Universidad Nacional Autónoma de México
Programa de Posgrado en Ciencias de la Administración

Seguridad de la Información: Estrategia de Gestión basada en Marcos de Referencia de Control y Seguridad para las Organizaciones en México.

Tesis

Para optar por el grado de:

Maestro en Administración de Organizaciones

Presenta:

Oscar Vital Cedillo

Tutor:

Dr. Ignacio Rivera Cruz
Facultad de Estudios Superiores Cuautitlán

Estado de México, mayo de 2019

ÍNDICE

Capítulo 4. Normas internacionales, controles o marcos de referencia como herramientas para la estrategia de gestión de la seguridad de la información en una organización

Índice de figuras

Índice de tablas

Agradecimientos

Esta es la parte del trabajo en la que con todo merecimiento deberán estar nombradas las personas más influyentes en esta etapa de mi vida, que tuvieron que ver con la decisión de estudiar la maestría y en su caso el combustible para llevarla a buen puerto.

Doy las gracias a mi esposa por su gran apoyo, la paciencia y la comprensión durante todo el proceso, sin ella no hubiera sido posible nada de esto.

Indudablemente a mi Madre, Padre y Hermano al verme formado e inculcado el valor del compromiso.

Obviamente y sin duda, que en la parte académica debo hacer un reconocimiento especial a mis profesores Dr. Aldo Vigueras, Dr. Jerónimo Martínez, Mtra. Diana Arenas, Mtro. Esteban Zarza, Dr. Pedro Guzmán, Dr. Gerardo Sánchez y de forma especial a mi tutor y profesor el Dr. Ignacio Rivera Cruz por todos sus consejos y enseñanzas trasmitidas, los antes mencionados como conjunto de grandes personas que cambiaron mi visión de la vida profesional y académica.

Simplemente mil gracias a todos.

Introducción

La investigación y la ciencia es uno de esos tantos temas que se han dejado de lado por décadas y es necesario que se posicione como el pilar del desarrollo de nuestra nación, darle la formalidad teniendo en cuenta factores como la aplicación del método científico, sus métodos auxiliares y de apoyo, basarse en una metodología específica de investigación, así como determinar el tipo y alcance de la misma. El planteamiento del problema es fundamental en una actividad de investigación, elementos como los objetivos e hipótesis son preponderantes para darle cause a la investigación; con respecto al presente trabajo de tesis se centrará principalmente en la información como el insumo y activo más importante de cualquier organización y como poder implementar la seguridad y su gestión mediante el apoyo de marcos de referencia internacionales.

Desde la antigüedad la información y su gestión han sido fundamentales para determinar el rumbo o el inicio de guerras, catástrofes financieras, revoluciones sociales y demás acontecimientos mundiales y por supuesto las organizaciones no son la excepción.

En muchos de los casos las organizaciones no alcanzan a visualizar lo fundamental que es llevar acabo la gestión de la seguridad de la información ni los efectos adversos y riesgos que puedan surgir de no implementarla, para evitar dichos inconvenientes existen normas internacionales y marcos de referencia que aportan para una buena implementación de la seguridad de la información y su gestión, todas esas herramientas sumadas a la capacitación y concientización del capital humano aportaran una mayor certidumbre en los procesos de la organización tanto internos como externos. La seguridad de la información no se trata de un tema de moda o de la época, al contrario, es un tema que se tuvo olvidado por mucho tiempo y que hasta hoy las organizaciones están volteando a ver nuevamente.

Capítulo 1. El Método

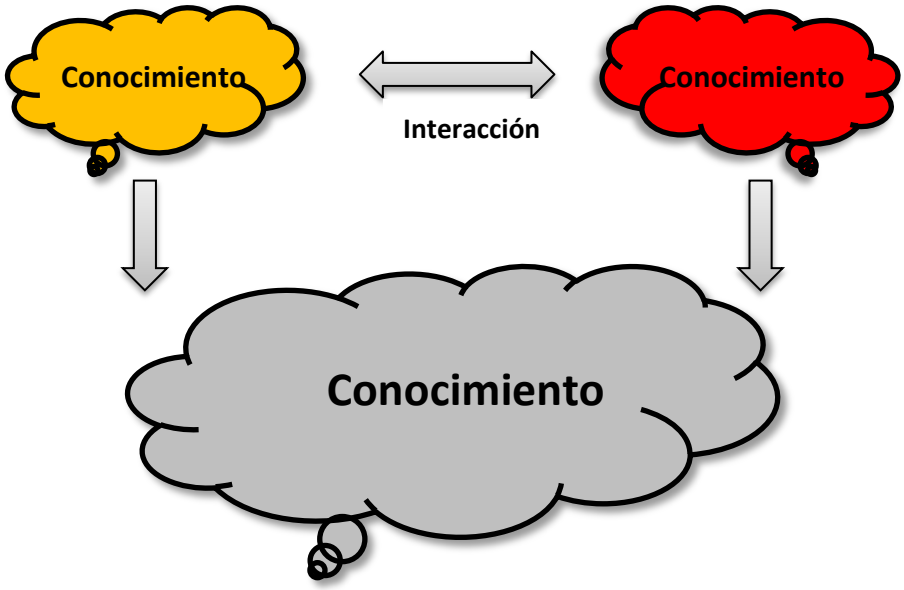
1.1 El quehacer científico

Como lo comenta Arellano (2003) a través del tiempo la humanidad ha lidiado con la tarea de entender las formas y maneras de como los científicos realizan sus actividades, dejando de lado la importancia de fomentar y transmitir la chispa de la curiosidad de la población joven para acercarlos al campo de la ciencia y la investigación, sin embargo, no todo está perdido.

Existen autores que plantean la manera de encaminarse a la investigación científica, la cual se centra inicialmente en entender el conocimiento científico, la ética científica y la importancia que tiene ésta en la vida del hombre, como segundo punto se establece el conocer él método científico y como aplicarlo, comprendiendo sus etapas y ámbito que abarcan y finalmente como tercer punto a llevar acabo es el realizar un reporte de todos los datos relevantes y de interés que posteriormente se puedan someter a procesos estadísticos y a futuros estudios, el reporte debe ser claro, preciso y fundamentado (Arellano, 2003).

Además, Arellano (2003) nos dice que el conocimiento no es algo lineal, sino que al contrario, en él existen ramificaciones que nos lleven a dar pasos hacia adelante y hacia atrás lo que se traduce en nuevos comienzos y desviaciones, ya que en una investigación cualquiera que sea su origen no podremos visualizar o ser conscientes de todos los pormenores desde un inicio, como son: detalles, imprevistos y obstáculos inherentes a una investigación (figura 1).

Figura 1. El conocimiento



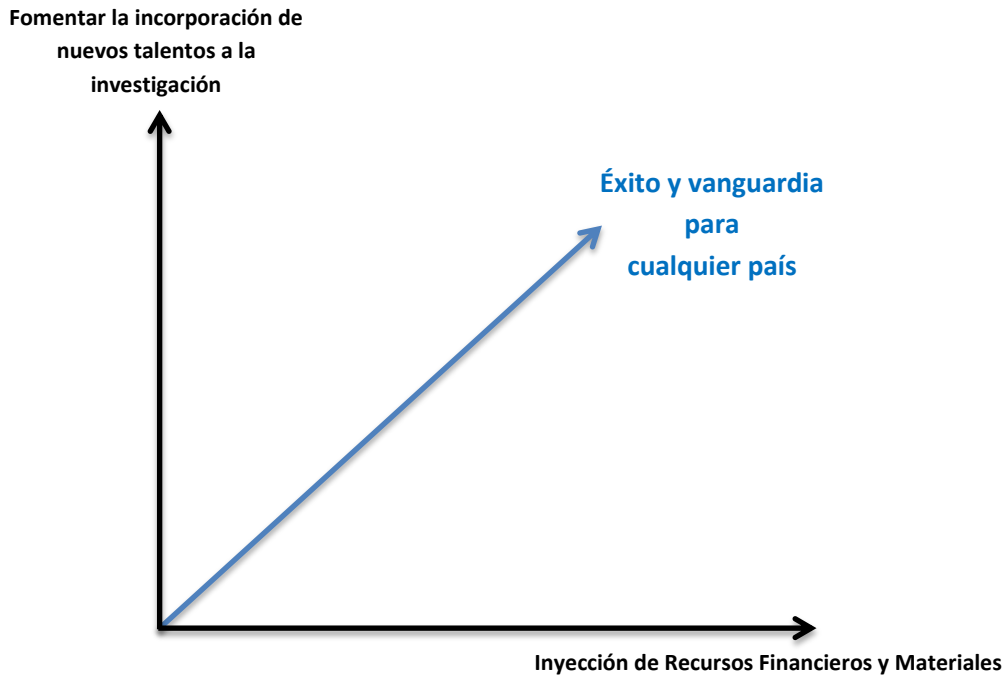
Fuente: Elaboración propia

Tenemos que una investigación científica confronta ideas o pensamientos con observaciones, para Stiles (2009) una buena investigación implica en sí misma estar abierto a cambios de ideas, estar atento a lo observado en la investigación pues mediante esto se confirman o rechazan ideas previamente concebidas, ya que la verdad empírica nunca es general y permanente, sin embargo, eso no quiere decir que sea errónea, hay que tener en cuenta que la ciencia siempre es y será acumulativa (Stiles, 2009).

En el caso de nuestra nación sabemos que enfrentamos un déficit en la generación de investigación científica, en el campo de la innovación y tecnología y por supuesto lo más importante, es generar y acercar al talento humano joven al terreno de la investigación, se requiere la inyección de recursos financieros y materiales para poder hacer frente a los nuevos retos y desafíos que implica la globalización. Sacar a nuestro de país del rezago en términos de investigación, abandonar la lista de los países que menos invierte en investigación y desarrollo

de tecnología, ya que tan sólo se asigna menos del 1% de PIB de nuestro país a esta actividad (Rivera, Ibarra, Moreno y Hernández, 2009) (figura 2).

Figura 2. Investigación y recursos financieros



Fuente: Elaboración propia

Sin lugar a dudas nuestro país se enfrenta a la posibilidad de diseñar una nueva plataforma de desarrollo en la investigación. Sabemos que tenemos varias áreas de oportunidad, que poseemos el potencial para subsanar esos inconvenientes y que en cuanto sean atendidas, nuestra nación florecerá y despuntara en el ámbito global (Rivera et al., 2009).

1.1.1 Ciencia

Como es de suponer el concepto de ciencia a lo largo del tiempo ha tenido diferentes acepciones y cuyas diferencias son atribuidas al campo de estudio y el

enfoque de quien lo define, gracias al aporte de dichos elementos el concepto se enriquece aun más.

Para algunos autores la ciencia puede conceptualizarse en un sentido amplio como un conjunto sistemático de conocimientos mediante los cuales se pueden establecer principios y leyes que a través de ello el hombre explica, describe y transforma el mundo que le rodea (Münch y Ángeles, 2007). Baena (2014) por su parte asevera que la ciencia también está definida como: la búsqueda contínua de la verdad. Sin embargo, los caminos y las formas para acceder a la verdad pueden ser múltiples, la duda sistemática es uno de esos caminos.

Con lo que respecta a Navarro (2014), la ciencia es un cuerpo organizado o sistematizado de conocimientos que hace uso de leyes o principios generales. Es un conocimiento acerca del mundo, del cual se puede alcanzar un acuerdo universal y criterios comunes para justificar presuntos conocimientos y creencias.

Para un servidor y después de estar influenciado por la literatura, la ciencia podría estar definida como el resultado de la aplicación sistemática de métodos y procesos los cuales están basados en la observación, razonamiento, análisis y experiencia con el objetivo de acrecentar el saber humano.

1.1.2 Método científico

Este concepto para muchos resulta ser algo complejo de definir y de llevar acabo, sin embargo en la vida cotidiana lo aplicamos de manera inconsciente, de hecho se basa en aspectos empíricos como la observación, la experiencia y la experimentación, a continuación formalizaremos de mejor manera este concepto.

El método científico es definido por algunos autores como la explicación, descripción y predicción de fenómenos, su principal cualidad es obtener con mayor facilidad y certidumbre el conocimiento científico (Münch y Ángeles, 2007). Para Bunge (1979) la definición del método científico se entiende como el conjunto de postulados, reglas y normas para el estudio y solución de los problemas, los cuales son institucionalizados por la denominada comunidad científica reconocida.

En un sentido más amplio, el método científico se refiere al conjunto de procedimientos que, apoyados con instrumentos o técnicas necesarios, examina y soluciona problemas de investigación.

De igual manera para otros autores como Navarro (2014) el método científico es un conjunto de pasos que se siguen en la generación de conocimiento, apoyado por una serie de reglas rigurosas que le den la propiedad de irrefutable, teórica y empíricamente, es decir, que el conocimiento es verdadero.

Personalmente considero al método científico como una de las partes medulares de la evolución tecnología y científica del humano, al dotarla de formalidad, fundamentación y certeza, lo anterior, respaldado por métodos de apoyo y auxiliares.

1.1.3 Métodos de apoyo y auxiliares

Son métodos que nos permiten llevar a cabo la investigación de manera adecuada y mediante los cuales podremos llegar a un resultado coherente y con una base sólidamente científica, entre los que se encuentran (Baena et al., 2014).

- Deductivo. Es un proceso basado en el razonamiento de juicios de tipo general para obtener conclusiones particulares o específicas, es decir va de lo general a lo particular.
- Inductivo. Es un proceso que parte de conclusiones particulares válidas y aceptadas para llegar conclusiones generales, en otras palabras, va de lo particular a lo general.
- Análisis. Se fundamenta de la idea que partiendo de un todo como objeto de estudio se separa en diversas partes o elementos para su estudio de manera individual.
- Síntesis. Al contrario que el anterior partimos de varios elementos, se estudia sus relaciones y coincidencias, y se integran en un conjunto o sistema conceptual.
- Experimental. Se basa en observaciones realizadas y acciones dirigidas en

donde el fenómeno se reproduce artificialmente en condiciones preestablecidas y controladas y con base en lo anterior proceder a formular hipótesis.

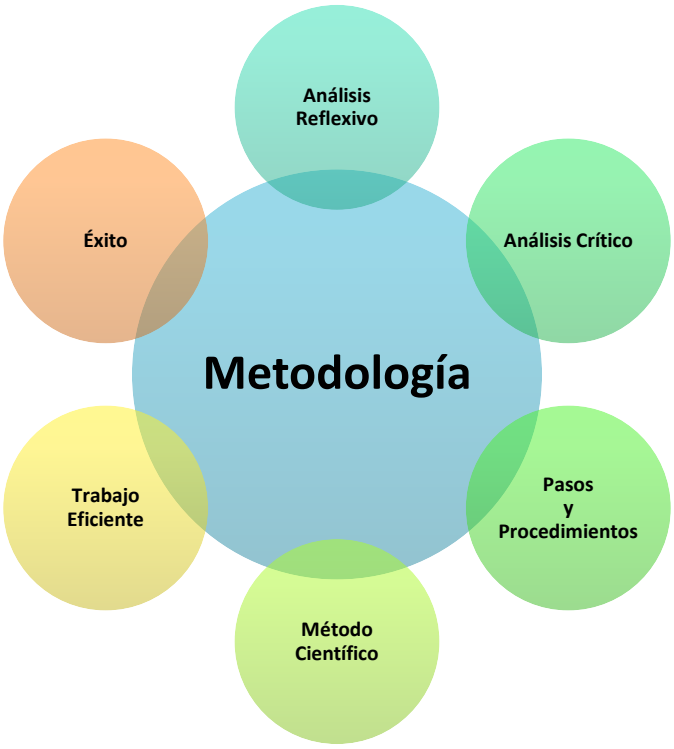
- Comparativo. Es un proceso de examinar de manera simultánea las semejanzas y diferencias de los elementos o fenómenos en estudio.
- Histórico. Este se basa en el análisis y registro de hechos y acontecimientos relevantes ocurridos en el pasado.
- Funcional. Nos dice que el conjunto de todo lo estudiado se entiende como unidad, este método trata de explicar y fundamentar el equilibrio social.
- Estructural. Se basa en la noción de un todo como objeto de estudio y que se ve afectado por la interacción o la modificación de cada una de sus partes que lo forman
- Dialéctico. Es un la forma o proceso de conocer la realidad que se desprende del objeto de estudio, analiza las diferentes posturas para obtener un mejor resultado.
- Matemático. Nos lleva al estudio y la generalización del aspecto cuantitativo, las relaciones generales y la estructura de los objetos y procesos, se basa en la medición de las características de los fenómenos.
- Estadístico y de probabilidades. Proceso basado en la recolección, presentación, análisis e interpretación de datos numéricos, representa a su vez un método auxiliar en la aplicación de otros.
- Etnográfico. Inicia con la antropología cultural. Consiste en la recolección de información proporcionada por los integrantes de una comunidad, dicha información consisten en la descripción detallada de sus costumbres, creencias, mitos, genealogías, historia, etc.

1.1.4 Metodología de las investigaciones

La metodología de investigación es aquella que permite el análisis reflexivo y crítico de los conceptos teóricos a desarrollar en una investigación, conlleva a la utilización de pasos y procedimientos para resolver problemas mediante la

aplicación del método científico. Otra característica de este tipo de metodología establece el rumbo correcto de una investigación asegurando un trabajo eficaz y eficiente frente el logro de resultados (Guerrero, 2014) (figura 3).

Figura 3. Elementos y características de una Metodología de investigación



Fuente: Elaboración propia

Para Bernal (2006) la metodología es un conjunto de aspectos operativos en el proceso de investigación, como lo vimos existen métodos de apoyo y auxiliares de los cuales podemos echar mano y así enfocarnos en las posibles líneas de acción. Al elegir un método de investigación debemos tener cuidado en que cumpla con la característica de estar debidamente fundamentado, ser claro, preciso, sistemático y verificable.

Para un servidor la metodología de la investigación es el conjunto de herramientas y recursos aplicados de forma secuencial, los cuales están

relacionados al campo de conocimiento del objeto de estudio y las posibles respuestas requeridas.

1.1.5 Tipo de Investigación

La ciencia se construye con la investigación; una actividad propia de la mente, que debe ser sistemática, controlada, empírica, pública y crítica de fenómenos naturales. Se guía por la teoría y las hipótesis sobre las presuntas relaciones entre esos fenómenos (Kerlinger y Lee, 2002). La investigación se dice que tiene dos propósitos: producir conocimientos, teorías y resolver problemas satisfagan las necesidades intelectuales comunes a toda la humanidad (Lukasiewics, 1970), la investigación puede tener diferentes vertientes como lo veremos a continuación.

Para Baena (2014) la investigación pura es el estudio de un cierto problema, destinado única y exclusivamente a la búsqueda de conocimiento, se dice que desarrolla la disciplina en términos abstractos y de ella se desprenden principios de carácter general.

