UNIVERSIDAD JOSE ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN GERENCIA Y TECNOLOGIA DE LA INFORMACIÓN

LA GERENCIA Y EL PROBLEMA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES MODERNAS (CASO GANDALF COMUNICACIONES, C.A)

Trabajo de Grado para optar al

Grado de Magister en Gerencia y Tecnología de la Información

Autor: Ing. César M. Álvarez C.

Tutor: MSc. Ing. Esteban De Freitas

San Diego, Febrero del 2018

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRIA EN GERENCIA Y TECNOLOGÌA DE LA INFORMACIÓN

CONSTANCIA DE ACEPTACIÓN DEL TUTOR

Mediante la presente hago constar que he leído el Trabajo de Grado elaborado por el ciudadano **Ing. César Miguel Álvarez Carrero** titular de la cédula de identidad **N° 18.167.045**, para optar al grado académico de **Magíster en Gerencia y Tecnología de la Información**, cuyo título es "**LA GERENCIA Y EL PROBLEMA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES MODERNAS (CASO DE GANDALF COMUNICACIONES, C.A)**" adscrito a la línea de investigación: **La Información como Valor Agregado en el Seno de las Organizaciones Públicas y Privadas.**

Y declaro que acepto la tutoría del mencionado proyecto durante su etapa de desarrollo hasta su presentación y evaluación por el jurado evaluador que se designe; según las condiciones del Reglamento de Estudios de Postgrado de la Universidad José Antonio Páez.

MSc. Ing. Esteban De Freitas

_____

Firma
C.I. V- 9.891.892

San Diego, Febrero del 2018

DEDICATORIA

A Dios y la Virgen por haberme permitido llegar hasta este punto y darme salud para lograr todos y cada uno de mis objetivos, a mi padre, madre, hermana y hermanos por apoyarme en todo momento, consejos, valores, motivación, ejemplos de perseverancia y constancia; y a todos aquellos que participaron de forma directa o indirecta en la elaboración de esta tesis de investigación.

¡Gracias a ustedes!

AGRADECIMIENTOS

A la Universidad José Antonio Páez, específicamente a la Dirección General de Postgrado por brindarme la oportunidad de realizar estos estudios de maestría y poder cumplir con el objetivo alcanzado.

A mi tutor y amigo el Profesor y Msc. Ing. Esteban De Freitas, por su asesoría y orientaciones durante el proyecto de investigación y luego durante la tesis, las cuales fueron muy útiles y acertadas para la realización de ésta investigación, pero sobre todo por paciencia y dedicación en todo momento.

A la Profesora Msc. Marisela Useche, Coordinadora de la Maestría en Gerencia y Tecnología de la Información, por brindarme toda su colaboración, consejos y su amistad; así como también a todos y cada uno de los profesores de de la Maestría por compartir sus conocimientos y asesorarme en la preparación de los trabajos de investigación.

A mis compañeros y compañeras de estudios por su constancia, colaboración y amistad.

A mi papá, mamá, hermana y hermanos por todo su apoyo y colaboración en la realización de ésta investigación, por acompañarme durante todo este camino y compartir conmigo alegrías y consejos sabios.

ÍNDICE

Pág.

CAPITULO III

MARCO METODOLÓGICO

CAPÍTULO IV

LAS TICS Y COMO ABORDAR LAS POTENCIALES AMENAZAS QUE PODRÍAN AFECTAR LA SEGURIDAD DE LA INFORMACIÓN EN EL SENO DE UNA EMPRESA

CAPÍTULO V

LA GERENCIA Y LAS HERRAMIENTAS TECNOLÓGICAS PARA EL CONTROL Y PREVENCIÓN DE LOS RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO VI

LA GERENCIA Y EL PROBLEMA DE LA SEGURIDAD DE LA INFORMACION EN LAS ORGANIZACIONES MODERNAS

Índice de Figuras

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRIA EN GERENCIA Y TECNOLOGIA DE LA INFORMACIÓN

"LA GERENCIA Y EL PROBLEMA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES MODERNAS (CASO DE GANDALF COMUNICACIONES, C.A)"

Línea de Investigación: La Información como Valor Agregado en el Seno de las Organizaciones Públicas y Privadas.

