Nacional promueve la publicación del Código de Derecho de la ciberseguridad, donde se da a conocer los diferentes aspectos en donde actúa la ciberseguridad, respaldado por leyes, ordenes, reglamentos y decretos sobre la normativa de seguridad nacional, infraestructuras críticas, normativa de seguridad, equipo de respuesta a incidentes de seguridad, telecomunicaciones y usuarios, ciberdelincuencia, protección de datos y relaciones con la administración.

Según el Real Decreto 421 del 12 de marzo de 2004, se regula el Centro Criptológico Nacional, el cual se encarga de "la seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifra, y La seguridad de los sistemas de las tecnologías de la información que procesan, almacenan o transmiten información clasificada" (Instituto Nacional de Ciberseguridad, 2013). Además de "Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones; Formar al personal de la Administración; Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia, entre otras. (Instituto Nacional de Ciberseguridad, 2013)

También se enfatiza en la Ley Orgánica 10 del 23 de Noviembre de 1995, del Código Penal, con el propósito de describir aquellas personas catalogadas como criminales responsables de delitos, las responsabilidades que tienen estos una vez que se sometan a cometer actos ilícitos: la reparación de daños e indemnizaciones, habla acerca de aquellas personas que no hayan actuado directamente, es decir que hayan sido cómplices, también los convierten en criminales, las estafas, y otros aspectos relevantes. Esta ley, va de la mano del Real Decreto del 14 de Septiembre de 1882, que trata acerca de la Ley de enjuiciamiento criminal, ya que es la que establece las medidas para hacer justicia frente a amenazas, denuncias y delitos.

La ley Orgánica 3, del 5 de diciembre de 2018, sobre la protección de Datos personales y garantía de los derechos digitales y la Ley Orgánica 1720 del 13 de diciembre de 1999, sobre la protección de datos de carácter personal junto con la Constitución Española, establecen que el "tratamiento de datos personales es un derecho fundamental protegido" (Instituto Nacional de Ciberseguridad, 2013), por lo que ninguna persona ajena puede manipular la información de otra, a menos que esta ultima de autorización de utilizarla, con esto se hace más que todo énfasis a los menores de edad y personas cuya información sea de cuidado; sin embargo en estas dos leyes se analiza que es un delito robar los datos personales de otros en general y es un derecho su confidencialidad.

Por otro lado, Colombia ha instaurado leyes, entre las que resaltan: La ley 1273 del 2009 (Título VII BIS), la cual modifica el Código penal de Colombia y expone los delitos informáticos que pueden cometer o son cometidos por personas que buscan manipular información importante acerca de una entidad o un ciudadano, lo que más les llama la atención a los Ciberdelincuentes, es la parte financiera,

contable y administrativa, ya que a través de estas pueden darse cuenta de todos y cada uno de los movimientos que se llevan a cabo en el trascurso de un tiempo, teniendo conocimiento y manipulación de información ajena y confidencial.

Por ello, el Código penal sanciona a esas personas que cometen actos delictivos informáticos en contra de otros (entidades y personas), para así poder tener control y disminución de estos tipos de casos. Algunas de las sanciones que establece este Código son: que se les mandara a la cárcel por un tiempo de 48 a 96 meses o una multa de 100 a 1000 Salarios Mínimos Mensuales Legales Vigentes, para aquellos que tengan un acceso abusivo y obstaculicen el funcionamiento de la información de un sistema informático, una base de datos o los sistemas o softwares contables, al igual que cuando "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" (Congreso, 2009) también incurrirá en dicha pena o multa.

Por lo tanto, se puede dar el caso que los mismos trabajadores sean los principales autores del crimen y se les facilite la interceptación de información o la utilización de softwares maliciosos para la obtención de datos importantes y así consecuentemente tener el poder de utilizar la información a favor de estos, acerca de esto el código penal expresa que "el que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses" (Congreso, 2009) y en el caso del uso de sistemas infectados o maliciosos y violación de los datos personales dispone que "El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes" (Congreso, 2009) y para aquellos que "con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes" (Congreso, 2009), incurrirán en la misma pena y sanción.