La Investigación aplicada tiene como objeto, el estudio de un problema destinado a la acción; este tipo de investigación aporta hechos nuevos, trata de llevar a la práctica las teorías generales y destinan sus esfuerzos a resolver las necesidades de la sociedad (Baena, 2014).

La investigación documental o bibliográfica es la búsqueda de una respuesta específica a partir de la investigación en documentos. Con lo que respecta a la investigación de campo esta tiene la finalidad recoger y registrar ordenadamente los datos relativos al tema escogido como objeto de estudio. La observación y la interrogación son las principales premisas que el investigador utiliza. (Baena, 2014).

Finalmente Baena (2014) nos comenta que la investigación experimental se presenta mediante la manipulación de una variable experimental no comprobada, en condiciones controladas, con el fin de escribir de qué modo o por qué causa se

produce una situación o acontecimiento particular. Con lo que respecta al presente trabajo de tesis se utilizará una investigación de tipo mixta, la razón es porque estará basada en la investigación bibliográfica y de campo para la elaboración del proyecto, el objetivo es desarrollar un trabajo teórico-práctico.

1.1.6 Alcance

Toda vez que ya se analizó el entorno y se identificaron las necesidades, podemos determinar un tema de estudio, posteriormente se elige la metodología de investigación, pasando ahora al tema de plantearse cual será el alcance de la investigación, para lo se describirán los siguientes tipos:

Inicialmente tenemos los estudios exploratorios, los cuales tienen por objetivo principal el familiarizarse con los tópicos o fenómenos desconocidos, poco estudiados o novedosos y profundizar en la investigación de los mismos, así como el impacto que tienen en su entorno Baena (2014).

Los estudios descriptivos sirven para analizar cómo es y cómo se manifiesta un fenómeno y sus componentes, para ubicar las variables y recolectar datos que muestren un evento, comunidad, fenómeno, hecho, contexto o situación que ocurre. Los estudios correlacionales se basan en cómo se vinculan diversos fenómenos entre sí, o no se relacionan, evaluar el enlace entre dos o más conceptos, categorías o variables (Baena, 2014).

Los estudios explicativos buscan encontrar las razones o causas que provocan los fenómenos, entenderlos y responder a las causas de los eventos, sucesos y fenómenos físicos o sociales (Baena, 2014). En el caso de este trabajo de investigación se utilizará un tipo de alcance descriptivo que sumado al tipo de investigación mixta en la que se basará, se espera obtener muy buenos resultados.

Para Baena (2014) ningún tipo de estudio es superior a los demás, todos son significativos y valiosos. La diferencia para elegir uno u otro tipo de investigación

estriba en el grado de desarrollo del conocimiento respecto al tema a estudiar y a los objetivos planteados.

1.2. Planteamiento del problema

1.2.1 El problema

Actualmente las organizaciones exitosas del siglo XXI deberán ser aquellas que sean adaptables, abiertas a la reorganización, lo anterior sumado al máximo aprovechamiento de las últimas tecnologías e incorporarlas a sus procesos y enfocados a alcanzar la excelencia e innovación, haciendo a las organizaciones aún más productivas, sustentables y socialmente responsables Sánchez (2017).

Con lo que respecta al manejo y resguardo de la información en muchas de las organizaciones no se lleva de la mejor manera, un ejemplo de ello son las organizaciones educativas, donde los procesos relacionados con la información no son cuidadosamente tratados, ya que no están sensibilizados con el valor que tiene este activo, otro aspecto, es que la infraestructura es subutilizada, lo que desencadena en procesos carentes de calidad.

Algo importante a considerar es que si las áreas de oportunidad planteadas no se consideran para ser atendidas, los procesos administrativos en la organización se verán comprometidos y serán afectados al ser susceptibles al colapso, comprometiendo la estabilidad de la organización e incluso en casos extremos llevar a la desaparición.

1.2.2 Preguntas de investigación

¿Qué es la seguridad de la información?

¿Los directivos y en general el capital humano están sensibilizados con las necesidades de la aplicación de la seguridad de la información en la organización?

¿Qué beneficios aportará la instrumentación de la seguridad de la información en los procesos y la infraestructura?

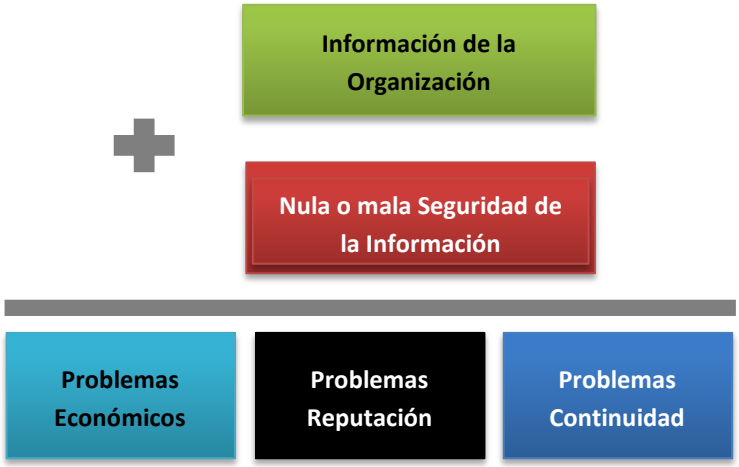
1.2.3 Justificación

Desde siempre la información en las organizaciones ha sido el activo más importante ya que de ahí se desprende todos los procesos administrativos y técnicos, detengámonos a pensar por un momento, que pasaría si una multinacional como Coca-Cola perdiera la famosa fórmula de su producto estrella o bien que bancos mundiales extraviaran parte o en caso aún más severo toda la información de sus cuentahabientes y sus registros bancarios, se detonaría un problema global, ésta idea nos lleva a que en la actualidad no existe empresa u organización que no necesite de la información para operar.

Ahora pasaremos de un supuesto a toda una realidad de nuestro tiempo y es el caso protagonizado por Cambridge Analytica y la red social Facebook, la primera una importante firma de análisis de datos que según investigaciones judiciales intervino de manera poco ética en las elecciones de los Estados Unidos en donde Donald Trump fue el beneficiado al obtener la presidencia del vecino del norte, dicha empresa se apoderó de información de millones de perfiles de usuarios de Facebook específicamente mas de 50 millones y mediante la cual desarrollaron técnicas y estrategias para tratar de influir sobre la decisión de los electores de esa nación.

Pero esa no fue la única consecuencia para Facebook, de hecho fue aun peor ya que en términos económicos en sólo un día sus acciones perdieron cerca del 7% de su valor, lo que se traduce en una pérdida de más de $6000 millones de dólares sumado a la mala reputación y desconfianza que sembró entre los usuarios de los Estados Unidos (figura 4).

Figura 4. Resultado de la falta seguridad de la información en una organización



Fuente: Elaboración propia

Lo anterior es un vivo ejemplo de lo importante que es el implementar mecanismos para la seguridad de la información y las consecuencias de no hacerlo adecuadamente, es pertinente comentar que este caso fue un evento relacionado con la tecnología pero no necesariamente la seguridad de la información es un sinónimo de computadoras y algoritmos criptográficos, es mucho más que eso, se trata de protección y el manejo de la información en todas sus formas, ya sea lógica o física (Daltabuit, Hernandez, Mallen & Vazquez, 2007).

Es por tal motivo que la seguridad de la información toma mayor notoriedad en un ambiente tan globalizado y automatizado y también sabemos que dicha seguridad deberá estar basada en un conjunto de herramientas y mecanismos comprobados y avalados internacionalmente que tienen como objetivos principales mantener la confidencialidad, la disponibilidad y la integridad del activo más importante (Villegas, 2008).

Pero como bien sabemos para cualquier proceso de cambio ya sea en el campo de la seguridad de la información o en cualquier otro, el factor humano es de suma importancia y este caso no es la excepción, los directivos de la organización, así como todos sus subordinados deberán estar conscientes de la

importancia de la información que manipulan y a la que tienen acceso, para ello cada organización debe procurar llevar a cabo un estudio y análisis del tema para saber qué tan profundo es el desconocimiento entre los empleados de la organización (Daltabuit et al, 2007).

Toda vez que se tiene un diagnóstico de la situación, se podrá proceder a una capacitación de los empleados sin importar qué puesto tengan, ya que si bien se puede tener tecnología de protección de punta o políticas de resguardo y manipulación de la información eficientes en el papel, mientras el capital humano las desconozca y no las ponga en práctica no servirán de nada y la situación permanecerá inalterable (Daltabuit et al, 2007).

Por lo anterior surge la necesidad de proteger este activo tan importante para todos y más aún cuando vivimos en la era del conocimiento, sin lugar a dudas se tienen registros que desde la antigüedad el hombre usaba sus propias técnicas de seguridad de la información, ejemplo de ello fue el cifrado César o bien la máquina enigma en la segunda guerra mundial (Daltabuit et al, 2007).

Con la implementación de seguridad de la información cada organización se asegurará que su información esté disponible y utilizable en cada momento sin importar las circunstancias, estará protegida y solo las personas autorizadas tendrán acceso a ella evitando que haya fuga de la información. Otra característica que tendrá la información es que permanecerá inalterable que nadie podrá modificarla más que el dueño de la misma.

Como consecuencia de la implementación de la seguridad de la información, la infraestructura se verá afectada de manera positiva, ya que será explotada de manera óptima, dejando de ser un recurso subutilizado y provocando que el flujo de los procesos sea más eficiente (Marquez, 2015)

1.3 Objetivos

1.3.1 Objetivo general

Presentar y describir una propuesta de estrategia para la implementación de la seguridad de la información para el mejoramiento en los procesos de confidencialidad, integridad y disponibilidad de la información en una organización.

1.3.2 Objetivos específicos

- Determinar el entorno tecnológico, de infraestructura y humano de las organizaciones entorno a la gestión de la información y su seguridad como parte de una estrategia que contribuya al mejoramiento de la organización.
- Analizar los orígenes de la inconsistencia y deficiencias en los procesos de implementación, infraestructura y sensibilización del capital humano como punto de partida para la corrección de las áreas de oportunidad de la organización en el plano de la seguridad de la información.
- Identificar las áreas de oportunidad en el proceso de implementación de la seguridad de la información como herramienta de cambio para la organización.
- Diseñar una estrategia de gestión de la seguridad de la información como mecanismos para la transformación de los procesos de almacenamiento, consulta y resguardo de la información en una organización.
- Proponer la instrumentación de marcos de referencia como pauta para la implementación y gestión de la seguridad de la información en una organización.

1.4. Hipótesis

Una óptima gestión en la seguridad de la información basada en marcos de referencia o normas internacionales permitirá la mejora en los procesos de manejo y resguardo de misma, coadyuvando al incremento de los niveles de confidencialidad, integridad y disponibilidad de la información.

1.4.1 Variable dependiente

Después de analizar y contrastar las diferentes variables de estudio se determinó mediante ejercicio de causa y efecto (Ishikawa) que la variable dependiente es:

- La seguridad de la información

1.4.2 Variables independientes

De igual manera y basado en el diagrama de Ishikawa, las causas o variables independientes son:

- Procesos
- Infraestructura
- Sensibilización del capital humano

1.4.3 Descripción de variables

Sánchez y Ángeles (2017) nos comentan que las variables de estudio independientes y dependientes, nos indican con mayor precisión características de un fenómenos de estudio, la medición de estas variables en el trabajo de investigación aportan valores que ayudan a la explicación del tema de estudio (tabla 1).

Tabla 1. Definición de variables

Variables independientes	Concepto
Capital humano	Para Werther y Davis(2014) es el elemento que hace posible el desarrollo de las organizaciones, es quien mantiene el movimiento y genera que las empresas evolucionen, sin este elemento sería imposible hablar de organizaciones.
Procesos	Hernández y Pulido (2011) argumentan que son un conjunto de fases sucesivas de un fenómeno con el fin de planear, organizar, integrar, dirigir y controlar.
Infraestructura	Es el conjunto de elementos, dotaciones o servicios necesarios para el buen funcionamiento de una nación, de una ciudad o de una organización cualquiera.
Variable dependiente	**Concepto**
Seguridad de la información	Daltabuit y Hernández (2007) la describen como una disciplina encargada de establecer metodologías y mecanismos basados en elementos como estándares y herramientas para proteger la información.

Fuente: Elaboración propia

1.5. Diseño de la investigación

Tipo

Debido a la naturaleza del trabajo de tesis, el tipo de investigación a desarrollar es de tipo no experimental, la cual presenta la característica de observar y medir el fenómeno, en lugar de manipular algunas de las variables que son afectadas en el estudio. A su vez tiene la característica de ser transversal ya

que se realizará la recolección de datos y la descripción de comportamiento de las variables en un tiempo o momento preciso (Sánchez y Ángeles, (2017).

1.6 Enfoque

Las investigaciones científicas vistas desde muy diversas corrientes del pensamiento, entre las que se encuentran el estructuralismo, empirismo, etnográfico, fenomenología, entre otras, han creado un grupo de propuestas para el estudio de fenómenos y formulación de juicios. A dichos enfoques se les conoce como: Estudios cuantitativos y estudios cualitativos.

Para esta investigación se utilizará un enfoque cualitativo, el cual se caracteriza por recolectar datos para probar hipótesis basado en la medición numérica y el análisis estadístico, dando como resultado el aporte en la creación de productos del intelecto humano en distintas ramas del saber (Sánchez y Ángeles, 2017).

Capítulo 2. La información, la seguridad de la información y su gestión

2.1 La información, su valor y su caducidad

Para Nicasio (2015) la información se entiende como todo aquel conjunto de datos organizados, relacionados y que en poder de un solo individuo u organización representa valor en sí misma sin importar su formato ya sea digital o físico; el uso de éste recurso, así como su reutilización producirá conocimiento socialmente útil.

La información no es estática, al contrario, se encuentra en constante movimiento, por tal motivo es de suma importancia conocer como la transferimos y a través de qué canal se transporta, si el medio es seguro y si los actores tienen acceso a éste. Es primordial considerar cuánto tiempo se puede conservar dicha información de tal manera que siga siendo útil para la organización y por supuesto en qué lugar se almacenará (Luna, Bojórquez y Hofmann, 2015).

Al igual que su manejo y custodia se debe considerar su correcta destrucción, en el caso de ser digital hacerlo mediante software especializado o bien si se tiene de forma física la estrategia de destrucción de los documentos para evitar que llegue a personas que puedan hacer mal uso de ella. (Ramos, 2013)

Sin lugar a dudas la información es utilizada como insumo estratégico para la toma de decisiones en las organizaciones, para autoevaluarse y determinar si los objetivos propuestos son alcanzables, el uso estratégico de la información conlleva a la creación de nuevo conocimiento enfocado en la optimización de recursos y a lograr que una organización o sociedad sea más eficiente; el conocimiento es un elemento que tiene en sí mismo la propiedad de la auto-replicación (Luna et al., 2015) (figura 5).

Figura 5. La información y la toma de decisiones

Fuente: Elaboración propia

Se dice que en países desarrollados, como el vecino del norte, la plantilla de trabajadores en su mayoría están dedicados al manejo de la información para todos sus procesos, mientras que una minoría se dedican a actividades físicas de producción, es decir, la información y el conocimiento están superando al esfuerzo físico en la manera de producir riqueza.

Basado en lo anterior, es imperativo contemplar herramientas y mecanismos que ayuden a mejor la forma de manipulación y almacenamiento de la información, por ejemplo poseer la infraestructura que brinde un buen rendimiento en los procesos de almacenamiento, gestión y seguridad de la información (Sánchez et al., 2010), ya que como sabemos, la información se transforma en conocimiento una vez procesada, lo que permite entrar a un ciclo de generación de información-conocimiento. Si bien, la información son datos estructurados que permanecen estáticos hasta que alguien o algo con los conocimientos y habilidades suficientes los procesa y los interpreta, ésta última debe de estar muy bien administrada para poder ser utilizada.

La información posee intrínsecamente algunas características que debemos considerar, como el valor que el dueño le atribuye, su caducidad o temporalidad y por supuesto factores externos tales como las personas que la gestionan (Ríos y Ramírez, 2016), en la actualidad nadie puede asegurar que unos cuantos se puedan beneficiar de ella ya que la información fluye por diferentes canales y direcciones.

La valor de la información se potencializa cuando intervienen las tecnologías de la información en todo el proceso de generación de conocimiento, encontrando como nicho principal, el área de los negocios ya que se trata de actividades lucrativas, ¿Y qué organización no requiere de recursos económicos para sobrevivir?

Un ejemplo de la importancia que se le da a la información y las repercusiones de un mal o buen manejo de ésta, es que surjan leyes relacionadas con su manipulación y gestión como lo es la Ley Federal de Transparencia y Acceso a la Información en nuestro país. Es un hecho que la información es uno de los principales activos de las organizaciones y de las personas y que sumada a su importancia en la vida empresarial, es necesario que tenga las siguientes características: Útil, Oportuna e Integra (Villegas, 2008).

2.2 Sociedad de la información y del conocimiento

Algunos autores proponen que el surgimiento de la llamada sociedad de la información, fue a mediados de la época de los 70´s, sin duda el nacimiento de está tuvo repercusiones en muy diversos ámbitos de la vida, el económico, el político y el social y para tal efecto se definen tres rasgos característicos de dicha sociedad, entre los que se encuentran: Una revolución en el ámbito tecnológico, el efecto de la globalización y finalmente los cambio de las organizaciones de pasar de un sistema de jerarquías verticales a las llamadas organizaciones en red (Sánchez et al., 2010).

A partir de esa época, la sociedad comenzó a experimentar los grandes cambios y la importancia de la información en la vida, está de más decir que las organizaciones y las relaciones humanas fueron afectadas desde su interior por dicho fenómeno, así como, en su desarrollo y la nueva manera de adaptación al nuevo escenario global.

Para la sociedad de la información, el conocimiento que se desprende resulta ser el único y mayor recurso significativo, dejando atrás y de manera discreta elementos o factores tradicionales de la producción como, la mano de obra y los recursos naturales, por su parte, el ingenio y la innovación se iban abriendo camino (Sánchez et al., 2010).

Posterior al surgimiento de la sociedad de la información, para ser un poco más preciso dos décadas después, surge un nuevo concepto “sociedad del conocimiento” lo que nos lleva a la aparición de una nueva estructura social, económica y política teniendo como base un intangible tan importante como lo es el conocimiento, que haciendo mancuerna con las Tecnologías de la Información y las Comunicaciones (TIC’s) se vislumbraba un gran impacto en nuestra vidas. (Sánchez et al., 2010)

Para Luna et al (2015) el conocimiento es un viaje que inicia con la aparición del dato y que posteriormente al agruparse forma un conjunto y que, posteriormente se convierte en lo que conocemos como información y que al final, mediante la interpretación, alcanza el grado de conocimiento funcional.