AUTOR: Ing. César M. Álvarez C.
TUTOR: MSc. Ing. Esteban De Freitas
Febrero, 2018

RESUMEN:

La gestión de la seguridad de la información para una organización moderna es un conjunto de lineamientos, principios y políticas preventivas que permiten gestionar de forma efectiva y eficiente el acceso y protección de la información, así como también permite asegurar la confidencialidad, disponibilidad, e integridad a esta misma, a la vez mitigando o minimizando las amenazas tanto externas como internas, que podrían dañar, perder o robar la información en las empresas modernas. En lo relacionado a la seguridad de la información, es relevante destacar que la información en las empresas tiene un valor al igual que cualquier otro recurso, de modo que debe ser protegida. Este estudio abarca el periodo de tiempo desde el 2011 hasta el 2016, y es de tipo histórico documental, con enfoques tecnológicos, operativos y gerenciales, se van a usar obras de reconocidos teóricos como Peter Drucker, Manuel Castells y los Laudon. El objetivo es investigar la gerencia y el problema de la seguridad de la información en las organizaciones modernas (Caso de Gandalf Comunicaciones, C.A.), se trata de que la empresa tenga herramientas que podrían solucionar la problemática relacionada con la gestión de la seguridad de la información, y de esta manera, ser competitivos tanto en el mercado nacional como internacional. Termina la investigación demostrando teóricamente la importancia de la gestión de la seguridad de la información y la gerencia para las organizaciones modernas.

Palabras Clave: Seguridad de la Información, Tecnologías de la Información y la Comunicación, Gerencia.

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
MAESTRIA EN GERENCIA Y TECNOLOGIA DE LA INFORMACIÓN

"MANAGEMENT AND THE PROBLEM OF INFORMATION SECURITY IN MODERN ORGANIZATIONS (CASE OF GANDALF COMUNICACIONES, C.A)"

Research Line: Information as Value Added in the Public and Private Organizations.

AUTOR: Ing. César M. Álvarez C.
TUTOR: MSc. Ing. Esteban De Freitas
Febrero, 2018

ABSTRACT:

The management of information security for a modern organization is a set of guidelines, principles and preventive policies that allow effective and efficient management of access and protection of information, as well as ensure confidentiality, availability, and integrity At the same time, mitigating or minimizing both external and internal threats, which could damage, lose or steal information in modern companies. In terms of information security, it is important to note that information in companies has a value just like any other resource, so it must be protected. This study covers the period of time from 2011 to 2016, and is historical documentary, with technological, operational and managerial approaches, will use works by renowned theorists such as Peter Drucker, Manuel Castells and Laudon. The objective is to investigate the management and the problem of information security in modern organizations (Case of Gandalf Communications, CA), is that the company has tools that could solve the problems related to the management of security of information, and in this way, be competitive in both the national and international markets. It ends the research theoretically demonstrating the importance of information security management and management for modern organizations.

Key Words: Information Security, Information Technology and Communications, Management.

INTRODUCCIÓN

En el mundo actual, con una sociedad cada día más globalizada, la información se ha convertido en uno de los activos más importantes para las organizaciones modernas, por lo que cuando la información se encuentra disponible y se utiliza de una forma responsable y segura, las organizaciones deben tener una adecuada gestión de los activos de información con el propósito de salvaguardar y controlar el acceso, almacenamiento y uso de la información. El aseguramiento y la protección de la seguridad de la información en las organizaciones modernas, representa un reto al momento de garantizar su confidencialidad, integridad y disponibilidad, en tal sentido, la seguridad de la información se ha transformado en uno de los aspectos de mayor preocupación a nivel mundial.

Las organizaciones modernas, deben ser conscientes de la variedad de amenazas existentes que hoy por hoy atentan contra la seguridad de la información, representan una vulnerabilidad y riesgo que al materializarse les puede ocasionar grades costos económicos, sanciones legales, su imagen y reputación se pueden ver comprometidas y pueden afectar la continuidad de las operaciones comerciales. También hay que considerar el ambiente tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y procedimientos estratégicos de las organizaciones. En este sentido, es preciso que los gerentes de TIC dentro de las organizaciones, velen por la seguridad de sus recursos, infraestructura e información, contantemente estén adoptando, implementando y mejorando las políticas o normas de seguridad orientadas a prevenir y/o detectar los riesgos, vulnerabilidades y amenazas que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de la información a través de los cuales se gestiona la información del negocio, ya sea de tipo pública o privada. En la disposición que las organizaciones modernas obtengan una visión general de los riesgos y amenazas que pueden afectar la seguridad su información, podrán establecer políticas de seguridad, con la ayuda de estándares internacionales, con el propósito de salvaguardar la integridad, disponibilidad y confidencialidad de la información, de la organización, empleados, clientes y proveedores.