Sin embargo, el título menciona dos aspectos que son los más relevantes y de mayor riesgo para una empresa, y es la suplantación de los sitios web de estas y la transferencia de activos o bienes sin consentimiento de la empresa, ya sea propiedad de esta o de sus clientes, y esto lo pueden hacer posible los ciberdelincuentes de tal manera que al suplantar sus sitios web tengan acceso a todas sus claves y procedimientos para infectar toda la red que cubre la empresa y así llegar a los sistemas contables y cuentas bancarias y empezar hacer movimientos que le generen lucro a estos delincuentes, por ello se establecen sus sanciones y multas correspondientes respecto a la suplantación "incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no

constituya delito sancionado con pena más grave." (Congreso, 2009) Y para la transferencia de activos "incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes" (Congreso, 2009)

Por consiguiente, la Ley 1928 del 24 de julio del 2018, trata acerca del convenio sobre la ciberdelincuencia, la cual se llevó a cabo con el propósito de prevenir situaciones que afecten las tres partes del triángulo de la seguridad, la confidencialidad, integridad y disponibilidad, debido a la constante actualización, desarrollo y progreso de la tecnología y la manera de conservar información importante, tipificando algunos delitos y las medidas que se deben tomar al presentarse alguno de estos, por ejemplo, en la parte de los delitos informáticos se establecen dos, que son la falsificación, relacionada con "la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténtico " (Congreso, 2018).

Si se analiza lo anterior, va relacionado con lo que dicta el Código penal acerca de la suplantación de sitios digitales, y el fraude, relacionado con el perjuicio del patrimonio ajeno a través de cualquier "introducción, alteración, borrado o supresión de datos informáticos y cualquier interferencia en el funcionamiento de un sistema informático" (Congreso, 2018), y así poder manipular a su favor y tener el control de estos.

Sin embargo existe otra normativa que trata acerca de estos temas y que son una guía para las empresas que están en el proceso de instauración de algún sistema o para la prevención de algún litigio futuro, y este es el caso de las ISO 27000, 27001 y 27002. La ISO 27000, "esta norma proporciona una visión general de los sistemas de gestión de la seguridad de la información, así como los términos y definiciones de uso común en la familia de normas de SGSI. Esta norma es aplicable a organizaciones de todo tipo y tamaño" (Normalización-ISO, 2017); es decir, que esta norma se centra en la seguridad de la información y las normas de calidad y la gestión de esta misma que es establecida por la organización internacional de normalización ISO.

También se menciona "con el uso de las normas de la familia SGSI, las organizaciones pueden desarrollar e implementar un marco para gestionar la seguridad de sus activos de información, incluyendo información financiera, propiedad intelectual, información confiada a una organización por clientes de terceros" (Normalización-ISO, 2017). En pocas palabras que lo que pretende es la protección de la información incluyendo procesos, sistemas y activos que puedan ser afectados y pongan en riesgo la estabilidad económica de la empresa; también la norma añade la importancia de los servicios informáticos y la manera en que se puede usar a nuestro favor a través de programas de detección y de limpieza y con la aplicabilidad de metodologías que cubran o garanticen el buen uso de la información y en su defecto la recuperación de esta.

La ISO 27001, "elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información" (Normalización-ISO, 2006), es decir que va totalmente enfocada

en la seguridad de la información y alineada a un enfoque especifico; así como busca la adopción de este enfoque que anteriormente era totalmente anónimo, pero que ha tomado auge en los últimas décadas, por tal motivo esta normatividad busca la concientización de los procesos de gestión de la seguridad de la información de acuerdo a las necesidades que va teniendo la empresa de cualquier ámbito.

La ISO 27002 que habla sobre el Código de práctica para controles de seguridad de la información, con referencia a que "la seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas las políticas, procesos, procedimientos, estructuras organizacionales y las funciones del software y del hardware" (Normalización-ISO, 2015), es decir que la protección de los datos no se va a lograr teniendo el mejor software o programa, sino que también se aplique la planeación y la gestión de los procedimientos y así controlar los procesos cuando se presente cualquier eventualidad.