El conocimiento como base de la administración exige nuevas estrategias, objetivos y metas de gestión que deben de tener un enfoque basado en la creatividad, innovación, adaptabilidad, competitividad, responsabilidad con el entorno, uso tecnológico y mejora continua, consolidando organizaciones exitosas con la capacidad de competir en los mercados ya existentes y por supuesto en los nuevos mercados digitales, con el fin de mejorar la calidad de vida de la sociedad. (Sánchez et al., 2010).

Fritz Machlup fue unos de los primeros en utilizar la expresión “sociedad del conocimiento”, se dio cuenta que al basar sus investigaciones en datos y proyecciones económicas del momento encontraba respuesta a ciertas áreas de oportunidad, coincidiendo con la idea que la información es un elemento principal para generar valor; durante la misma época Peter Drucker argumentaba en materia económica que gran parte del producto Interno Bruto (PIB) sería generado por el conocimiento y lo que se desprendiera de él, resaltando que para las futuras sociedades el saber era la clave del éxito y que finalmente el conocimiento genera aún más conocimiento y que éste debe ser encausado de la mejor manera posible con el objetivo de buscar el beneficio para la sociedad.

Para tal fin se requiere rescatar el objetivo de una sociedad educativa en donde la información y el conocimiento que se desprende de ella son las herramientas base de las relaciones humanas, el principal reto de nuestro siglo es generar organizaciones inteligentes, para ello debemos tener una excelente gestión de la información que facilite la generación de conocimiento listo para ser aplicado (Sánchez et al., 2010).

Parte fundamental para la generación de conocimiento está basado en contar con los canales de distribución y comunicación adecuados, es mediante ésta y la interacción con el medio que podremos conocer más de nosotros mismos, nuestras debilidades, fortalezas, oportunidades y amenazas, lo que les permitirá tener una mejor toma de decisiones enfocadas para lograr alcanzar nuestros objetivos (Madrigal, 2009).

En el año de 2005 en Túnez y durante la Cumbre Mundial sobre la Sociedad de la Información, se hizo un exhorto a la Asamblea General de las Naciones Unidas para la declaración del día 17 de mayo como el Día Mundial de la Sociedad de la Información y del cual se desprende a su vez el día Mundial de Internet, cosa que no resulta menor ya que desde siempre la información es el insumo principal para cualquier actividad realizada por el hombre.

Como ya lo hemos visto, los canales por los que fluye la información son de singular importancia para el desarrollo de un país, sus organizaciones y sus individuos y es en estos últimos en donde el INEGI (Instituto Nacional de Estadística y Geografía) se enfoca y realiza algunas encuestas que dan muestra qué tanto nuestra sociedad tiene acceso a las tecnologías de información. Ejemplo de éstas encuestas es la ENDUTIH 2017 (Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares).

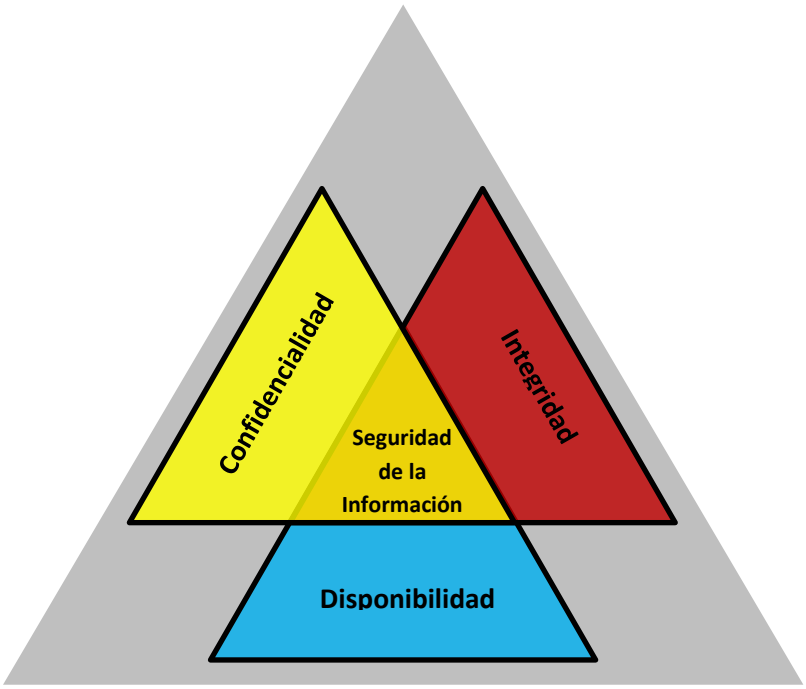
La encuesta arroja que 63.9% de la población de nuestro país, hace uso de internet ocupando el doceavo lugar después de las potencias mundiales. Más de la mitad de los hogares mexicanos cuentan con la infraestructura para conectarse a internet, la mayor afluencia de conectividad evidentemente son las zonas urbanas, utilizando los dispositivos móviles como mayor instrumento para la comunicación con el 89.7% de las veces y cuya principal finalidad es la de buscar información de diversa índole, seguida del entretenimiento y en tercer lugar la comunicación con otras personas (INEGI, 2017).

La posibilidad de acceso a la información y conocimiento son innegables, sin embargo todo este cumulo de posibilidades se puede ver afectado tanto por agentes internos y externos si este elemento principal al que denominamos información se ve comprometido, lo que requiere la implementación de medidas de protección y buen manejo de misma y para ello tenemos la seguridad de la información.

2.3 La Seguridad de la información

Para Villegas (2008) la seguridad es entendida como una característica de cualquier sistema informático o no informático y la cual refleja el nivel de riesgo a sufrir un daño, por su parte el daño o peligro es todo aquello con potencial real de generar una afectación su integridad, confidencialidad o disponibilidad (figura 6). Para muchos especialistas el concepto de seguridad de la información es utópico ya que en la actualidad no se puede asegurar un sistema al 100%.

Figura 6. Pilares de la seguridad de la Información



Fuente: Elaboración propia

En la actualidad, como se había mencionado anteriormente, el activo más importante para cualquier organización es la información, ya que repercute directamente en su éxito o fracaso, por tal motivo el aseguramiento de ésta y de los sistemas (informáticos o no) que la gestionan resulta ser una de las prioridades para cualquier empresa u organización, cumpliendo la siguiente premisa: que a mayor importancia o relevancia de la información, se deberá hacer mayor énfasis e inyección de recursos para su protección (Villegas, 2008).

Si se trata de asegurar la información, no cabe duda que el factor o capital humano representa una dicotomía, mientras que sabemos que es el elemento en el que se fundamenta cualquier organización también es el principal riesgo y debilidad de la seguridad de la información, por lo que se debe de tener mayor cuidado con ello y trabajar en la prevención y concientización del personal (Villegas, 2008).

Según el origen de la amenaza, la seguridad de la información se puede dividir en dos partes:

Por un lado, la seguridad lógica que consiste en dotar de aplicativos y procesos que sirvan como barreras de protección para el resguardo y acceso de los datos, asegurando que solo personal autorizado tenga acceso a ellos.

La otra es la seguridad física que consiste en la utilización de barreras físicas y procesos de control, como medidas preventivas ante amenazas a los recursos de estos controles van encaminados a proteger el hardware y medios de almacenamiento de datos. (Maza y Cabrera, 2013)

Ahora bien, ¿Qué es una vulnerabilidad?, es un punto débil que se encuentra en todo el proceso de gestión de la información y que pueden ser explotados por una amenaza, dichas amenazas pueden ser de diverso origen por ejemplo: natural, por hardware, software, de infraestructura y el más importante y peligroso y recurrente de ellos, el humano. (Maza y Cabrera, 2013). Es por ello que todos los directivos de la empresa sin importar al giro o rama en la que se desempeñe su organización, deben estar conscientes de la importancia de mantener una correcta seguridad de la información para asegurar el buen funcionamiento de la organización.

2.4 Importancia de la Seguridad de la Información

Si bien he abordado algunos términos y conceptos de la seguridad de la información, hay preguntas que se irían contestando por si mismas como por ejemplo, ¿Por qué cualquier organización debe hacer un buen manejo y protección de su información?, ¿Actualmente qué organización no utiliza equipo de cómputo para almacenamiento, administración y consulta de información?, no es fácil contestarlas y aunque hubiera organizaciones que no requiera de equipos sofisticados de almacenamiento, sin lugar a dudas requiere de proteger sus activos aunque sea con obstáculos físicos y a eso ya se le denomina seguridad de la información, no confundir con seguridad informática, ya que está ultima se basa

en elementos puramente computacionales, en otras palabras la seguridad informática es una parte de otras tantas de la seguridad de la información.

El uso de tecnologías de la información en la mayoría de las veces nos rebasa individualmente y las organizaciones no son la excepción, por lo que debemos incorporarnos al nuevo esquema de la digitalización para dotar de una mayor agilidad en nuestros procesos potencializando el crecimiento, competitividad y eficiencia de nuestra organización (Villegas, 2008).

Como resultado de la integración de las TIC's en una organización sabemos que traerá de forma inherente nuevos retos como la gobernabilidad y la alineación de los elementos de TI con el giro de la organización, la entrega de valor, gestión de los riesgos, gestión de servicios y sobretodo la seguridad de la información, esta última no es la instalación de herramientas como antivirus, antispyware, firewalls y demás recursos técnicos, sino que es crear políticas, procedimientos, objetivos de control, es planear, organizar, dirigir y controlar (Ruíz, 2010).

Al ejercer la seguridad de la información, existen beneficios para la organización, sin embargo, el no hacerlo o llevarlo de manera empírica y sin los fundamentos necesarios, repercute y nos genera resultados no esperados, por ejemplo, de las organizaciones que sufren una pérdida de datos masiva, más de la mitad de ellas o no regresa a operar o simplemente en los siguientes años se espera su debacle, mientras que sólo un pequeño porcentaje logra reponerse del golpe.

En cifras relacionadas con el fraude y corrupción, más de 70% de las empresas en nuestro país ha tenido algún caso de fraude en el último año y de estos casos más del 40% fue ejecutado por personal de las propias organizaciones, lo que reafirma que la parte humana es la principal área de oportunidad para la seguridad de la información y su implementación (Ruíz, 2010).

2.5 Riesgos del manejo de la información

El concepto de riesgo para norma ISO 31000:2009 está definido como el efecto de la incertidumbre en la consecución de los objetivos, por su parte otros autores lo definen como la secuencia u ocurrencia de diversos eventos, los cuales pueden tener un impacto ya sea positivo o negativo, inclusive ambos a la vez, claro que lo importante es evitar el impacto negativo ya que se traduce en riesgo que impide la creación de valor. Finalmente tenemos un enfoque distinto en donde el riesgo es definido tomando sólo en cuenta la parte negativa en la que deberá tener las siguientes condiciones para poder ser considerado como riesgo: 1) existencia tangible de la probabilidad de una pérdida, y 2) la incertidumbre siempre presente sobre el resultado final (Frick, 2016).

Las avances tecnológicos en nuestros días son una constante y cualquier organización que pretenda triunfar en su respectivo campo deberá estar al día de las nuevas tecnologías funcionales para poder competir en el ámbito tan globalizado en el vivimos, es cierto que entre mayor infraestructura tecnología tiende a tener mayores riesgos basados en la dependencia y seguridad de la misma, ejemplos de elementos de riesgo en una organización son los servidores de correo, web, de datos, intranet y dispositivos móviles, no cabe duda que todos los anteriores son indispensables en la productividad y que sumados con la información que depositamos en ellos deben ser gestionados con mucho cuidado. (Ramos, 2013)

Ramos (2013) asevera que desafortunadamente que en muchas de las organizaciones la seguridad de la información no se toma en serio sino hasta que tanto sus activos y la estabilidad de la organización se ven comprometidos, lo anterior es el resultado de una toma de decisiones que se desarrolló de manera apresurada, sin contar con los métodos y procedimientos serios que favorezcan la continuidad del negocio. Este tipo de incidentes son más comunes de lo que pensamos y la responsabilidad casi siempre se la atribuimos a los virus o a

hackers pero lamentablemente no es así, son descuidos que las organizaciones tienen desde su concepción de lo que es seguridad de la información y por supuesto de lo que valen sus activos, recordar que no es lo mismo seguridad de la información y seguridad informática.

Para la Administración de la Seguridad de la Información, es crítica la elaboración de un análisis y evaluación de riesgos de forma sistemática, de esta manera es posible identificar áreas de oportunidad y evaluar los posibles riesgos asociados con los activos de información, de tal manera que contribuya al seguimiento del progreso con respecto al nivel de riesgo y que esto aporte a una mejora en el proceso de toma de decisiones de la organización (Frick, 2016).

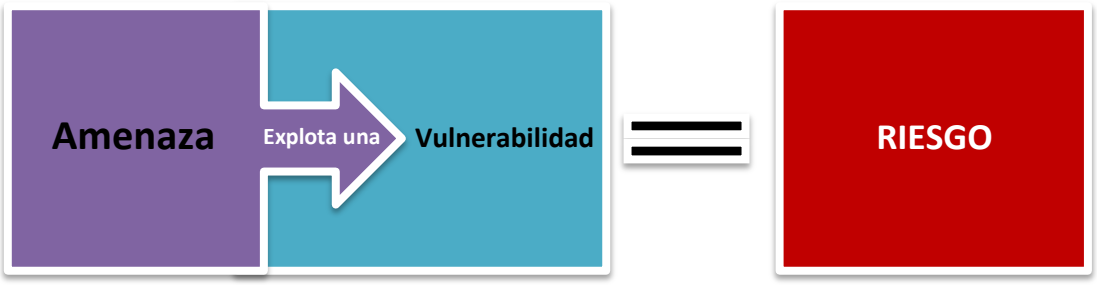
Para que el riesgo sea correctamente detectado y posteriormente tratado, la organización debe comenzar por analizar sus actividades diarias, las de mayor importancia y las que no lo son tanto, el análisis de riesgos es una herramienta que nos brinda el conocimiento de una manera formal que activos son más susceptibles a ser comprometidos y cuáles no.

Denominamos formalmente como activo a todo aquel elemento que es considerado de importancia y que contribuye para que la empresa u organización funcionamiento y alcance los objetivos organizacionales de la mejor manera (Ramos, 2013). No está de más reafirmar que para la empresa u organización el elemento medular para su funcionamiento y productividad es la información ya sea de forma física o digital (tangible o intangible) y que pueden estar presentes en lo que se conoce como activos de Información que son todos aquellos medios o dispositivos que nos ayudan para almacenarla, procesarla y transferirla.

Las escalas para clasificar un activo pueden ser de tipo cualitativas o cuantitativas, las primeras relacionadas como por ejemplo con cuestiones de reputación y prestigio, percepción y las segundas con el valor monetario de que implica la perdida y violación de este (Ramos, 2013).

Para determinar con mayor precisión el riesgo al que se ve expuesto el activo debemos tener en cuenta la severidad del riesgo, su probabilidad, su recurrencia, su magnitud, el costo y que tan efectivo puede resultar la aplicación de controles vs el costo de la aplicación. Tenemos que definir el alcance del análisis, segmentar por áreas, procesos y llevar acabo la clasificación de activos, identificar amenazas, vulnerabilidades, posible impacto y probabilidad basada en el posible daño en caso de que la amenaza explote la vulnerabilidad, posteriormente determinar y proponer medidas para mitigar cualquier inconveniente que surja (González y Martínez, 2008) (figura 7).

Figura 7. Riesgo



Fuente: Elaboración Propia

Otro factor muy importante en el tema de riesgos en la seguridad de la información es identificar las amenazas que puedan afectar a nuestros activos, dichas amenazas como en el tema de las vulnerabilidades las existen internas y externas, con las primeras debemos tener mayor cuidado, claro, sin volvernos paranoicos pensando que el enemigo lo tenemos en casa, mientras que con las externas la maniobrabilidad resulta ser un poco menos compleja.

Una amenaza puede concebirse como todo aquello que intente o pretenda afectar incluso destruir un activo, las amenazas pueden clasificarse dependiendo de su origen, lo pueden ser naturales (desastres naturales), infraestructura como software, hardware y por supuesto el humano (Maza y Cabrera, 2013).

Una amenaza intrínsecamente tiene el potencial de provocar un daño a los activos, los cuales pueden ser información, procesos y sistemas de información

(Ramos, 2013). Como ejercicio medular para identificar y determinar todos los elementos antes mencionados es indispensable llevar a cabo el análisis FODA de nuestra organización con respeto a la información y la manera en que actualmente la manejamos.

Hoy en día las organizaciones no tienen que partir de cero para llevar a cabo un análisis de riesgos adecuados, así como, poder comenzar a implementar la seguridad de la información, existen organizaciones, estándares y marcos de gestión de riesgos y seguridad de la información que se pueden tomar como base y punto de partida para su correcta implementación, entre los que se encuentran:

- ISACA (Information Systems Audit and Control Association) con COBIT 5 The Risk IT Framework, Enterprice Value: Governance of IT Investments, The Val IT Framework.
- COSO (Committee of Sponsoring Organizations of the Treadway).
- NIST(US National Institute of Standards and Technology)
- ISO 31000:2018
- La familia ISO/IEC 27000
- ISO/IEC 31010 (Frick, 2016).

2.6 Convergencia con el proceso administrativo

La administración es una acción indispensable en cualquier organización, es la herramienta más poderosa para la permanencia y competitividad, a través de sus técnicas y procesos se logra mayor rapidez, efectividad, productividad, eficiencia y calidad. El proceso administrativo es el nombre que se le da al conjunto de funciones administrativas, incluyendo la planeación, organización, integración, dirección y el control (figura 8), el proceso administrativo es cíclico, dinámico e interactivo (Münch, 2014).

Figura 8. El Proceso Administrativo

Fuente: Elaboración propia

Para Münch (2014) la planeación se presenta como la primera función administrativa por ser la base de las demás Es la proyección de escenarios futuros y el rumbo hacia donde se dirige la empresa u organización, así como los resultados y objetivos que se pretenden obtener y llegar mediante las estrategias para lograrlos minimizando los riesgos, se trata de un modelo teórico para la acción futura.

La organización es el diseño y determinación de los procesos, estructuras, funciones y responsabilidades, con el establecimiento de métodos y técnicas encaminadas a la simplificación del trabajo, gracias a esta se obtiene: reducción y eliminación de los costos y duplicidad e incremento de la productividad

La Integración es la función a través de la cual se eligen y obtienen los recursos necesarios para poner en marcha las operaciones, en ella se comprenden recursos materiales, tecnológicos, financieros y humanos. (Hernández, 2006).

La dirección por su parte consiste en la ejecución de todas las fases del proceso administrativo mediante la conducción y orientación de los recursos y el ejercicio del liderazgo, en otras palabras es poner en acción y dinamizar la empresa, es llevar a cabo los planes de acuerdo con la estructura organizacional, mediante la guía de los esfuerzos del personal a través de la motivación, la toma de decisiones, la comunicación y el ejercicio del liderazgo, es en la dirección donde se realiza todo lo previamente planeado y se ejecutan todos los elementos de la administración.

En la etapa de control se establecen estándares para evaluar los resultados con el objetivo de corregir, prevenir y mejorar continuamente las operaciones (Münch, 2014).