CAPITULO I

EL PROBLEMA

1.1. Planteamiento del Problema

Actualmente en éste mundo, que cada vez se vuelve más competitivo y exigente, con respecto a la creciente evolución de las tecnologías de la información y la comunicación, y motivado al incremento de la globalización, las organizaciones modernas se han visto en la necesidad de planificar y gestionar de forma adecuada y oportuna la información que producen, a través de las TICs, lo cual es un trabajo complejo que demanda una base sólida de aplicación de conceptos fundamentales en áreas como las ciencias de la computación y sistemas de información, así como también gestiones gerenciales y habilidades del personal, por ejemplo, un sistema de información es un grupo de componentes interrelacionados, una combinación organizada de personas, hardware, software, redes de comunicaciones y recursos de datos que trabajan en conjunto, para procesar, auditar, almacenar, transformar y distribuir la información, de modo que funcione como una herramienta en la toma de decisiones y control dentro de una organización; en las tecnologías de la información existen aspectos importantes de software a considerar como la fiabilidad, seguridad, facilidad de uso, disponibilidad, eficacia y eficiencia para los fines pronosticados, todos estos aspectos son vitales para cualquier tipo de organización o empresa.

Para la gerencia moderna, la gestión de la seguridad de la información debe ser un factor de aplicación de suma importancia, y de prioridad, en tanto que se entiende que la información es un recurso de valor agregado, y debe ser salvaguardado como cualquier otro bien o recurso propiedad de la empresa, las organizaciones modernas deben estar al tanto de la importancia de este recurso y como protegerlo, para las organizaciones, se hace énfasis de que esto debe ser una prioridad en tanto que el escenario en la actualidad es un reto, debido a que las empresas por lo general, no solo cuentan con altos niveles de información por proteger, si no que presentan vulnerabilidad debido a que sus operaciones y las maneras en la cual trabajan, en tanto que en la actualidad, la gestión de la seguridad de la información como valor agregado prioritario para la gerencia de las organizaciones modernas se considera que es una necesidad imperiosa para este tipo de empresas.

En tanto que se habla de valor agregado, debido a que la información es dinero, cuando se pierde, se roban o se daña la información, la empresa puede perder mucha cantidad de dinero que podría poner en desbalance sus finanzas, por lo tanto para la gerencia, la gestión de la información debe ser una prioridad en las organizaciones modernas, esto va a reducir posibles amenazas a la información en el futuro, la protección de los bienes y recursos, e incluso garantizar la continuidad de las operaciones de la empresa, de modo que se eviten re trabajos, perdidas de información, o cualquier actividad que no agregue valor desde la perspectiva del cliente, que comprometa las ganancias y la reputación de la organización moderna, y que afecten las operaciones y producciones de bienes y servicios. El objetivo de la gestión de la seguridad de la información es establecer una serie de medidas de prevención, que permitan la protección de la información, confidencialidad de los datos de la empresa, y garantizar la disponibilidad y el resguardo de la información.

Manuel Castells, en su libro "*La Ciudad Informacional: Tecnologías de la Información"* Edición (2014), explica que las telecomunicaciones se han venido convirtiendo en la clave para la expansión y máxima explotación de las nuevas tecnologías, las cuales han permitido el perfeccionamiento de los diferentes enlaces entre diferentes dispositivos, es decir, aplicaciones basadas en la microelectrónica a los procesos de trabajo en fábricas y oficinas en las organizaciones modernas, para así facilitar la formación de las tecnologías de la información (p. 09). En consecuencia, se infiere que las tecnologías de la información y comunicaciones para las organizaciones modernas son importantes porque ayudan a la buena gestión gerencial de otras áreas, como lo son la contabilidad, las finanzas, la administración de las operaciones, la mercadotecnia, la administración de recursos humanos y cualquier otra función principal de negocios. Es de vital importancia tener un conocimiento de las tecnologías de la información y las comunicaciones para entender cualquier área operacional en la organización, por eso es de igual importancia, tener un conocimiento sobre todo lo referente a los sistemas de información en nuestras organizaciones modernas para que nos permitan y nos otorguen las condiciones necesarias para que las TICs logren todos y cada uno de los objetivos planteados de ventajas competitivas para las empresas, y en derivación, contar con una buena gestión en la seguridad de la información, que en el futuro inmediato es importante para las organizaciones modernas.