La norma expone los requisitos de seguridad de información estableciendo que "existen tres fuentes principales de requisitos de seguridad: a) La valoración de los riesgos para la organización, teniendo en cuenta la estrategia y los objetivos de negocio globales de la organización. Por medio de una valoración de riesgos se: a) identifican las amenazas a los activos, se evalúa la vulnerabilidad y la posibilidad de que ocurran, y se estima el impacto potencial; b) Los requisitos legales, estatutarios, de reglamentación y contractuales que una organización, sus socios comerciales, contratistas y proveedores de servicios deben cumplir, y su entorno socio-cultural. c) El conjunto de principios, objetivos y requisitos del negocio para el manejo, procesamiento, almacenamiento, comunicación y archivo de información, que una organización ha desarrollado para apoyar sus operaciones." (Normalización-ISO, 2015)

Con estas normativas que Colombia ha instaurado como guía para la prevención de robo de información, no ha sido lo suficientemente efectiva, debido a que no solo se debe ocupar el hecho de crear aspectos legales que contrarresten estos casos sino que también actualizar la normatividad constantemente con el objetivo de crear medidas que sean aún más eficientes aplicarlas a la hora de proteger la información en caso de un ataque que pueda afectar toda la parte tecnológica de la empresa o de una persona, este análisis es soportado por el informe entregado este año por la plataforma Comparitech, el cual expresa que "al país no le fue muy bien en la calificación de su legislación, que mide qué tan actualizada está para brindar garantías de ciberseguridad.

El puntaje fue de 4 sobre 10, aunque ningún país pasó de 7, ni China ni Francia, los mejor posicionados en ese ítem." (Semana, 2019), Consecuentemente este estudio arroja que "entre 60 países estudiados, donde Argelia, el que ocupó el primer puesto, tiene los peores índices de ciberseguridad, y Japón, en el último puesto, tiene los mejores, Colombia quedó en el renglón 39. Es decir, el país está en el rango medio de la seguridad en la red." (Ingenieria, 2019) Y además "en Colombia se producen el 0,5% de los ataques al software financiero con el que se pretende robar a los usuarios. En los países peor calificados, ronda el 2%" (Ingenieria, 2019).

Estas cifras aún son preocupantes

aunque algunos lo tomen de manera normal, debido a que da soporte a lo expuesto anteriormente, en donde deja evidencia que no se está desarrollando más allá de lo que debería, sistemas especializados y no se ha invertido lo necesario para mitigar estos hechos, por ello muchas de las empresas de este país han presentado ataques cibernéticos puesto que no cuentan con el apoyo necesario por parte del gobierno, en términos de la profundización de estos temas y también que estas empresas al presentarse este tipo de situaciones, no tengan lo suficiente para implementar otros sistemas que sean más profesionales, debido a su alto costo. Todo esto va ligado a que el Gobierno Colombiano trate de incorporar estas buenas prácticas de control en la seguridad informática tomando como referencia otros países, y así poder instaurar o implementar unas estrategias que logren minimizar estos delitos que afectan tanto en menor como en mayor medida a las empresas y personas.

5.Conclusiones

Los sistemas contables que poseen cada empresa de este país, suelen ser un blanco directo para aquellos ladrones de información financiera, por ello utilizan diferentes técnicas para obtener acceso a los servicios y redes que posee una empresa o persona, para así poder tomar control y extraer toda la información necesaria. Es por ello que cada vez que los empleados estén en su sitio de trabajo, deben tener presente algunas alternativas básicas de seguridad para proteger o contribuir de alguna manera a la conservación de la información financiera de la empresa.

Las situaciones de riesgo en el que se presentaron en estas empresas tienen lugar debido a las deficiencias que se presentan en las buenas prácticas en seguridad informática, el desconocimiento de las actuaciones que se deben tener en cuenta, y el no pensar como estos ciberdelincuentes, debido a que si uno lo hace, se instaura automáticamente una barrera más estable, puesto que se tiene conocimiento de sus actuaciones y estrategias.