Tiene la finalidad de contribuir con:

- Una mejora continua
- La detección y prevención de errores o fallas
- Tener una retroalimentación del proceso
- Aseguramiento de la calidad
- Comprobar la eficiencia de la gestión

Es la fase donde se evalúan los resultados obtenidos con relación a lo planeado.

Haciendo una analogía etapa por etapa del proceso administrativo y extrapolándolo a la seguridad de la información tenemos los siguientes aspectos identificados.

Para la planeación, la empresa u organización debe hacer un profundo análisis de las áreas de oportunidad y sus fortalezas en términos de infraestructura y procedimientos relacionados con la gestión de la información, concretamente echar mano de herramientas como el FODA enfocándolo a la gestión de la información, lo anterior servirá como punto de partida para la proyección de

futuros escenarios en donde intervengan nuevas tecnologías, es fundamental hacer una investigación de estas últimas para saber cuáles serían aplicables a nuestro entorno, para aumentar la compatibilidad y lograr el éxito.

Para la organización, determinar los actores que manejaran la información y crear perfiles de gestión, previo una adecuada concientización y capacitación del personal acerca de la importancia del tema y como la aplicación de medidas pueden ayudar al mejoramiento de los procesos internos haciéndolos más seguros y confiables basados en metodologías y estándares ISO ya comprobados enfocándolos en la integridad y disponibilidad de la información, evitar redundancia en los procesos y hacer más eficiente la gestión de la información (Daltabuit et al., 2007).

Para la integración, en esta etapa se debe hacer la conjunción de los elementos anteriores como el análisis interno de nuestros activos, identificación de los actores y sus funciones, herramientas de infraestructura, elementos clave como métodos o referencias ISO (la familia 27000 es un buen marco de referencia) y de ser necesario considerar recursos financieros que provean liquidez para solventar eventualidades en la puesta en marcha.

Para dirección, en esta etapa debe ser llevada por personal capacitado en el tema de la seguridad de la información para que la ejecución del total de las etapas se lleve de manera adecuada y en caso de algún contratiempo le dé buen cause, motivando y concientizando al personal, enfatizando que lo que se está realizando está encaminado al bienestar de todos ya que la información es el principal activo de la institución y fuente de trabajo (González y Martínez, 2008).

Para el control, una vez que se establecieron las medidas y estándares previamente se contrastan con los resultados esperados, parámetros a tomar en cuenta pueden ser tiempo de atención, tiempo en los procesos, eventos de seguridad reportados antes y después de la implementación de los controles de

seguridad, con la finalidad de evitar y no redundar en burocratismos a su vez de proteger de mejor manera nuestros activos.

Como se puede observar, al igual que en muchas otras disciplinas o actividades tanto individuales o como parte una organización el proceso administrativo tiene suficiente cabida y aplicación y la seguridad de la información no es la excepción.

Desde siempre la información ha sido relacionada como fuente del conocimiento y de poder, ya que a través de ésta se facilita el desarrollo de habilidades que potencialicen, fortalezcan y hagan crecer al individuo en todas sus áreas. En la llamada era del conocimiento, el factor humano es el principal elemento para una organización y sociedad competitivas, mientras que a mediados del siglo XX en nuestro país tenía una escolaridad promedio de 2.19 años, en países como Singapur en Asia contaban con 2.71 años, para el año 2010, el país asiático alcanzó un promedio de casi 11años de escolaridad, en comparación con México que apenas llegó a casi 9 años de escolaridad (Ríos y Ramírez, 2016).

En el aspecto económico el país asiático alcanzó un PIB per cápita cinco veces mayor el de México, se puede observar la relación de educación y el crecimiento económico, es decir, un país mejor preparado se traduce en una económica más fuerte y parte medular de una mejor educación es el acceso a acervos de mayor y mejor información y por ende generación de nuevos conocimiento y para todo lo anterior es necesario una gestión optima de la información (Luna, Bojórquez y Hofmann, 2015)

Al igual que en cualquier organización ya sea de tipo lucrativa o no lucrativa, pública o privada, la información es importante para el desarrollo de un sin número actividades de muy diversa índole y que decir de una institución educativa que maneja información que va desde historiales académicos de alumnos, material académico de profesores, artículos científicos, acervo

bibliográfico, material audiovisual, tesis, pasando por los diversos trámites administrativos que representan el funcionamiento cotidiano de una institución educativa escolaridad (Ríos y Ramírez, 2016).

Es por ello que al igual que cualquier otra empresa u organización debe tener el suficiente cuidado en el manejo, almacenamiento, consulta y procesamiento de la información, muchos pueden pensar que la información de una dependencia educativa es de menor categoría o rango que la de una empresa sin embargo no es así ya que al no tener una buena forma de manipular dicha información se corre el riesgo de caer en manos fraudulentas y que hagan mal uso de ella, poniendo en riesgo la vida académica de muchos individuos y finalmente en la credibilidad y la reputación de la institución educativa a la que le suceda (Luna et al., 2015).

Una información mejor administrada en una institución educativa repercute en mejores servicios educativos, posibilitando el perfeccionamiento en procesos de control y difusión de información, acervos del conocimiento y cultura, permeando de mejor manera a las esferas sociales, culturales y científicas con las que se relaciona.

2.7 El futuro de la información y su seguridad

La digitalización trajo una serie de cambios radicales en la administración de la información que evidentemente influyen de manera directa e importante en el saber humano y generación del conocimiento, que modifica hábitos, costumbres y que al final del camino cambia la forma de pensar del ser humano (Adell, 2017).

Si miramos hacia el horizonte, podremos observar que las tecnologías de la información y forma en que gestionamos la información seguirán alcanzando niveles superiores que al momento resultan inimaginables hasta llegar al punto en el que sean tan cotidianas y tan indispensables que solamente nos daremos cuenta de ellas cuando nos hagan falta, el oxígeno es un buen ejemplo, es un

elemento tan importante, común y necesario para la vida que sólo lo recordamos cuando nos falta la respiración. La llamada Ley de Moore se hace presente en este tema, afirmando que la potencia de computo, específicamente la de los procesadores se duplica por cada par de años mientras que el costo de reduce considerablemente (Pisani, 2003).

Zapien (2013) nos habla que en esta década ya estamos viviendo el llamado cómputo en la nube en donde podemos tener la posibilidad de almacenamiento y gestión “infinitos”, la tercerización de los servicios tecnológicos serán muy importantes para cualquier organización incluyendo las educativas, teniendo como ventajas:

- Reducción en los costos para la institución
- Ahorro de recursos financieros destinados a licencias de software
- Una disponibilidad superior
- Aplicación de infraestructura de seguridad dedicada

Sin embargo no todo es miel sobre hojuelas tiene sus desventajas como:

- La pérdida del control de tu propia información, claro existen acuerdos de confidencialidad pero ya existe un tercero que gestiona tu información
- La seguridad depende de una solo elemento o punto de falla
- Dependencia total de infraestructura ajena

El cómputo en la nube sin duda es sinónimo de potencia y capacidad que no deja de ser un equipo remoto en el cual existe un riesgo latente de que sea comprometido o tenga una falla física y la información se vea afectada.

Algunos visionarios proponen y aseguran que al final la información estará en sistemas de gestión distribuidos, cuya característica será que la información permanecerá dispersa en redes públicas y privadas y en movimiento evitando que la información se quede almacenada en un solo lugar evitando o haciendo más

difícil que sea afectada y como consecuencia la estabilidad de la organización se vea comprometida (Pisani, 2003).

Sin temor a equivocarnos surgirán nuevas maneras y formas de codificación de la información, así como su almacenamiento y los canales de transferencia en el que desplaza, seguirán las revoluciones tecnológicas en términos de almacenamientos, consulta, transmisión y resguardo, los estándares internacionales y políticas seguirán evolucionando tratando de emparejarse en esta carrera con las nuevas tecnologías y en su conjunto forman parte la sociedad de la información.

Capítulo 3. Contexto y panorama de la seguridad de la información

3.1 Contexto Local

Como ya lo hemos visto una de las principales prioridades de cualquier organización que tenga entre sus metas organizacionales la continuidad y el éxito debe preocuparse por una adecuada custodia de su información, en la actualidad el flujo de información que manejan las organizaciones sumado a la necesidad del uso de las TIC's, proyecta una tendencia creciente cuyo comportamiento tiende a ser de tipo exponencial y que hasta el momento no se observan indicios de frenar su acelerado crecimiento (Ramos, 2013).

Las instituciones bancarias por dar un ejemplo, son víctimas cotidianas de intentos de robo de información, en muchos de los casos se quedan en eso y en otros, logran su objetivo de extraer datos de cuentahabientes incluso y realizar operaciones bancarias fraudulentas como fue el caso del Sistema Bancario Mexicano y la herramienta denominada SPEI (Sistema de Pagos Electrónicos Interbancarios) en donde fuentes extraoficiales aseguran la perdida de mucho dinero (BANXICO, 2018).

Por semanas el sistema bancario nacional fue noticia ya que las consecuencias del robo fueron la sustracción de entre 300 y 400 millones de pesos del Sistema Financiero Nacional la noticia vio la luz el pasado mes de abril del año 2018 en donde la infraestructura de diversos bancos que se conectan al sistema SPEI del Banco central de México fue vulnerada, si bien toda la nota gira entorno a elementos de servidores, redes, programación y demás elementos tecnológicos el origen del problema aún es más básico y resulta ser una falta o una deficiente supervisión de los procesos y mecanismos efectivos en la custodia de la información (López, 2015).

Existen diferentes líneas de investigación pero todas inician o terminan con el factor humano, que van desde que las instituciones financieras contrataron a un

proveedor externo para la programación de sus herramientas para la cual tuvieron que proporcionarles todas las credenciales, información de sus procedimientos de conexión y demás información sensible relacionada con el lugar de las cuentas concentradoras del dinero, al parecer confiando en la buena voluntad del proveedor, extrañamente la mayoría de los bancos que perdieron dinero contrataron al mismo proveedor para el desarrollo de sus herramientas (López, 2015).

Por otro lado existe la versión que sólo se trató de personal interno de los bancos cosa poco creíble que todos al unísono decidieran realizar la misma acción en contra de sus propios bancos y aunque así hubiera sido llegaríamos a la misma conclusión, la mala gestión en el resguardo de la información sensible (credenciales de conexión) sería visible.

Y una última es la conjunción de los elementos internos y externos para llevar la acción, al parecer es la más aceptada, miembros del sistema bancario nacional en trabajo conjunto con agentes externos y consientes de las deficiencias de los procesos de custodia y supervisión de información sensible decidieron explotar esos esas vulnerabilidades (López, 2015).

El ejemplo anterior no intenta hablar o hacer un análisis tecnológico, por el contrario, simplemente tiene como objetivo mostrar como una mala gestión de la información sumado con áreas de oportunidad al momento de implementar la seguridad de la información pueden provocar grandes problemas incluso a gigantes del sistema financiero.

La cantidad de ejemplos puede ser amplia y tienen algunos factores en común son procesos inadecuados, tipo de infraestructura, su administración y principalmente el factor humano este último es el eslabón de la cadena y muchos de los casos representa el más débil de los eslabones.

Entre las organizaciones que manejan grandes cantidades de información están las instituciones, para muestra tenemos a la Universidad Nacional Autónoma de México (UNAM) la cual debe administrar expedientes de alumnos de los diferentes de niveles escolares y académicos de todas las dependencias adscritas a esta, así como planes de estudio y demás tramites escolares como Becas, movilidad nacional e internacional, acervo bibliográfico, investigación, proyectos, productos editoriales, entre muchos otros que tienen relación con la vida académica, a continuación se muestra algunas cifras relacionadas (tabla 2 y 3) (UNAM, 2019).

El resguardo físico y/o digital de cada expediente es tarea importante, ahora imaginemos los procesos relacionados con la información de la población universitaria.

Tabla 2. Población escolar

2017-2018

	Primer Ingreso	Reingreso	Total
Posgrado	**11,684**	**18,626**	**30,310**
Sistema Escolarizado	11,601	18,592	30,193
Sistema Universidad Abierta	83	34	117
Licenciatura	**46,749**	**157,442**	**204,191**
Sistema Escolarizado	38,705	133,171	171,876
Sistema Universidad Abierta y Educación a Distancia	8,044	24,271	32,315
Bachillerato	**36,953**	**77,163**	**114,116**
Escuela Nacional Preparatoria	16,781	35,339	52,120
Colegio de Ciencias y Humanidades	19,424	40,144	59,568
Iniciación Universitaria	748	1,680	2,428
Propedéutico de la Facultad de Música	**231**	**667**	**898**
T O T A L	**95,617**	**253,898**	**349,515**

Fuente: Dirección General de Planeación, UNAM

Tabla 3. Personal Académico 2018

Total de académicos	**40,578**
Total de nombramientos académicos	**49,279**
Investigador	2,659
Profesor de Carrera	5,503
Técnico Académico	4,496
Profesor de Asignatura	31,792
Ayudante de Profesor	4,642
Otros	187

Fuente: Dirección General de Planeación, UNAM

Por otro lado tenemos los procesos y manipulación de información relacionados con el funcionamiento de las propias dependencias de la universidad (tabla 5) entre las que podríamos mencionar como la oferta educativa (tabla 4) contar compras y suministros, contratos, investigaciones académicas, planes de estudio, etc.

Tabla 4. Oferta Educativa 2018

Programas de posgrado	**41**
Planes de estudio	**92**
Doctorado	36
Maestría	56
Programas de especialización	**42**
Especializaciones	246
Licenciaturas (carreras)	**122**
Opciones educativas	221
Técnico profesional	**36**
Bachillerato	**3**

Fuente: Dirección General de Planeación, UNAM

Tabla 5. Entidades Académicas

PLANTELES DE EDUCACIÓN MEDIA SUPERIOR 2018	
Escuela Nacional Preparatoria	9
Colegio de Ciencias y Humanidades	5
PLANTELES DE EDUCACIÓN SUPERIOR 2018	
Facultades	15
Unidades multidisciplinarias	5
Escuelas nacionales	8
CENTROS E INSTITUTOS DE INVESTIGACIÓN 2018	
Investigación científica	**30**
Institutos	23
Centros	7
Investigación humanística	**18**
Institutos	11
Centros	7

Fuente: Dirección General de Planeación, UNAM

Lo anterior es una pequeña muestra de un mundo de manejo y gestión entorno de la información, la ANUIES (Asociación Nacional de Universidades e Instituciones de Educación Superior) cuenta con 195 instituciones de educación superior de todo el país.

Ahora bien, Imaginemos que pasaría si debido a un problema en los protocolos o mecanismos relacionados con la seguridad de la información se perdiera parte o la totalidad de los expedientes académicos de alumnos, académicos, o por otro lado cayeran en manos de personas con no muy buenas intenciones, las consecuencias serían bastante severas.

Si echamos un vistazo a nuestro alrededor, podremos darnos cuenta que nuestro país se encuentra ya en este nuevo esquema mundial de la comunicación,

podemos reflexionar en él un sin número de actividades relacionadas con la información y cuyo actor principal es ésta última, ejemplo de ello son los correos electrónicos de carácter empresarial y personal que realizamos, en el sector financiero las transacciones bancarias, consultas masivas de información, educación virtual o en línea y todo el sin número de actividades de entretenimiento y esparcimiento que conlleva esta gran conectividad global (Ramos, 2013).

Los esfuerzos realizados para que nuestro país esté siempre conectado son importantes, instituciones públicas y privadas invierten gran parte de su capital para mantenerse a la vanguardia, sin duda se requiere que el gobierno federal contribuya aún más en dicho campo, asignar mayor presupuesto a la ciencia y tecnología son parte medular, ya que mucho de esto tiene que ver con la generación del conocimiento y las nuevas tecnologías de la información, así como los elementos para su protección (Márquez, 2015).

Si bien nuestra nación intenta ponerse a la vanguardia en temas tecnológicos, el asunto de la seguridad de la información no se encuentra del todo maduro, mientras otros países del mundo ya cuentan con leyes regulatorias acerca del tema e incluso firman convenios internacionales con otras naciones, México sigue como un simple observador, sin convertirse en un elemento activo y formar parte de los diversos convenios que surgen y se desarrollan en el planeta (Ramos, 2013).

Muestra de lo anterior es que nuestro país ha sido testigo de la firma del Convenio de Budapest que se llevó a cabo en Hungría. En dicho convenio aún no ha sido ratificada la adhesión de nuestro país a pesar de las diversas ventajas que podría aportar a nuestra nación, tales como la de reforzar políticas, la definición de estrategias, así como el establecimiento de una legislación adecuada y aplicación de medidas prácticas sobre el cibercrimen y la seguridad cibernética en el país, el Convenio nos permitiría robustecer nuestras leyes y regulaciones

contra el cibercrimen de todo nivel, así como en el progreso en temas de cooperación internacional contra delitos informáticos (Ramos, 2013).

Adicionalmente y durante la Conferencia Octopus sobre la Cooperación en contra del Cibercrimen realizada en Estrasburgo Francia, se discutió sobre la vinculación de la protección de datos personales con las posibles estrategias contra los crímenes cibernéticos que se establezcan en cada país, lo anterior debido al incremento de la incidencia del robo de información personal con fines delictivos a nivel global, claro que México estuvo atento al evento, sin embargo se requiere que pase de ser un miembro pasivo de las reuniones y se convierta en un elemento activo con mayor participación y compromiso para aplicar dichas recomendaciones. (Pérez, 2014).

De forma imperativa nuestro país debe de tomar acción al respecto, de acuerdo a cifras proporcionadas por el Instituto Federal de Acceso a la Información y Protección de Datos de México (IFAI), el gobierno mexicano tiene poco más de 3000 bases de datos registradas tan solo a nivel Federal, de las cuales, aproximadamente el 97% contiene sólo información básica de identidad, en tanto que el 3% restante, reúne datos personales sensibles tales como origen étnico, de salud o información genética, religión, así como preferencias sexuales, creencias políticas, entre otros datos. Del mismo modo, se encuentra que por lo menos el 90% usuarios cotidianos de Internet en nuestro país han brindado datos de identificación por este medio, los datos más comunes son: nombre, edad, dirección, RFC, CURP, género y fotografías; sin dejar de lado los portales de banca en línea, tiendas online, y redes sociales etc. Estas últimas tres son por excelencia los lugares en donde los datos personales tienen mayor índice de intercambio (Ramos, 2013).

La tendencia es que todos los países deben considerar tanto las políticas de protección de datos como la ciberseguridad como parte de los derechos fundamentales de los ciudadanos para tener sociedades democráticas completas.

Con el compromiso de luchar por este objetivo en México Jacqueline Peschard en su periodo como comisionada presidenta del IFAI manifestó interés en sumarse al Convenio 108 del Consejo de Europa (CE) para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos Personales, en años posteriores diversos diputados han presentado diversas iniciativas para mejorar y afinar aún más la Ley Federal de Protección de Datos Personales, los esfuerzos son aislados y a cuenta gotas sin embargo seguimos avanzando (Pérez, 2014).