Para las empresas modernas en Venezuela, es relevante la gerencia y solucionar los problemas de la seguridad de la información, específicamente para la empresa Gandalf Comunicaciones, C.A, ya que estas soluciones teóricas relacionadas a la protección y salvaguarda de la información genera ventajas competitivas tanto en los mercados nacionales como internacionales.

Jeimy Cano, investigador de Estudios de Comercio Electrónico, Telecomunicaciones e Informática y profesor en la Universidad de los Andes en Colombia, en su artículo *"La Función de Seguridad de la Información"*, publicado en el 2014, se refiere a varios aspectos importantes como lo son las condiciones que debe tomar en cuenta un gerente para ser exitoso en condiciones actuales, así como también menciona que para el año 2020 se presentaran múltiples escenarios que las organizaciones deberán afrontar y advierte la transformación en la gestión y seguridad de la información, a través de dos modelos: el Modelo Actual de la Seguridad de la Información y el Modelo Evolutivo de la Seguridad de la Información (p. 03). Todo indica que la información se ha colocado en un lugar protegido como uno de los principales recursos que poseen las organizaciones modernas de hoy día, los gerentes o directivos que se encargan de las tomas de decisiones en las organizaciones han comenzado a entender que la información no es sólo un producto de la dirección empresarial en sus distintos departamentos, sino que a la vez sostiene a los servicios y puede ser uno de los tantos factores críticos para la determinación del éxito o fracaso de los mismos. En este mismo orden de ideas, si deseamos maximizar la utilidad que posee la información, las organizaciones modernas la deben manejar de forma correcta y eficiente, tal y cómo se manejan los demás recursos existentes, y esto deber ser prioritario. Los gerentes de la organización en los departamentos de tecnología de la información y comunicaciones, deben comprender a nivel general que existen costos asociados con la fabricación, comercialización, seguridad, acopio y recuperación de toda la información que es manejada dentro de la organización. El uso de las TICs como una herramienta para la gerencia moderna, es indispensable para posicionar de forma ventajosa a la organización Gandalf Comunicaciones, C.A dentro de un negocio especifico.

Peter Drucker en su libro *"Su visión sobre: la administración, la organización, la economía, la sociedad"* (1996), sostiene que la información es la herramienta que hace ver los negocios de una manera diferente, por lo tanto la alta gerencia debe requerir la información en el momento adecuado, y en consecuencia, protegerla de amenazas internas y externas.

La información necesaria básicamente para la gerencia, según el teórico Drucker (1996), es:

> Información básica, información de productividad, información de competencia e información de asignación de recursos, con la finalidad de generar riquezas, y que la empresa continúe en marcha; ésta información permite dirigir la táctica. Para la estrategia la alta gerencia requiere información organizada del entorno (p. 56).

Así mismo, Peter Drucker sostiene, que la estrategia debe basarse en información relacionada con los mercados, clientes y no clientes; la tecnología propia de la empresa y de la competencia, finanzas en el ámbito mundial y el ambiente económico mundial. Por lo que, el gerente tiene que estar informado, tanto de sus subordinados como de la red de su entorno, lo cual le permite reunir información de suma importancia, para dirigir la táctica y la estrategia de la organización, no obstante que sin una adecuada gestión de la seguridad de información, como un valor agregado prioritario, estos planes de competitividad podrían fracasar o verse afectados, en especial en las organizaciones modernas. Sin embargo, lo amplio que puede ser el horizonte de oportunidades de la información y de su gestión de seguridad, para mantener y aumentar la competitividad de las empresas, debe tenerse presente el adecuado manejo de la información, como cualquier otro recurso financiero, humano, entre otros. Por lo tanto, la gestión tecnológica en seguridad de la información es fundamental como herramienta para planificar el uso de la información en las empresas y definir su relación con las áreas funcionales como la mercadotécnica, operaciones, producción, finanzas y el talento humano.

Se considera necesario para la empresa Gandalf Comunicaciones, C.A de Venezuela, contar con herramientas teóricas basadas en las TICs, que permitan a la empresa adaptarse a los cambios tecnológicos y su relación con las oportunidades del mercado y las amenazas presentes en él, así como la capacidad de diseñar las estrategias para el acceso y utilizar

adecuadamente la tecnología para aprovechar las oportunidades o enfrentar las amenazas del ambiente donde compite, protegiendo en todo momento la información. Por lo expuesto, la gestión de la seguridad de la información es una actividad esencial en cualquier tipo de organización en Venezuela, ya sea pública o privada, esta misma logra manejar más eficientemente la información, fortalecer los recursos existentes e incrementar las habilidades y destrezas del personal y de la organización de rápido aprendizaje, por esa razón se considera un valor agregado de prioridad.