Tomando como referencia los dos países estudiados, ambos brindan aspectos que son muy importantes a la hora de contrarrestar, prevenir y disminuir situaciones de ataques cibernéticos, no solo exponen las ayudas que podemos adquirir para proteger nuestra información sino también los procesos, la información y la cultura que debemos tener a la hora de manipular datos que sean importantes en las organizaciones. Se muestra claramente que estos países tienen sus propias estrategias pero una puede servir de ejemplo para la otra y ayudarse mutuamente con el propósito de crear un ambiente de seguridad en el ciberespacio de todos los datos personales de cada una de las organizaciones y personas en general.

No se trata de que tan seguros sean los softwares contables, ni los sistemas técnicos que tenga la empresa para la prevención de amenazas, sino de que tan capacitados están los empleados para no dejar visiblemente datos que pueden ser utilizados por los hackers, o aquellos sitios utilizados para la suplantación de páginas y robar las credenciales de acceso a los sistemas de una organización o simplemente el robo de la información al abrir un correo con un archivo adjunto; las buenas prácticas de generación de conciencia en seguridad informática es una buena y excelente alternativa de seguridad comercial de información, debido a que se incorporan elementos de

fácil entendimiento y acceso, como lo son folletos, videos, informes de casos, etc. los cuales sirven como ejemplo y educación, no solo para los empleados, sino también para los dueños y directivos de empresas; no basta con solo tener los mejores sistemas de protección contra intrusos, ya que aunque estos puedan prevenir los ataques efectivamente, el problema resulta de un punto ciego que no estamos prestando atención y muchas empresas lo dejan a un lado, que son los trabajadores, el principal objetivo es que todos y cada uno de los integrantes de las empresas sepan cómo actuar ante ataques cibernéticos y tengan conocimiento de lo que puede ser sospechoso al momento de abrirlo.

Esta es la alternativa de solución más importante, que no solo los del área de sistema estén capacitados, sino que todos estén preparados para cualquier eventualidad.

6. Referencias bibliográficas

Álvarez Marañón, G., & Pérez García, P. P. (2004), **Seguridad informática para empresas y particulares**. Madrid, SPAIN: McGraw-Hill España.

Congreso (2009), Ley 1273 de 2009. Diario Oficial, 4.

Congreso (2018), Ley 1928 de 2018. Diario Oficial, 49.

Díaz, B. E. G., Tarapuez, E., & Hernández, R. P. (2017), Estrategia y calidad en empresas colombianas de servicios. **Revista Venezolana de Gerencia**, 22(80), 593-609.

Ferreira, J. R. B., & Torres, E. E. P. (2017), Modelos explicativos del proceso de innovación tecnológica en las organizaciones. **Revista Venezolana de Gerencia**, 22(79), 387-405.

Hernández, R. M., & Dopico, M. I. B. (2017), Gestión de riesgos: reflexiones desde un enfoque de gestión empresarial emergente. **Revista Venezolana de Gerencia**, 22(80), 693-711.

INCIBE (2014), Buenas prácticas en el área de informática. from https://www.incibe.es/protege- tu-empresa/que-te-interesa/buenas-practicas-área-informática

Ingeniería, A. (2019), Colombia se encuentra posicionada en el ranking de Ciberseguridad mundial. from https://www.apingenieria.com/colombia-se-encuentra-posicionada-en-el-ranking- de-ciberseguridad-mundial/

Marín Ochoa, B. E. (2012), Infografía digital: todo comenzó en las cavernas. Tram [p] as de la Comunicación y la Cultura.

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010), Delitos informáticos y entorno jurídico vigente en Colombia. **Cuadernos de Contabilidad**, 11(28).

Roa Buendía, J. F. (2013), Seguridad informática. Madrid, SPAIN: McGraw-Hill España. Semana. (2019), Así está Colombia en el ranking de ciberseguridad mundial. Retrieved10/08/2019, from https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

Instituto Nacional de Ciberseguridad, C. d. S. N. (2013), *código de derecho de la ciberseguridad*.