Sin duda, un aspecto a destacar de la ley antes mencionada es la buena clasificación que planteó acerca de los datos o activos (patrimoniales, financieros y sensibles), división que ha resultado benéfica para la normatividad. Los órganos federales encargados de vigilar el cumplimiento de dicha ley son la Secretaria de economía y el Instituto Federal de Acceso a la Información y Protección de Datos, que incluso pueden sancionar en caso de transferencia no autorizada de datos sin consentimiento del titular, el obtener datos de cualquier empresa mediante engaños y el almacenamiento de datos sensibles sin propósito alguno que no sea autorizado por el propietario es un delito. (Ramos, 2013).

México va por el camino correcto, sin embargo debe apretar el paso aún más, ya que mientras nuestro país lo hace de forma pausada, algunas otras naciones se encuentran en plena carrera tecnológica sin mirar atrás, si bien no podremos ponernos a la altura de grande potencias, sí podemos hacer nuestro mejor esfuerzo por mejorar o solventar las áreas de oportunidad que se nos presentan actualmente de manera más ágil, todo en beneficio de un futuro más prometedor de nuestra población.

3.2 Contexto Mundial

Desafortunadamente México y Brasil se disputan el primer lugar entre los países de Latinoamérica que registran mayor actividad maliciosa de tipo informático y de seguridad de la información, seguidas de Argentina y Colombia

según informe de una prestigiosa empresa dedicada al diseño y programación de antivirus.

A nivel empresarial la pérdida de información debida a actividad maliciosa y la falta de un buen manejo de la información, se traduce a una afectación de más de 500 millones de personas en el mundo en los últimos años, de los cuales un 20% está relacionado por el mal manejo y administración de los datos dentro de su organización y que decir de las 10 millones de personas por año que se ven vulneradas al ser víctimas de robo de identidad (Ramos, 2013).

Por exponer algunos ejemplos la compañía Facebook estuvo involucrada en un escándalo de robo de información siendo ella la victima al no seguir procedimientos seguros para el resguardo y manejo de la información de sus usuarios, lo anterior porque una compañía de análisis de datos relacionada con la campaña presidencial del entonces candidato Donald Trump pudo acceder y almacenar una gran cantidad de información de los usuarios de esa red social (Riley, 2018).

Todo se dio a conocer cuando medios de comunicación de los Estados Unidos y la Gran Bretaña revelaron que la empresa dedicada al análisis de datos Cambdridge Analytica pudo haber influido en la victoria de Donald Trump al robar millones de perfiles de Facebook y con esa información diseñar algoritmos y mecanismos para influir en la elección de esos votantes.

Facebook dio permiso a un profesor de psicología de la Universidad de Cambridge para aplicar un test mediante una supuesta aplicación que recopilaba cierta información de los usuarios, según el profesor era una simple prueba de personalidad pero la finalidad era muy diferente y Facebook no se percató de ello (Riley, 2018).

En efecto, la aplicación era una prueba de personalidad pero al instalarla los usuarios autorizaban el compartirle datos más personales como amigos relacionados, gustos, ubicación y demás aspectos que serían utilizados para otro fin; una vez hecho lo anterior el profesor entregó más de 50 millones de perfiles a la empresa Cambridge Analytica para uso y análisis (BBC, 2018).

En ese momento Cambridge Analytica trabajaba en desarrollar técnicas de influencia psicológica y de todo tipo para ser aplicadas a usuarios y tratar de cambiar sus comportamientos, claro nada impedía aplicarla a futuros electores, posteriormente se supo fue contratada para darle asesoría a la campaña de Trump según declaraciones del personal que trabajó en la empresa.

El presidente ejecutivo de Facebook Mark Zuckerberg negó que su plataforma se haya prestado para tal fin, lo que sí es una realidad es que desde esos momento la empresa hizo grandes cambios al interior de la misma y en sus algoritmo, si bien Facebook basa su sistema de negocio en vender información de sus usuarios a los anunciantes y marcas que le piden sus servicios, nunca pensó que un tercero se metiera al centro de sus bases de datos y sustrajera su información (Riley, 2018).

Por supuesto que las dos empresas tanto Cambridge Analytica como Facebook están bajo investigación por la Unión Europea, la Gran Bretaña y autoridades Estadounidenses ya que existen varios responsables, autoridades de los Estados Unidos señalan que plataformas como esas no pueden controlarse a sí mismas y que requieren mayor supervisión y control del estado lo que se traduciría en la ruina de la empresa de Zuckerberg (BBC, 2018).

Es un hecho que la empresa fue vulnerada, a pesar de ser un monstruo tecnológico el manejo y resguardo de su información no fueron las adecuadas en ese momento, sus procesos y protocolos relacionados con la información fueron

tan malos que le acarrearon problemas económicos, de reputación y credibilidad para sus clientes e inversionistas

Para cualquier negocio la parte económica es fundamental y en este caso Facebook en solamente un día vio como sus acciones caían más de 37 millones de dólares lo que representaría casi un 7% del valor y esto debido al escándalo del famoso test de personalidad que se relacionaban directamente con acusaciones de robo de datos, chantajes e intromisiones de carácter político (BBC, 2018).

El problema no paro ahí ya que algunas otras naciones en el mundo comenzaron a tener desconfianza sobre esa plataforma, países de Latinoamérica como Argentina, Brasil, Colombia, México entre otros externaron su preocupación por el asunto de robo de información ya que al igual en que casi todo el mundo la firma se encuentra presente. Lo que resulta un poco contradictorio es que la empresa ha prestado sus servicios por más de 25 años y se han involucrado en más de 100 campañas políticas en diferentes partes del mundo entre los que se encuentran justamente los países antes mencionados (Riley, 2018).

La información fue y será el insumo más importante para todos, en esta era de la información y comunicación como ya vinos resuelve o ayuda a campañas políticas, influencia directa en gobiernos, cambio de cultura, venta de productos y éxito de las compañías pero su mal manejo repercute en su reputación, bancarrota y desaparición de cualquier institución u organización.

Un ejemplo más de lo acontecido en el mundo y en donde la información es el centro y el origen de toda controversia está registrado en el año 2010 y lleva el nombre de Wikileaks está muy relacionado con la seguridad de la información, la privacidad y confidencialidad (Pacheco, 2011)

Wikileaks es una organización que desde el año de 2006 permite que personas de manera libre, sin filtros y anónimamente puedan subir al sitio web

información de interés público, se tiene que para el año de 2010 se publicó en ese sitio más de 250000 mensajes entre las embajadas del mundo y el Departamento de Estado del país más poderoso del Mundo lo que se traduce en la mayor filtración de documentos oficiales secretos de la historia del mundo, dicho caso refleja que nadie se encuentra exento del peligro de robo de información eso incluye al departamento de estado de una potencia como lo es el vecino del norte (Pacheco, 2011).

Para mitigar muchos de los problemas mencionados las corporaciones basan su administración en estándares internacionales y normatividad relacionada, contrario a lo que la mayoría puede pensar los estándares o marcos de referencia son apoyo para cualquier organización sin importar su tamaño y giro, no se tiene que ser una transnacional o multinacional para intentar implementarlos y llevarlos a la practica en beneficio de su organización ya que la información es tan importante como el dinero que se encuentra en sus cuentas bancarias (Márquez, 2015).

El esfuerzo de la comunidad internacional es evidente, la gran cantidad de espacios, el surgimiento de organismos internacionales encargados de normar y recomendar acciones para un mejor manejo de la información y la aplicación de la seguridad de la información son muestras de ello, otro ejemplo es que el Consejo de Europa que a través de la realización de eventos como convenciones y conferencias enfocadas a resolver problemas relacionados con la seguridad de la información, reúnen a la mayor cantidad de expertos en el tema, congregando a más de 80 naciones, empresarios, organizaciones públicas y privadas con el fin de mejorar la cooperación contra el cibercrimen en todos los niveles (Ramos, 2013).

Otro esfuerzo palpable de la comunidad internacional es el convenio de Budapest resaltando que es el único acuerdo internacional que permea aspectos relevantes de carácter legislativos y enfocados al derecho penal, derecho procesal y la cooperación internacional, tratando de enfatizar la importancia de crear

política penal contra el robo y mal uso de la información, para que en cada uno de los miembros que forma parte del convenio se avale la transnacionalidad a la persecución del delito y evitar así, que los ladrones de información al pasar a otro país eviten hacer frente a la justicia (Pérez, 2014).

Dicho convenio garantiza el respeto a sus derechos y libertades a los ciudadanos y organizaciones de los país incorporados, principalmente a la libertad de mantener su información privada sensible e intocable y en caso contrario, ejecutarla para que caiga todo el peso de la ley a quien intente robar dicha información. Estructuralmente hablando, el convenio consta de 27 artículos distribuidos en 7 capítulos en donde el objetivo es la garantía al respeto de los derechos y libertades de toda persona sin distinción de su nacionalidad respecto a la manipulación de sus datos ya sea en el sector público o privado (Ramos, 2013).

Claro está que lo más importante es la custodia de la información y los procesos que intervienen en ella, sin embargo se requiere también de una parte fundamental como lo es tener un verdadero control interno y contar con unos componentes sólidos, entre los marcos de referencia y estándares internacionalmente reconocidos.

Mediante el esfuerzo coordinado de diversos organismos internacionales se han creado marcos de referencia indispensables, que son parte medular para una buena gestión de la información, control interno, administración de riesgos, así como de su seguridad (Ramos, 2013).

Entre los más importantes se presentan el marco de referencia COSO 2013 para la implementación de un buen control interno en una organización, el trabajo debe comenzar desde dentro, otro es la serie de los estándares de la familia ISO 27000 resaltando por su importancia el ISO/IEC 27001, ya que en él se presentan los requisitos que deberá poseer un sistema de gestión de seguridad de la información y el ISO/IEC 27002, que es una guía de buenas prácticas donde se describen los objetivos de control y los controles que se recomiendan enfocados

en mantener la seguridad de la información, éstos últimos son tan importantes que cualquier organización a nivel mundial, no debe dejar pasar por alto y debe consultar para llevarla cabo y más aún en esta era de la información, comunicación y conocimiento en la que vivimos (Ruíz, 2010).

Capítulo 4. Normas internacionales, controles o marcos de referencia como herramientas para la estrategia de gestión de la seguridad de la información en una organización

4.1 Metodología COSO Versión 2013 “Control Interno”

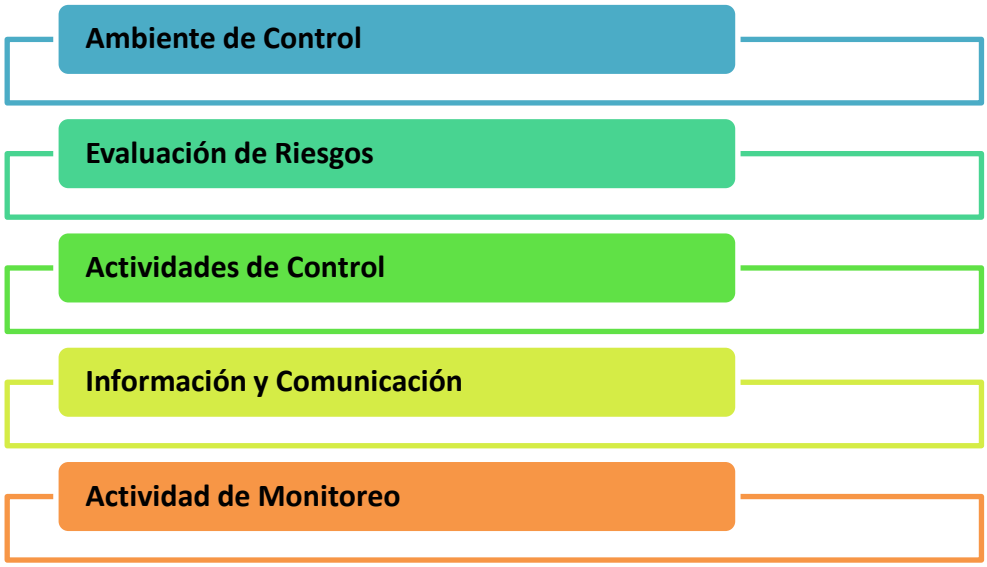
COSO (Comité de Organizaciones Patrocinadoras de la Comisión Treadway) es un Marco de referencia integral enfocado al control interno de una organización, surgido en el año de 1992 es ampliamente reconocido y aceptado en el mundo, se enfoca en diseñar, implementar, controlar y evaluar la efectividad del control interno de manera eficiente, la última versión que habla de dicho tema es la 2013, aunque existen otras versiones como la 2017 no se enfocan en el mismo tópico, es decir no sustituye a la 2013, como veremos más adelante la 2017 se centra en el control de riesgo de una organización (COSO, 2013).

El control interno ayuda a las organizaciones a lograr objetivos importantes y a mantener y mejorar el desempeño en forma integral que se basa en principios distribuidos en cinco componentes de control que junto con la aplicación de la seguridad de la información (ISO 27001) y su hermana COSO 2017 dan forma a un tridente que sin duda beneficia de manera importante a cualquier empresa u organización y el alcanzar sus objetivos (COSO, 2017).

4.1.1 Descripción de COSO 2013

Este marco de referencia está formado por cinco componentes los cuales basan su funcionamiento o aplicación en 17 principios de control que se encuentran distribuidos entre todos los componentes, a continuación se describe cada componente de control y sus principios asociados (figura 9).

Figura 9. Componentes de COSO 2013



Fuente: Elaboración propia

4.1.2 Ambiente de Control

En COSO (2013) este componente tiene como propósito que los colaboradores tengan claridad con respecto a la misión, visión, objetivos y las funciones que deben desempeñar, al igual que las políticas que se establezcan, todo lo anterior en marco ético organizacional, para que la aplicación de este componente sea efectivo se deben establecer líneas de mando y estructuras de manera que los colaboradores identifiquen y comprendan su contribución en el logro de los objetivos organizacionales, los principios presentados para este componentes son:

- La organización deberá mostrar compromiso tanto por la integridad como por los valores éticos.
- El Consejo de Administración demuestra una independencia de la administración y ejerce una supervisión del desarrollo y el rendimiento de los controles internos.

- La Administración establece, con la aprobación del Consejo, las estructuras, líneas de mando, reporte y las autoridades y responsabilidades apropiadas en la búsqueda de objetivos.
- La organización demuestra un compromiso con las actividades de atraer, desarrollar y retener personas competentes en alineación con los objetivos.
- La organización retiene individuos comprometidos con sus responsabilidades de control interno en la búsqueda de objetivos.

4.1.3 Evaluación de Riesgos

Cada una de las organizaciones se enfrenta a una serie de riesgos tanto internos como externos, la evaluación de riesgos es un proceso de tipo dinámico e iterativo que nos lleva a identificar y evaluarlos para posteriormente atenderlos, lo que implicaría el logro de los objetivos organizacionales (COSO, 2013).

Una condicionante previa que se debe presentar para la evaluación de los riesgos es el establecimiento de los objetivos, vinculados a los diferentes niveles de la organización, se debe hacer gestión específica de objetivos dentro de las categorías relacionadas con operaciones, informes y cumplimiento de claridad que sea suficiente para ser capaz de identificar y analizar los riesgos a dichos objetivos.

En COSO (2013) la actividad de evaluar los riesgos también requiere que la administración considere el impacto de posibles cambios en el exterior y dentro de su propio modelo de negocio que pueden hacer que el control interno sea ineficiente, los principios a los que responde este componente son:

- La organización determina objetivos específicos y de manera clara para que la identificación y la evaluación de los riesgos asociados sea más precisa.

- La organización identifica los riesgos para el logro de sus objetivos en toda la entidad y analiza los riesgos como base para determinar las acciones de cómo deben gestionarse.
- La organización debe considerar posibles fallas en la evaluación de riesgos por lo que debe hacer sin prisas y bien enfocados en el proceso.
- La organización identifica y evalúa los cambios que podrían impactar significativamente el sistema de controlar.

4.1.4 Actividades de control

Este es el segundo componente del marco de referencia COSO (2013), las actividades de control son todas aquellas acciones establecidas a través de políticas y procedimientos que ayudan a que se lleven a cabo las directivas establecidas por la administración para mitigar los riesgos para el logro de los objetivos. Las actividades de control se deben realizar en todos los niveles de la organización.

Dichas actividades pueden ser de naturaleza preventivas, pueden ser procesos manuales o automatizados utilizando tecnología. La segregación de funciones está comúnmente integrada en la selección y desarrollo de las actividades de control, los principios asociados a este componente son:

- La organización selecciona y desarrolla actividades de control que contribuyen a la mitigación de los riesgos para el logro de objetivos de la organización.
- La organización selecciona y desarrolla actividades de control general con apoyo de la tecnología para contribuir al logro de objetivos.
- La organización implementa actividades de control a través de políticas que establecen lo que se espera y procedimientos que ponen en práctica las políticas acción.

4.1.5 Información y comunicación

La información es necesaria para que la organización asigne responsabilidades de control interno para apoyar el logro de sus objetivos. La alta dirección obtiene, genera y utiliza información relevante y de calidad de fuentes internas y externas para respaldar el funcionamiento de otros componentes del control interno. La comunicación es un proceso continuo e iterativo que consiste en proporcionar, compartir y obtener la información necesaria. La comunicación interna es el medio por el que la información se propaga en toda la organización, que fluye hacia arriba, abajo, y en toda la empresa. Permite al personal recibir un mensaje claro de la alta dirección. La comunicación externa permite saber el estatus y los cambios que está sufriendo el entorno, los principios son los siguientes (COSO 2013).

- La organización obtiene, genera y utiliza información relevante y de calidad para respaldar el funcionamiento de controlar.
- La organización comunica internamente la información, incluidos los objetivos y responsabilidades de control interno, necesarios para respaldar el funcionamiento del control interno.
- La organización se comunica con partes externas sobre asuntos que afectan el funcionamiento del control interno.

4.1.6 Actividades de monitoreo

Las evaluaciones continuas, separadas o alguna combinación se utilizan para determinar si cada uno de los cinco componentes del control interno están presentes y funcionando. Las evaluaciones continuas, integradas en los procesos de la organización proporcionan información oportuna. Los resultados son valorados contra criterios previamente establecidos, los principios relacionados con este componente de control (COSO, 2013).

- La organización selecciona, desarrolla y realiza evaluaciones continuas y / o separadas para determinar si los componentes del control interno están presentes y en funcionamiento.
- La organización evalúa y comunica las deficiencias de control interno de manera oportuna a las partes responsables de tomar medidas correctivas, incluida la administración superior y la junta directiva.

Como podemos ver esta metodología establece los requisitos para un sistema efectivo de control interno que funciona para la implementación de la seguridad de la información. Un sistema efectivo proporciona una seguridad razonable con respecto al logro de los objetivos de una organización. Un sistema efectivo de control interno reduce, a un nivel aceptable el riesgo de no lograr un objetivo como el de no implementar la seguridad de la información, existe una metodología dedicada al apoyo en el tema de control de riesgos que a continuación se presenta.

4.2 Metodología COSO Versión 2017 “Control de Riesgos”

Este proyecto fue encargado por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO), que se dedica a proporcionar un liderazgo innovador a través del desarrollo de marcos y guías integrales sobre control interno, gestión de riesgos empresariales y disuasión de fraudes diseñados para mejorar la organización, el desempeño y la supervisión y para reducir el alcance del fraude en las organizaciones. COSO es una iniciativa del sector privado, patrocinada y financiada por diversas organizaciones entre los que se encuentran contadores, administradores, auditores y ejecutivos financieros.

Durante la última década, este marco de referencia ha ganado una amplia aceptación por parte de las organizaciones que se han enfocado en tratar de gestionar el riesgo, también es una realidad que a lo largo de este tiempo, los origines o fuentes del riesgo han cambiado, han surgido nuevos riesgos y tanto los gerentes como los ejecutivos han mejorado su conocimiento y supervisión de la

gestión de riesgos de la empresa al tiempo que requieren una mayor y mejor información acerca de los riesgos (COSO, 2017).

La administración tiene la responsabilidad general de administrar el riesgo para la organización, pero es importante que la administración vaya aún más lejos utilizando a la gestión de riesgos como una ventaja competitiva.

Dicho sistema de control de riesgos comienza con la implementación de capacidades de administración de riesgos empresariales como parte de la selección y refinamiento de una estrategia. En particular, a través de este proceso es como se puede obtener una mejor comprensión como el riesgo puede impactar en la estrategia (COSO, 2017).

La gestión de riesgos enriquece el diálogo de gestión al agregar una perspectiva de las fortalezas y debilidades de una estrategia a medida que cambian las condiciones, y cómo una estrategia se ajusta a la misión y visión de la organización. Permite que la administración se sienta más segura de que ha examinado estrategias alternativas. Una vez que se establece la estrategia, la administración de riesgos proporciona una manera efectiva para que la administración cumpla su función, sabiendo que la organización está en sintonía con los riesgos que pueden impactar la estrategia y los está administrando bien. La aplicación de gestión de riesgos en la organización ayuda a crear confianza y dar confianza a las partes interesadas en el entorno actual.

El Marco de Gestión de Riesgos COSO (2017) muestra la importancia de la gestión de riesgos en la planeación estratégica y la incorpora a toda la organización, ya que el riesgo influye y están alineados a la estrategia y el desempeño en todas las áreas, departamentos y funciones.

Los cinco componentes (figura 10) del marco actualizado están respaldados por un conjunto de principios, los cuales permean y son aplicables a toda la organización, son manejables en tamaño y describen prácticas que pueden

aplicarse de diferentes maneras para diferentes organizaciones, independientemente de su tamaño, tipo, o sector. Cumplir con estos principios puede proporcionar a la gerencia una expectativa razonable de que la organización entiende y se esfuerza por administrar los riesgos asociados con su estrategia y objetivos organizacionales.

Figura 10. Componentes de COSO 2017

Fuente: Elaboración propia

4.2.1 Gobernabilidad y Cultura

Gobierno de una organización establece la manera en que se manejará y el rumbo que tomará enfocándose en los objetivos y metas organizacionales, por su parte la cultura se refiere a los valores éticos, los comportamientos deseados y la comprensión del riesgo, los principios que se establecen para este componente son:

- La Junta directiva ejerce una supervisión sobre los riesgos
- Establecer estructuras operativas.

- Definir la cultura deseada
- Demostrar compromiso con los valores éticos fundamentales
- Atraer, desarrollar y retener individuos competentes

4.2.2 Estrategia y establecimiento de objetivos

Para COSO (2017) la gestión del riesgo organizacional, la estrategia y el establecimiento de objetivos son elementos fundamentales en el proceso de planeación estratégica, el riesgo es definido, contrastado y alineado con la estrategia, los objetivos ponen la estrategia en práctica mientras tanto vamos identificando, evaluando y respondiendo a los riesgos, los principios de este segundo componente son:

- Analiza el contexto organizacional
- Define apetito de riesgo
- Evalúa Estrategias Alternativas
- Formula objetivos de empresariales

4.2.3 Desempeño

Los riesgos que pueden impactar en el logro de la estrategia y los objetivos deben ser identificados y evaluados, los riesgos son priorizados por la severidad, la organización selecciona las respuestas de riesgo y toma una registro de la cantidad de riesgos que ha asumido. Los resultados de este proceso se informan a los interesados, los principios son (COSO, 2017):

- Identifica el riesgo
- Evalúa la severidad del riesgo
- Prioriza los riesgos
- Implementa respuestas ante los riesgos
- Desarrolla un portafolio (catalogo) de riesgos

4.2.4 Revisión

Al revisar el desempeño de la organización se puede considerar qué tan bien están funcionando los componentes de administración de riesgos de la empresa a lo largo del tiempo y en su caso cuáles serían las revisiones necesarias para implementar en un futuro, los principios asociados a este componente son:

- Evalúa los cambios sustanciales provocados
- Revisiones de Riesgo y Rendimiento
- Buscar la mejora en la gestión del riesgo

4.2.5 Información, comunicación y reportes

La gestión de riesgos demanda de un proceso continuo para obtener y compartir la información necesaria, tanto de fuentes internas como de fuentes externas, que fluya de arriba hacia abajo y en toda la organización, los principios son del componente se presentan:

- Aprovechar la información y la tecnología y echar mano de ellas.
- Comunicar los riesgos de información.
- Llevar a cabo informes sobre riesgo, cultura y rendimiento.

No hay duda de que las organizaciones seguiran enfrentándose con un futuro lleno de volatilidad, complejidad y ambigüedad. La gestión del riesgo será una parte importante de la forma en que una organización se administra y se encamina a un futuro aún más competido. Independientemente del tipo y tamaño de una organización, las estrategias deben mantenerse fieles a su misión y visión, ágiles en su proceso de toma de decisiones, una notable capacidad para responder a los cambios y de adaptabilidad manteniendo altos niveles de confianza en su interior como en su entorno (COSO, 2017).

A medida que nos encaminamos hacia el futuro, hay varias tendencias que tendrán un efecto en la administración de riesgos organizacionales ejemplo de esto son los siguientes:

La proliferación de datos, a medida que más y más datos estén disponibles, la velocidad a la que pueden y deben ser analizados necesariamente deberá aumentar, la administración de riesgos empresariales deberá adaptarse. Los datos tendrán origen tanto interno y externo a la organización y se estructurarán de nuevas formas. Las herramientas avanzadas de análisis y visualización de datos evolucionarán y serán muy útiles para entender el riesgo y su impacto cuando este sea en sentido positivo como negativo (COSO, 2017).

Echar mano y aprovechar de la última tecnología y la automatización, muchas personas sienten que hemos entrado en la era de los procesos automatizados y la inteligencia artificial. Independientemente de las creencias individuales o grupales, es importante que las prácticas de administración de riesgos consideren el impacto de estas tecnologías y las que vienen, y aprovechen sus capacidades. Las relaciones, tendencias y patrones fueron irreconocibles en su momento pueden ser descubiertos, proporcionando una nueva fuente de información crítica para el manejo de riesgos (Maza, 2013).

Una muy frecuente preocupación expresado por ejecutivos de negocios es el costo de la implementación de administración de riesgos, los procesos de su cumplimiento y las actividades de control en comparación al valor agregado obtenido como empresa sin embargo en muchos de los casos el no implementarlo resulta aún más costoso. Los beneficios derivados de la gestión de riesgos superarán por mucho las inversiones y proporcionarán a las organizaciones confianza en su capacidad para manejar el futuro.

La gobernabilidad debe coordinarse eficientemente para proporcionar el máximo beneficio a la organización. Esto representa una de las mayores

oportunidades para que la gestión de riesgo redefina su importancia para la organización (Nicasio, 2015).

A medida que las organizaciones mejoren la integración de la gestión del riesgo con la estrategia y el desempeño, se generarán más oportunidades para fortalecer a la organización y así tener las herramientas para combatir ante cualquier eventualidad y abriéndose camino a nuevas oportunidades.

Las organizaciones necesitan ser más adaptables al cambio. Deben pensar estratégicamente sobre cómo manejar la creciente volatilidad, complejidad del mundo, particularmente en los niveles superiores de la organización que es de donde parte todo, gracias a marcos de referencia como loas COSO 2013 y COSO 2017 podemos conformar bases cada vez más sólidas en el tema de control interno y evaluación de riesgo que serán aplicados en conjunto con marcos de referencia enfocados a la seguridad de la información como el ISO 27001 (Calder, 2008).

4.3 Familia ISO/IEC 27000

En el mundo existen algunas normas internacionales en las cuales podemos basar nuestra implementación de la seguridad de la información, ejemplo de ello es la familia de normas ISO/IEC 27000 que hare una breve semblanza de las ISO más relevantes y que se ajustan para la implementación en una institución educativa y nos centraremos principalmente en las norma ISO/IEC 27001 y 27002, antes de iniciar debemos preguntarnos ¿qué es ISO?

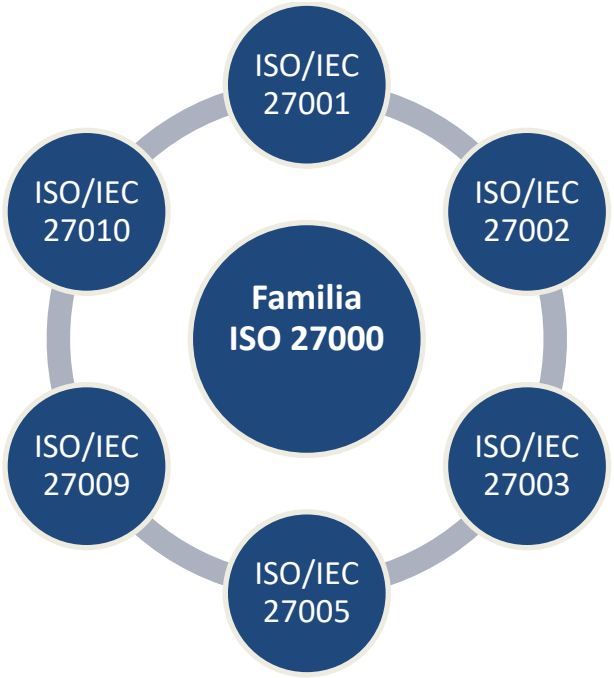
La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) forman el sistema especializado para la estandarización mundial que sumados diversos comités técnicos, organizaciones internacionales, gubernamentales y no gubernamentales colaboran en campos de interés mutuo de las tecnologías de la información y cuya tarea principal es la de preparar estándares internacionales para que una ISO sea publicada se requiere

la aprobación de al menos el 75% de los organismos que emiten un voto (ISO, 2013).

La familia de normas ISO/IEC 27000 es un conjunto de normas desarrolladas y aprobadas por los organismos antes mencionados y que proporcionan todo un marco de referencia para el diseño, desarrollo, implementación, gestión y control de la seguridad de la información para cualquier organización sin importar su tamaño o actividad en la que se desempeñe, en este caso lo abordaremos desde la perspectiva de una institución educativa.

La familia de estas normas está compuesta por más de 30 normas distintas que apuntan al mismo tema que es la seguridad de la información pero con ámbitos bien definidos cada una, a continuación se mencionan las más recomendables a tomar en cuenta para fines de este trabajo de investigación (Beckers, 2011) (figura 11).

Figura 11. Familia ISO 27000



Fuente: Elaboración propia

4.3.1 ISO/IEC 27001

Esta es la norma que funge como estandarte de esta serie ya que en ella se plasman los requisitos para implementar todo un sistema de gestión de la seguridad de la información, cabe hacer mención que la palabra sistema no hace referencia a ningún software u herramienta programada, sino más bien, a todo un conjunto de elementos enfocados y trabajando para un fin común. El anexo A de esta norma enumera los objetivos de control y controles aplicables para la implementación de la seguridad de la información, este anexo hace referencia a la norma ISO/IEC 27002 (Solarte, Enríquez y Benavides, 2015).

4.3.2 ISO/IEC 27002

Esta norma resulta ser una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información aplicables en una empresa, por su naturaleza esta norma no es certificable y su aplicación se hace de forma discrecional, dichos controles se encuentran agrupados en dominios y son la base practica para la implementación de la seguridad de la información (Disterer, 2013).

4.3.3 ISO/IEC 27003

Esta norma tampoco es certificable y se trata de una guía que se centra sólo en los aspectos críticos necesarios para el diseño e implementación con éxito de la seguridad de la información. El propósito de esta Norma Internacional es proporcionar orientación en el desarrollo de la implementación plan de seguridad dentro de una organización de acuerdo con ISO / IEC 27001 (Nicasio, 2015).

4.3.4 ISO/IEC 27005

Provee líneas de acción para abordar el tema de la gestión del riesgo en la seguridad de la información, apoyando y soportando los conceptos generales plasmados en la norma ISO/IEC 27001 y está diseñada para ayudar a la

aplicación de la seguridad de la información con un enfoque de gestión de riesgos, cabe hacer mención que al igual que la norma anterior no certificable (Ruíz, 2010).

4.3.5 ISO/IEC 27009

En esta se definen los requisitos específicos para uso en áreas o sectores específicos que pretendan hacer uso de la norma ISO/IEC 27001, es decir, intenta proponer controles particulares para necesidades específicas de las organizaciones, debido a la naturaleza mencionada se trata de una norma no certificable.

4.3.6 ISO/IEC 27010

Funge como una guía para la gestión de la seguridad de la información cuando se comparte entre otras dependencias u organizaciones, esta norma puede aplicarse en el intercambio y difusión de información tanto local como internacional, dentro de la misma industria, sector o giro al que se dedique la organización, algunos de los controles se pueden observar en el Anexo de la norma ISO/IEC 27001 (Nicasio, 2015).

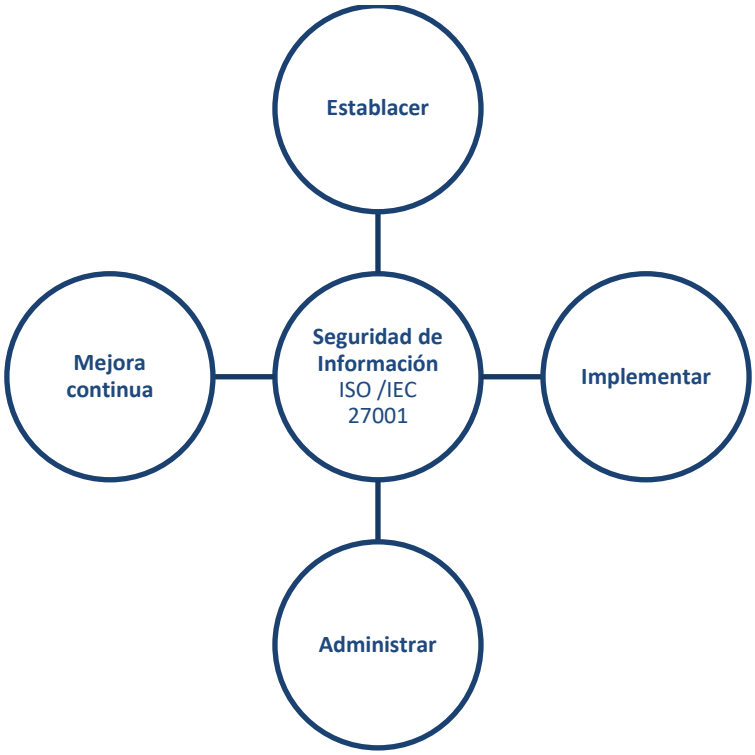
4.4 Profundizando en la ISO/IEC 27001

Como podemos observar todas y cada una de las normas presentadas hace referencia a la norma ISO/IEC 27001 por lo que nos centraremos en el estudio de está y lo que nos puede aportar para la implementación de la seguridad de la información.

La norma ISO analizada es la ISO / IEC 27001: 2013, es decir, pertenece a su segunda edición 2013-10-01 y lleva por Título “Tecnología de la información - Seguridad técnicas - Seguridad de la información sistemas de gestión – Requisitos”, en este caso la Norma ISO/IEC 27001:2013 2ª Edición cancela y reemplaza a su predecesora la ISO/IEC 27001: 2005.

Este estándar internacional ha sido diseñado para sentar las bases y mostrar los requisitos para el establecimiento, la implementación, la administración y la mejora continua enfocado a la seguridad de la información (figura 12), el optar por un sistema de gestión de la seguridad de la información es una decisión estratégica para cualquier organización y deberá estar encaminado a lograr los objetivos y necesidad de la misma (ISO, 2013).

Figura 12. ISO/IEC 27001



Fuente: Elaboración propia

En la implementación de seguridad de la información la confidencialidad, la integridad y la disponibilidad de la información son fundamentales, así como la gestión de riesgos. La seguridad de la información están importante que debe ser integrada como parte de los procesos de las organizaciones. El estándar puede ser un punto de referencia y puede ser utilizado tanto interna como externamente y poder verificar si la organización cumple con los requisitos mínimos de seguridad

de la información, estos requisitos son genéricos y están enfocados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o actividad (Ladino, Villas y López, 2011).

Antes de comenzar la organización debe identificar los problemas externos e internos que sean de relevancia para que el planteamiento de los procedimientos de solución sean los más correctos, también debe determinar los límites y la aplicabilidad de la seguridad de la información para establecer su alcance. Al determinar este último, la organización debe considerar: los problemas externos e internos, los requisitos para su implementación, las dependencias entre las actividades y procesos que se realizan en la organización, de preferencia todo deberá estar debidamente documentado (ISO, 2013).

En el caso de la alta dirección deberá demostrar liderazgo y compromiso con respecto a la implementación de la seguridad de la información mediante la verificación de las medidas aplicables para seguridad de la información, los objetivos y en general la dirección estratégica sean compatibles.

Por otro lado garantizar la integración de la seguridad de la información en los procesos de la organización, asignar y garantizar que los recursos necesarios (humanos y materiales) para el sistema de gestión de la seguridad de la información estén disponibles, concientizar y apoyar a todo el personal sobre la importancia de la aplicación de la seguridad de la información, garantizar el logro de los objetivos propuestos, promover la mejora continua y demostrar su liderazgo haciéndose participes de todo el proceso (Calder, 2008).

La gerencia debe establecer políticas apropiadas y en línea con los objetivos y metas de la organización, las políticas establecidas deberán estar documentadas y transmitidas por diversos canales a toda la organización, la alta dirección con ayuda de especialistas se asegurarán de que las responsabilidades y las autoridades para los roles relevantes para la seguridad de la información

sean debidamente asignadas y comunicadas para garantizar que la implementación se apegue con los requisitos de la Norma Internacional.

Al planificar la implementación de la seguridad de la información, la organización debe considerar los problemas, requisitos, los riesgos y oportunidades a los que se debe hacer frente reduciendo los efectos no deseados y estar evaluando constantemente el desempeño de lo implementado (Ruíz, 2010).

En la Norma ISO (2013) establece que para los riesgos, la organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información mitigándolos mediante controles previamente establecidos e identificando el origen o la fuente del mismo todo plasmado en una bitácora.

La organización debe establecer objetivos de seguridad de la información con las siguientes características:

- Ser coherentes con las políticas de seguridad de la información
- Medibles
- Claros y concretos
- Realistas
- Desafiantes pero alcanzables
- Dinámicos, es decir, actualizarse según corresponda.
- Específicos en tiempo

Al planificar cómo lograr sus objetivos de seguridad de la información, la organización debe determinar:

- ¿Qué se hará?
- ¿Qué recursos serán requeridos?
- ¿Quién será responsable?
- ¿Cuándo se completará?
- ¿Cómo se evaluarán los resultados?

Una vez que la organización determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua de la seguridad de la información, la organización debe:

- Determinar la competencia necesaria de cada persona y de su trabajo, así como el nivel de impacto en la seguridad.
- Asegurarse de que las personas sean competentes estén capacitadas o con la experiencia apropiada.
- Brindar capacitación al personal para tal efecto.

Las personas que trabajen en la organización deben conocer:

- Las políticas de seguridad de la información
- Su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios de un mejor rendimiento de la seguridad de la información
- Las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información.

La organización debe determinar la necesidad de comunicaciones internas y externas relevantes, tomando los siguientes aspectos:

- Sobre qué comunicar
- Cuándo comunicarse
- Con quien comunicarse
- Quién se comunicará
- Los procesos por los cuales se efectuará la comunicación.

La organización debe considerar la posibilidad de documentar de cada uno de los procesos que se realicen, en la documentación registrada sobre la seguridad de la información se debe plasmar:

- El tamaño de la organización y su tipo de actividades, procesos, productos y servicios
- La complejidad de los procesos y cuáles son sus interacciones
- La competencia de las personas.

Al crear y actualizar información documentada, la organización deberá garantizar que sea de manera apropiada, teniendo:

- Identificación y descripción (por ejemplo, un título, fecha, autor o número de actualización)
- Formato (por ejemplo, idioma, versión de software, gráficos) y medios (por ejemplo, papel, electrónico)

En el caso de una institución educativa en su mayoría lo documentación manejada es información en formato físico, para el control de la información documentada, la organización deberá tener en cuenta lo siguiente:

- Distribución, acceso, recuperación y uso
- Almacenamiento y preservación
- Control de cambios (por ejemplo, control de versiones)

La organización debe mantener la información documentada en la medida necesaria para tener la confianza de que los procesos se llevaron a cabo según lo planificado, llevar bitácora que dé certidumbre y tener el control de los cambios planeados y revisar los efectos de los cambios involuntarios, tomando medidas para mitigar los efectos adversos, según sea necesario (ISO, 2013).

La organización deberá realizar evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, también se debe evaluar el rendimiento de la seguridad de la información y la efectividad de todos los controles que fueron establecidos con anterioridad para determinar si es necesario la adecuación a estos (Dister, 2013).

La organización debe establecer:

- Lo que debe ser monitoreado y medido, incluidos los procesos y controles de seguridad de la información
- Los métodos de monitoreo, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos

Por otro lado los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerados válidos, la dirección debe determinar:

- Cuando se realice el monitoreo y la medición
- Quién debe monitorear y medir
- Cuando los resultados del monitoreo y la medición sean analizados y evaluados
- Quién analizará y evaluará estos resultados.

La organización debe llevar a cabo auditorías internas a intervalos previamente programados para la generación de información sobre si la aplicación de la seguridad de la información se ajusta las objetivos y necesidades de la organización, está por demás decir que las auditorias estarán hechas por personas que garanticen la objetividad y la imparcialidad del proceso, el resultado deberá ser informado a todo el personal involucrado (Ladino et al., 2011).

La alta dirección debe revisar todos los mecanismos y controles aplicados para la seguridad de la información de la organización para garantizar su eficacia. La revisión de la gerencia incluye la consideración de:

- El estado de las acciones aplicadas y en proceso
- Registro de problemas ocurridos y su solución
- Retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias en:
    - Acciones preventivas y acciones correctivas

- Resultados de monitoreo y medición
- Resultados de la auditoría
- Cumplimiento de los objetivos de seguridad de la información
- Retroalimentación de las partes interesadas
- Los resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos
- Oportunidades para la mejora continua.

Los resultados de la revisión de la gestión deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier otra necesidad de cambios en la implementación de la seguridad de la información (Disterer, 2013).

A continuación se mencionan algunos objetivos de control para la implementación de la seguridad de la información, para la implementación de la seguridad de la información se necesita, proveer de la dirección en la gestión y el soporte para la seguridad de la información de acuerdo con las necesidades de la organización.

Inicialmente debemos definir un conjunto de políticas para la seguridad de la información, aprobado por la gerencia, publicado y transmitido a todos los colaboradores y en si es el caso a las partes externas relevantes, evidentemente llevar a cabo la revisión las políticas de seguridad de la información en intervalos de tiempo predefinidos o si se producen cambios significativos para suficiencia y eficacia (ISO,2013).

Posteriormente diseñar y establecer un marco de gestión para iniciar y controlar la implementación y el funcionamiento de la seguridad de la información dentro de la organización, por ejemplo:

- Asignar funciones y responsabilidades relacionadas con la seguridad de información a todo el personal involucrado, una vez distribuidos

los deberes se reducen las oportunidades de modificación o uso no autorizado o no intencionado de los activos de la organización.

- Mantenerse informados de los temas relacionados con la seguridad de la información, foros, asesorías con especialistas, mantener relación con medios especializados en la materia.
- La seguridad de la información se tomara en cuenta en la gestión de proyectos en un futuro.

Las recomendaciones de la ISO (2013) argumenta que en caso de existir alguna ventana de teletrabajo, diseñar políticas y medidas de seguridad para gestionar los riesgos introducidos mediante el uso de dispositivos móviles o a distancia, se implementará una política y medidas de seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de teletrabajo.

En el tema de los Recursos Humanos la alta dirección debe garantizar que los empleados y contratistas comprendan sus responsabilidades y que sean adecuados para las funciones para las que se los considera, llevando a cabo una evaluación de antecedentes de todos los candidatos para el empleo se llevarán a cabo de conformidad con las leyes, reglamentos y ética pertinentes y serán proporcionales a los requisitos del negocio, la clasificación de la información a acceder y los riesgos percibidos.

Los acuerdos contractuales con los colaboradores y contratistas deben establecer sus responsabilidades y las de la organización para la seguridad de la información, una vez contratados, asegurarse que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información, por su parte la administración verificará que todos los colaboradores apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización (ISO, 2013).

Todos los empleados de la organización y en su caso los contratistas deberán recibir educación y capacitación apropiadas sobre la concientización y

actualizaciones periódicas en las políticas y procedimientos de la organización, según sea relevante para su función laboral y en caso de fallas o que algún empleado infrinja lo establecido implantar un proceso disciplinario formal y comunicado para tomar medidas en contra los empleados que hayan cometido una violación de las políticas de seguridad, concientizar y responsabilizar a los usuarios por salvaguardar su información de autenticación.

Para la gestión de activos identificar los activos de la organización y definir las responsabilidades de protección apropiadas, procediendo a:

- Identificar los activos asociados con las instalaciones de procesamiento de información y la elaboración del inventario, los activos mantenidos en el inventario serán propiedad de la organización.
- Diseñar las reglas para el uso de la información, así como como de los activos asociados con las instalaciones de procesamiento de información, lo anterior debidamente documentado.
- Todos los colaboradores devolverán todos los activos de la organización en su posesión al finalizar la jornada laboral

Para el tema de la clasificación de la información se debe asegurar que la información se clasifique y reciba un nivel de protección apropiado de acuerdo con su importancia para la organización, la información se clasificará en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada (Ladino et at., 2011).

Se debe desarrollar e implementar un procedimiento para el etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por la organización, así como, desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de antes realizada.

El ISO (2013) asevera que es muy importante evitar la divulgación, modificación, eliminación o destrucción no autorizadas de la información almacenada en los medios, mediante la implementación de procedimientos para la gestión de medios extraíbles, en el caso de la eliminación de medios deben desecharse de forma segura cuando ya no se requiera, utilizando procedimientos formales, los medios que contienen información deben estar protegidos contra accesos no autorizados, mal uso o corrupción durante el transporte.

Para lo asociado al control de acceso diseñar políticas para el control de acceso, basada en los requisitos de seguridad comercial, de información y de perfiles de usuarios, a los usuarios o colaboradores sólo se les proporcionará acceso a los servicios de redes y trabajos en red que han sido específicamente autorizados para usar, sumado a implementar un proceso formal de registro, revocación de los derechos y eliminación de usuarios para permitir la asignación de derechos de acceso a la información, sistemas y servicios.

Dentro la clasificación de la información secreta de autenticación se controlará a través de un proceso de gestión formal llevando una revisión periódica de los derechos de acceso de los usuarios que comúnmente lleven la consulta o manipulación de la misma, por su parte derechos de acceso de todos los colaboradores y usuarios de la parte externa a las instalaciones de procesamiento de información se eliminarán al finalizar su empleo, contrato o acuerdo (ISO, 2013).

Es primordial evitar el acceso no autorizado a sistemas y aplicaciones, el acceso a la información y las funciones del sistema de aplicación se restringirán de acuerdo con la política de control de acceso para ello diseñar e implementar procedimientos de inicio de sesión seguros, ejemplo de ello son los sistemas de gestión de contraseñas que son interactivos y garantizarán las contraseñas de calidad, sin descartar el uso de programas o aplicaciones para tal fin.

En relación a algo más específico la ISO (2013) recomienda que podemos hacer uso de controles criptográficos, son una muy buena opción ya que promueven la protección de la confidencialidad, autenticidad y / o integridad de la información. Para eso se deben desarrollar e implementar políticas sobre el uso de controles criptográficos para la protección de la información, definiendo la duración de las claves criptográficas a lo largo de todo su ciclo de vida.

Y qué decir de la seguridad física, evitar el acceso físico no autorizado, daños e interferencias a las instalaciones de procesamiento de información en la organización mediante la definición de perímetros de seguridad con respecto a las áreas e infraestructura que contienen información sensible o crítica evitan dejar puntos de acceso sin supervisión, las áreas seguras deben estar protegidas por controles de entrada apropiados para garantizar que solo el personal autorizado tenga acceso

Por otro lado debemos tener en cuenta las amenazas externas y ambientales, para ello diseñar e implementar medidas de protección física contra desastres naturales, ataques maliciosos o accidentes, la ubicación en donde se establecerá la infraestructura es fundamentan, el equipo de procesamiento y resguardo de la información debe estar ubicado y protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado (Solarte et al., 2015).

El equipo debe estar protegido contra fallas de energía y otras interrupciones causadas por fallas en los servicios de apoyo, sumado a que tanto la energía y las telecomunicaciones que transportan datos o servicios de información deben estar protegidos contra interferencias o daños.

El equipo, la información o cualquier medio que contenga la información no deben sacarse del sitio sin autorización previa en caso de hacerlo la seguridad se aplicará a los activos fuera del sitio teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. Todos los elementos de los

equipos que contienen medios de almacenamiento deben verificarse para garantizar que cualquier información sensible y software con licencia se haya eliminado o sobrescrito de forma segura antes de su eliminación o reutilización (ISO, 2013).

Con lo que respecta a las operaciones y todos los procedimientos operativos deben documentarse y ponerse a disposición de todos los usuarios que los necesiten se deberán controlar los cambios en la organización, los procesos comerciales, las instalaciones de procesamiento de la información y los sistemas que afectan la seguridad de la información.

Por otra parte de debe monitorear el uso de los recursos y se deben diseñar los futuros proyectos pensando y asignando recursos a la seguridad de la información, eso incluye la redundancia en el resguardo y protección de la información, la redundancia y las copia de seguridad son muy importantes y deben de realizarse y probarse regularmente de acuerdo con una política de respaldo acordada.

Y en general el llevar registro y monitoreo de todos procesos ya que nos dan certidumbre de cómo se realizan, los registros de eventos muestran las actividades del usuario, errores, fallas y eventos de seguridad de la información, dichos registros deben ser producidos, conservados y revisados regularmente y resguardados contra la manipulación y el acceso no autorizado incluyendo las actividades del administrador del sistema, para este tipo de registros la sincronización del reloj es fundamental, se recomienda llevar la sincronización basada en una única fuente de tiempo de referencia (ISO, 2013).

La revisión de nuestra plataforma tecnológica es medular ya que en la actualidad dependemos mucho del almacenamiento de información en servidores y debemos prevenir la explotación de vulnerabilidades técnicas mediante equipo especializado si es necesario, estableciendo e implementando las reglas que rigen la instalación de software por parte de los usuarios (Disterer, 2013).

Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información, los trabajos en red deben ser gestionados y controlados para proteger la información en sistemas y aplicaciones, los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red deben identificarse e incluirse en los acuerdos de servicios de red de trabajo, ya sea que estos servicios se presten internamente o se subcontraten.

Siguiendo con el tema de las comunicaciones y tecnología también se debe hacer la segregación en redes, es decir, crear grupos de trabajo y servicios de información, los usuarios y los sistemas de información se subdividen en la red.

ISO (2013) exhorta que para la transferencia de información se deben implementar políticas, procedimientos y controles formales para proteger la transferencia de información mediante el uso de todo tipo de medios o infraestructura de comunicación, la información involucrada en los mensajes electrónicos debe estar apropiadamente protegida y se identificarán, revisarán y documentarán periódicamente los requisitos para la confidencialidad o los acuerdos de no divulgación que refieran las necesidades de la organización para la protección de la información.

Es necesario garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para los sistemas de información que proporcionan servicios a través de redes públicas. La información involucrada en las transacciones debe estar protegida para evitar transmisiones incompletas, fuga de información, modificación o reproducción no autorizada de mensajes y divulgación no autorizada (Beckers, 2011).

En el campo de la utilización de software especializado la organización debe implementar políticas de utilización de versiones seguras, en el caso que las organizaciones desarrollen sus propios sistemas deben establecer y proteger

adecuadamente los entornos de desarrollo que cubran todo el ciclo de vida de desarrollo del sistema, en caso que la organización encargue a un tercero el diseño y desarrollo de un sistema, la organización debe supervisar y monitorear la actividad del desarrollo del sistema subcontratado y realizar pruebas de la funcionalidad seguridad durante el desarrollo y finalmente se establecerán programas de prueba de aceptación y criterios relacionados para nuevos sistemas de información , actualizaciones y nuevas versiones.

Abordando el tema de la proveeduría todos los requisitos de seguridad de la información relevantes deben establecerse, acordarse y documentarse con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización, los acuerdos con los proveedores incluirán requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y las comunicaciones y el suministro de productos, la organización debe monitorear, revisar y auditar regularmente el servicio del proveedor, los cambios en la prestación de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, se gestionarán teniendo en cuenta la criticidad de la información, los sistemas y procesos involucrados y la reevaluación de los riesgos (ISO, 2013).

Con lo que respecta a la gestión de incidentes de seguridad de la información las responsabilidades y los procedimientos de gestión se establecerán para garantizar una pronta respuesta, eficiente y ordenada a los incidentes de seguridad de la información presentados, los eventos e incidentes de seguridad de la información se informarán a través de los canales de gestión apropiados lo más rápido posible para llevar a cabo las acciones pertinentes.

Al igual que muchos otros procesos los incidentes de seguridad se deben de documentar junto con su acción de mitigación aplicada para que en caso de

que surgiera alguna otra eventualidad del mismo tipo poder actuar con mayor prontitud y eficiencia a la contingencia, una continuidad de operaciones en la organización o como algunos le llaman continuidad del negocio debe ser el principal objetivo de cualquier plan de seguridad de la información, por ello la organización deberá constantemente estar verificando y validando los controles diseñados (Calder, 2008).

Finalmente y no por ser un asunto menos importante, la información siempre tiene un dueño o propietario y debe cumplir con ciertas normas o reglas para su resguardo y protección por lo tanto debemos tener presentes y documentarnos sobre las legislaciónes o leyes aplicables con la naturaleza de la información por ejemplo:

- Derechos de propiedad intelectual. Se deben implementar los procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de activos patentados.
- La privacidad y la protección de la información de identificación personal se garantizarán según lo requerido en la legislación y reglamentación pertinente cuando corresponda y en el lugar determinado.
- Regulación de controles criptográficos. Se deben usar de acuerdo con todos los acuerdos, leyes y reglamentos pertinentes, el tamaño de la llave de cifrado y algunos otros aspectos específicos.

Para aplicar todo lo antes mencionado debemos tener en mente que se trata de todo un proceso de una planeación en la organización, de organizar todos los elementos funcionales y listos para comenzar la aventura, la integración de las herramientas, elementos y mecanismos para trabajar como uno solo, la dirección y liderazgo de quien encabeza las operaciones y las gestione tratan de permear de esa responsabilidad y compromiso a los demás integrantes de la organización y finalmente la acción de estar evaluando y controlando resultados para llevar a

cabo los ajustes en tiempo y forma adecuados preservando la continuidad del negocio y enfocados en una mejora continua (ISO, 2013).

Conclusiones

El conocimiento es el resultado de un proceso no lineal ya que de una simple idea se puede desprender conocimiento de diversa índole y de cada uno se desprenden aún más, también es consecuencia de la investigación al confrontar ideas, lo anterior nos acerca al concepto de ciencia para lo cual deberemos llevar acabo la aplicación sistematizada de procesos y métodos que mediante la observación, el razonamiento, el análisis y la experiencia se le otorga formalidad y fundamentación para aumentar el saber humano.

Con lo que respecta al Método científico resulta ser parte importante que influye en los avances tecnológicos y en la ciencia que con la conjunción de métodos de apoyo y auxiliares nutren aún más el proceso de investigación de hacer ciencia.

Para que cualquier investigación transite por la ruta correcta, incrementando la eficiencia en los resultados se requiere definir una metodología de investigación, para el presente trabajo se determinó un tipo de investigación bibliográfica y de campo, con respecto al alcance y diseño de la investigación resulta ser del tipo no experimental con un enfoque cualitativo y se caracteriza por ser descriptiva al analizar como es y cómo se manifiesta el fenómeno y sus componentes.

El problema planteado es la seguridad de la información en las organizaciones de nuestro país el cual desde hace años ha tomado notoriedad debido a los avances tecnológicos y no propiamente porque sea un asunto tecnológico y sino porque la información en un gran porcentaje la tenemos almacenada en medios digitales en comparación con el resguardo físico.

Los factores preponderantes y que están íntimamente relacionados con este problema son la infraestructura, los procesos de manejo y resguardo y el más importante la concientización del factor humano que va desde los altos directivos hasta los operativos y más abajo en el organigrama.

El análisis de la situación actual que vive la organización es importante para eficientar la aplicación de la seguridad de la información, la infraestructura es uno de los puntos de partida para la implementación, no es necesario tener gran cantidad de recursos invertidos en ella, sin embargo la infraestructura deberá estar asignada y administrada de manera adecuada, en algunos de casos el tener en exceso representa perdida por lo costos de mantenimiento y en caso contrario la falta de ella contribuye a una posible pérdida, por tal motivo la relación infraestura-procesos debe de estar en un balance adecuado y eso se determina con la etapa de toma de decisiones por parte del capital humano de la organización.

Las posibles consecuencias de una nula o deficiente la implementación de seguridad de la información en las organizaciones desemboca en posibles resultados adversos en campo económico, de reputación y continuidad y como contraparte una eficiente aplicación de esta atraerá una mejora en sus procesos, eficiencia en la consulta dotándola de confidencialidad, integridad, disponibilidad y certidumbre que contribuyan al éxito organizacional.

El conocimiento se desprende de la información y ésta a su vez de cualquier conjunto de datos organizados ya sea en formato físico o digital que se posea, la información es el insumo estratégico de las organizaciones que se relaciona con el proceso de toma de decisiones, es el activo que se convierte en el elemento medular del funcionamiento y productividad de las organizaciones.

En las décadas de los 70’s y 90’s, primero con la sociedad de la información y posteriormente con la sociedad del conocimiento se le dio forma a lo que actualmente tenemos en el área del saber humano y que sumado a los avances de las distintas ciencias que intervienen potencializan los alcances para cualquier organización.

La información al ser un elemento importante tiene intrínsecamente asociado un valor, caducidad, amenazas y vulnerabilidades, entre los que se encuentran el factor humano y la infraestructura propias de cada organización.

Con lo que respecta a su valor, este es asignado por el dueño de la misma, solo él sabe cuánto le costaría si su secreto industrial o sus estrategias de crecimiento le significarían a su organización en caso de ser reveladas, su caducidad está asociada con los factores valor-tiempo, es decir, que tanto vale cierta información en un momento determinado. Las vulnerabilidades y amenazas son inherentes a las cosas con valor ya que factores malintencionados del entorno se centran en encontrarlas o bien en crearlas por lo que es imperativo abordar el tema de la seguridad de la información de la mejor manera posible.

La seguridad de la información es la disciplina que mediante herramientas y mecanismos brindan certidumbre en sus procesos de resguardo, manipulación y almacenamiento de la información, la seguridad de la información no se trata de un asunto puramente tecnológico o que tenga que ver con sistemas informáticos, de hecho su campo de acción va más allá, ya que trata a la información en cualquiera de sus formas, los pilares de la seguridad de la información son la confidencialidad, integridad y disponibilidad.

La creación de políticas, procesos y procedimientos enfocados a la seguridad de la información y que contribuyan al cumplimiento de los objetivos organizacionales son actividades primordiales que deben estar plasmadas en la agenda de la organización.

Entre los riesgos por una mala gestión de los procesos relacionados con la información y su seguridad están los fraudes, la fuga de información, generar un desprestigio, interrumpir las operaciones (continuidad) del negocio, lo anterior se puede solventar realizando un análisis de riesgos de manera sistemática para llevar a cabo una adecuada mitigación y corrección según sea el caso.

En la actualidad se cuenta con Organizaciones y Marcos de Referencia enfocados en brindar alternativas para el análisis, la implementación y gestión de la seguridad de la información y que se encuentran alcance de todas las organizaciones para darle mayor solidez y formalidad.

Al igual que en muchas otras disciplinas el proceso de la implementación de la seguridad de la información pueden ser extrapoladas al proceso administrativo al contar con mecanismos y herramientas enfocadas en la planeación, organización, integración, dirección y control, debemos estar atentos a las nuevas tecnologías y avances que surjan en los diferentes campos en donde se desenvuelva nuestra organización con el objetivo de seguir vigentes y con la proyección de un futuro mejor.

Una mala implementación o la falta de presencia de la seguridad de la información en los procesos es una constante en el ámbito organizacional de nuestro país un ejemplo de ello es el sistema Bancario Mexicano en donde Banco Central junto con otras instituciones bancarias desafortunadamente se vieron involucradas en la perdida de cientos de millones de pesos dejando en un hilo la confianza y la credibilidad de que el dinero está seguro, es un hecho que la seguridad fallo en algún punto ya sea en la capacitación, supervisión o sensibilización del capital humano con respecto a la seguridad de la información porque al final de cuentas quien maneja los sistemas de resguardo y consulta sin importar si es físico o digital son manos humanas, por lo cual debemos marcar protocolos y mecanismos de prevención para evitar incidentes intencionales y no intencionales.

En el contexto como nación vamos por buen camino con el compromiso de ponerse a la vanguardia en tecnología, sin embargo debemos redoblar esfuerzos inyectando mayores recursos en ciencia y tecnología ya que son los pilares del desarrollo para cualquier país, por otro lado la seguridad de la información desde hace algunos años se encuentra en el proceso de maduración por lo que es un área de oportunidad para muchas organizaciones ya que desde su punto de vista no la ven necesaria del todo, esto debido a que por fortuna no se han visto afectados, no obstante es un tema que tarde o temprano deberán implementar debido al mundo tan globalizado y conectado en el que vivimos.

Por otro lado en el contexto mundial al ser un espacio aún más amplio podemos contar variados ejemplos relacionados con tropiezos en la implementación de la seguridad de la información, empresas gigantescas como: Facebook, Cambridge Analytica y Wikileaks son claros ejemplos de cómo no se deben implementar la seguridad de la información, las consecuencias como siempre recaen en el aspecto económico y es justo ahí en donde algunos sectores comunidad internacional dan origen a organizaciones encaminados al fortalecimiento de la seguridad de la información, proponiendo reformas a leyes o bien planteando nuevas enfocándose en la regulación de la información que es transmitida y utilizada por diversos medios.

La evolución de estándares y marcos de referencia están en pleno crecimiento y se encuentran disponible para el beneficio de las organizaciones de todo el mundo, entre algunos de los antes mencionados tenemos a COSO:2013, COSO:2017 y la familia ISO 27000 principalmente la ISO/IEC 27001 sobre Sistemas de Gestión la Seguridad de la Información. Ninguna organización puede montarse a la ola de la vanguardia y del éxito sin la implementación de un verdadero control interno, para tal fin existen marcos de referencia que nos aportan la información, herramientas y mecanismos necesarios para una mejor implementación,

Es por ello que finalmente y como pudimos observar a través del trabajo, se enuncian y se proponen marcos y normas de referencia tanto de control, análisis de riesgos y de seguridad de la información y que en su conjunto conformen la estrategia para la implementación de la seguridad de la información, teniendo como punto de partida a COSO:2013 que mediante la ejecución y atención a sus cinco componentes de control: ambiente de control, evaluación de riesgos, actividades de control, información y comunicación y como último componente la actividad de monitoreo pretenden hacer una sinergia para que la organización alcance sus objetivos fortaleciendo la cultura organizacional, la forma de gestionar

los riesgos y la manera en que los afronta, por supuesto que entre dichos objetivos se deberá encontrar la implementación de la seguridad de la información.

Relacionado con el control interno y con igual importancia se sugiere el marco de referencia COSO:2017 especializado en la Gestión de Riesgos empresariales que nos orienta de como la organización puede gestionar los inevitables inconvenientes que puedan surgir con respecto al funcionamiento de nuestra organización, esta herramienta posee cinco componentes: gobierno y cultura, estrategia y establecimiento de objetivos, desempeño, revisión e información y finalmente comunicación y reportes, lo que dará como resultado una mayor visión de los riesgos que se encuentran asociados a los objetivos organizacionales que se quieren alcanzar.

Toda vez que tenemos un control interno adecuado en nuestra organización y la implementación de una gestión de riesgos que nos muestre las áreas de oportunidad, el siguiente paso es acercarnos a la utilización de un marco de referencia como lo es el ISO/IEC 27001 que nos ayuda a sentar las bases para la implementación, administración y la mejora continua entorno a la seguridad de la información, se propone la utilización de controles enfocados a los procesos en donde se ve involucrada la información como un elemento clave que van desde el factor humano hasta lo tecnológico pasando por lo administrativo.

Lo anterior y todo en su conjunto no se trata de una receta que se deba seguir o bien que tenga que ser un proceso secuencial, como es natural, muchas organizaciones están acostumbradas a funcionar de diversas maneras por lo que se recomienda que de forma paralela se realicen las acciones que proponen estos marcos de referencia, el trabajo es arduo pero el resultado será favorable en muchos aspectos que permearan tanto al interior como fuera de la organización.

Referencias

Adell, J. (2017, Noviembre). *Tendencias en educación en la sociedad de las tecnologías de la información*. Edutec-e. Recuperado de http://www.edutec.es/revista/index.php/edutec-e/article/view/570

Afzal, W. (2012). *Management of Information Organizations*. Cambridge, Reino Unido: Chandos Publishing.

Baena, G. (2014). *Metodología de la investigación.* Distrito Federal, México: Patria.

BANXICO (29 de agosto de 2018). *Reporte de análisis forenses*. BANXICO. Recuperado de http://www.banxico.org.mx/spei/d/%7B4A977A24-0889-3F24-A717-DF9DBBA118C1%7D.pdf

BBC (21 de marzo de 2018*). 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día*. BBC. Recuperado de https://www.bbc.com/mundo/noticias-43472797

Beckers, K. (2011). *Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing*. IEEE Explore. Recuperado de https://ieeexplore.ieee.org/abstract/document/6045958

Bunge, M.(1979). *La ciencia. Su método y su filosofía*. Recuperado de https://drive.google.com/file/d/0B5tVYXnH1yduNGVjMTVmZjMtMWE5ZC00MDk3LWE4MWUtNDc3YTI1MmM1OWEw/view?hl=es

Bytheway, A. (2014). *Investing in Information:The information management body of knowledge*. Suiza: SPRINGER.

Calder, A. (2008). *IS027001/ ISO27002 a pocket Guide. Reino Unido: IT* Governance Publishing.

Cherdantseva Y., Hilton, J., Rana, O. & Ivins, W. (septiembre 2016). *A multifaceted evaluation of the reference model of information assurance & security*. ELSEVIER. Recuperado de http://www.sciencedirect.com

Commitee of Sponsoring Organizations of the Treasway Commisision. (mayo 2013). *Internal Control-Integrated Framework*. Durham, Estados Unidos. Recuperado de https://www.coso.org/Pages/ic.aspx

Commitee of Sponsoring Organizations of the Treasway Commisision. (junio 2017). *Enterprise Risk Management.* Recuperado de https://www.coso.org/Pages/guidance.aspx

Daltabuit, E. & Hernández , L. (2007). *La seguridad de la información*. , Distrito Federal, México: Limusa.

Davenport, T. & Prusak, L. (1998). *Working Knowledge: How organisations manage what they know*. USA: Harvard Business School Press.

Departamento Administrativo Nacional de Estadísticas. (2017). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2017*. INEGI. Recuperado de: http://www.beta.inegi.org.mx/proyectos/enchogares/regulares/dutih/2017

Disterer, G. (abril de 2013). *ISO/IEC 27000, 27001 and 27002 for Information Security Management*. Scientific Research. Recuperado de https://serwiss.bib.hs-hannover.de

Dhillon,G., Syed, R. & Pedron, C., (octubre 2015) *) Interpreting information security culture: An organizational transformation case study*. ELSEVIER. Recuperado de http://www.sciencedirect.com

Díaz, V. (2009). *Metodología de la investigación científica y bioestadística*. Santiago, Chile: RIL editores.

Dor ,D. & Elovici, Y. (septiembre 2016). *A model of the information security investment decision-making process*. ELSEVIER. Recuperado de http:// www.sciencedirect.com

Flowerday, S. & Tuyikeze, T., (junio 2016*) Information security policy development and implementation: The what, how and who*. ELSEVIER. Recuperado de http://www.sciencedirect.com

Frick, G. (2016). *Administración de la seguridad de la información basada en la gestión de riesgos en Latinoamérica*. Universidad de Palermo, Buenos Aires, Argentina.

González, Y. A. & Martínez, C. A. (2008). *Metodología para establecer un plan de seguridad de la información*. Universidad Nacional Autónoma de México, Distrito Federal, México.

Guerrero, G. (2014). *Metodología de la investigación*. , Distrito Federal, México: Patria.

Hernández, S. (4a Ed.). (2006*). Introducción a la Administración, teoría general administrativa, origen, evolución y vanguardia*. México, D.F., México: McGraw-Hill

ISO 27001 (2013*). ISO/IEC 27001: Information security management*. Recuperado de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Itradat, A., Sultan,S., Al-Junaidi, M., Rawa'a,Q., Feda'a,M. & Daas, F., (abril 2014) *Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study*. JJMIE. Recuperado de http://www.jjmie.hu.edu.jo

Kearney, W & Kruger, H. (mayo 2016). *Can perceptual differences account for enigmatic information security behaviour in an organisation?*. ELSEVIER. Recuperado de http://www.sciencedirect.com

Kerlinger, F. & Lee, H. (2002). *Investigación del comportamiento. Métodos de investigación en ciencias sociales*. , Distrito Federal, México: McGraw-Hill.

Ladino, A., Villas, M., Lopez, P. (abril de 2011*). Fundamentos de ISO 27001 y su Aplicación en las empresas. Scientia Et Technica*. Recuperado de http://www.redalyc.org/articulo.oa?id=84921327061

López, I. (15 de mayo de 2015*).Esto es lo que se sabe del robo millonario tras el hackeo a los bancos*. Forbes. Recuperado de

https://www.forbes.com.mx/esto-es-lo-que-se-sabe-del-robo-con-el-ciberataque-a-los-bancos/

Lukasiewics, J. (1970). *Estudios de lógica y filosofía*. Madrid, España: Occidente.

Luna, I., Bojórquez, J. & Hofmann, A. (2015). *Gobierno Abierto, el valor social de la información pública*. Ciudad de México, México: Instituto de Investigaciones Jurídicas, UNAM

Pacheco, F. (19 de enero de 2011). *Fuga de información: ¿una amenaza pasajera?. ESET Latinoamérica*. Buenos Aires, Argentina. Recuperado de http://www.eset-la.com/pdf/prensa/informe/fuga_de_informacion.pdf

Pérez, G.(2014). *La cooperación judicial en la unión europea: eurojust y sus principales desafíos frente a la delincuencia transnacional grave*. Universidad Nacional de Educación a Distancia, España

Pisani, F. (29 de mayo de 2003). *El futuro de las tecnologías de la información*. El País. Recuperado de https://elpais.com/diario/2003/05/29/ciberpais/1054173082_850215.html

Madrigal, B. (2a Edición).(2009). *Habilidades Directivas*. México, D.F., México: McGraw-Hill

Márquez, D. (2015). *Datos personales y seguridad de la información del sector empresarial en México*. Universidad Nacional Autónoma de México, Distrito Federal, México.

Maza, A. & Cabrera, C. (2013). *Diagnóstico del plan de seguridad de las tecnologías de la información y comunicación en una organización*. Universidad Nacional Autónoma de México, Distrito Federal, México.

Münch, L. & Ángeles, E. (2007). *Métodos y técnicas de investigación*. , Distrito Federal, México: Trillas.

Münch, L. (2a Ed.). (2014). *Administración. Gestión organizacional enfoques y proceso administrativo*. Naucalpan, Estado de México: Pearson Education

Navarro, J. (2014). *Epistemología y metodología*. , Distrito Federal, México: Patria.

Nazareth, D. & Choi,J., (noviembre 2014). *A system dynamics model for information security management*. ELSEVIER. Recuperado de http://www.sciencedirect.com

Nicasio, O. (2015). *Diseño e implementación de un sistema de gestión de calidad en seguridad de la información SGSI*. Universidad Nacional Autónoma de México, San Juan de Aragón, Edo. de México.

Ögütçü, G., Müge, O. & Chouseinoglou, O. (noviembre 2015). *Analysis of personal information security behavior and awareness*. ELSEVIER. Recuperado de http://www.sciencedirect.com

Ramos, J. D. (2013). *Administración de la seguridad de la Información*. Universidad Nacional Autónoma de México, San Juan de Aragón, Edo. de México.

Real Academia Española. (2017). *Diccionario de la lengua española*. Recuperado de http://dle.rae.es/?id=9AwuYaT.

Ríos, J. & Ramírez, C. (2016). *El valor social de las bibliotecas y de la información*. Ciudad de México, México: UNAM

Riley, C. (9 de marzo de 2018). *Lo que necesitas saber sobre el escándalo de Facebook por la filtración de información. CNN*. Recuperado de https://cnnespanol.cnn.com/2018/03/19/facebook-trump-filtracion-datos-cambridge-analytica-usuarios/

Ruiz, R.M. (2010). *Guía de implementación de un sistema de gestión de seguridad de la información alineado a la norma ISO 27001*. Universidad Nacional Autónoma de México, San Juan de Aragón, Edo. de México.

Sánchez, G. & Ángeles M. (2002). *Tesis profesional: ¡Un problema! ¡una hipótesis!¡una solución!.* Distrito Federal, México: UNAM Fes Cuautitlán.

Sánchez, G. & Angeles, M. (2017). *Tesis y otras modalidades de titulación: Estrategias metodológicas*. Cuautitlán, México: FESC-UNAM.

Sánchez, G., Ángeles, M., Valdés, L., Flores, J., Muñoz, M. & Aguirre, J. (2010). *La economía del conocimiento: reto para las organizaciones*. Cuautitlán, México: FESC-UNAM.

Sánchez, G., Ángeles, M., Valdés, L., J., Muñoz, Olvera, E. & Galicia, D. (2010). *La administración en México: tendencias en la sociedad del conocimiento*. Cuautitlán, México: FESC-UNAM.

Solarte, F., Enríquez, E. y Benavides, M. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*. Revista Tecnológica ESPOL. Recuperado de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Tamayo, M. (2004). *El proceso de la investigación científica: Incluye evaluación y administración de proyectos de investigación*. , Distrito Federal, México: Limusa.

Tsohou, A., Karyda, M. & Kokolakis, S. (abril 2015). *Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs*. ELSEVIER. Recuperado de http:// www.sciencedirect.com

UNAM (2019). *La UNAM en números. Dirección General de Planeación*. Ciudad de México, México. Recuperado de http://www.estadistica.unam.mx/numeralia/

Villegas, E. (2008). *Seguridad de la información en medios de almacenamiento masivo*. Universidad Nacional Autónoma de México, San Juan de Aragón, Edo. de México. UNAM

Zapien, L. (1 de febrero de 2013). *Tecnologías de Información y competitividad: Presente y futuro*. UNAM. Recuperado de http://www.revista.unam.mx/vol.14/num2/art10/#up