En contraparte, la gestión tecnológica de la información, y su seguridad, hace de la innovación el elemento o factor disparador más importante, desarrollando una cultura organizacional totalmente identificada con esta forma de conducir cualquier tipo de actividad, con lo cual se facilita la entrada de nuevos bienes y servicios, o de cambios en los procesos de producción o de entrega de los mismos, sin desatender el recurso de la información, fundamental en la sociedad del conocimiento, y fomentando la competitividad de la organización en pro de los clientes finales.

Por todo lo anteriormente señalado, las TICs y la gerencia se han convertido en parte fundamental en las actividades empresariales, gubernamentales, académicas y de la vida diaria, donde la información adquiere mayor importancia y requiere del tratamiento adecuado para su aprovechamiento, de allí surge la necesidad de proteger la información y asegurarse que sea precisa, disponible y confiable, por la razón que dicha información es un bien intangible, y se almacena dentro de los sistemas de información, puede ser salvaguardada dentro de archivos de computadoras y se envía a través de redes de comunicaciones de forma digital, por otro lado, los datos digitales son más propensos a destrucción, fraude, usurpación, o ingreso a la información de dichos datos por parte de personas no autorizadas, como también debemos considerar en cuenta que la falla de un sistema de información o el funcionamiento indebido del mismo, le genera a las organizaciones modernas que dependen de éstos sistemas, grandes pérdidas en su capacidad de operación y en los servicios que ofrecen. Por lo tanto, la gestión de la seguridad de la información es el establecimiento de las políticas para administrar y controlar eficientemente el funcionamiento de un sistema de información, que permitan protegerlo del acceso de personas no autorizadas, alteración de datos o daños físicos a su plataforma tecnológica.

En consecuencia, los gerentes de los departamentos de TICs deben adoptar correctamente los conocimientos, prácticas y experiencias para atender y proteger la infraestructura tecnológica de información de una organización y al personal que lo utiliza en dichos departamentos. Se ha observado en las organizaciones de Venezuela que no se le presta la debida atención a la importancia de la seguridad de la información para que pueda agregar valor desde el punto de vista gerencial, se ha observado también, deficiencias gerenciales de la selección de productos de hardware y software adecuados para la organización, esto genera pérdidas de tiempo, la falta gerencial de instalación, la adaptación y el mantenimiento de los sistemas de información, proporcionando así un entorno inseguro que no apoya las actividades de los usuarios del sistema de una organización, y afecta a todos los niveles de la empresa. En tal sentido, también se observa que algunas organizaciones o empresas hoy en día no reconocen el valor de las redes de comunicaciones y no están utilizando éstas tecnologías de la información y comunicaciones TICs para garantizar la productividad de su fuerza de trabajo y el servicio a sus usuarios.

Por lo tanto, el objetivo de este estudio es investigar la gerencia y el problema de la seguridad de la información en las organizaciones modernas (Caso de Gandalf Comunicaciones, C.A.) En la actualidad las organizaciones a nivel mundial, trabajan considerablemente en establecer medidas que les permitan resguardar su información, pero aún existen organizaciones que no cuentan con los últimos adelantos tecnológicos en materia de gestión de seguridad de la información, así como también no tienen una cultura de seguridad para los usuarios dentro de la organización o planes de contingencia que les permitan recuperarse rápidamente de un ataque externo o interno en sus sistemas de información. En este sentido, el tema de investigación seleccionado, permitirá al investigador, mediante la aplicación de los conceptos teóricos y prácticos, sobre la seguridad de la información en las redes de comunicaciones, dar a conocer la gestión y los riesgos de seguridad en las TICs, y mostrar el desempeño de la seguridad en los sistemas de información que apoyan las gestiones empresariales de la empresa Gandalf Comunicaciones, C.A.

Por todo lo señalado es que se justifica elaborar y presentar la propuesta de tipo histórico/documental, que sirva de herramienta de TICs para que la empresa Gandalf Comunicaciones, C.A.**,** pueda contar con soluciones teóricas que aborden las problemáticas

del control y seguridad de la información; y de esta manera aumente sus niveles de competencia en los mercados nacionales e internacionales. Esta investigación tiene enfoque tecnológico y operativo, tiene como título "La Gerencia y el Problema de la Seguridad de la Información en las Organizaciones Modernas (Caso de Gandalf Comunicaciones, C.A.)", adscrito a la línea de investigación: "La Información como Valor Agregado en el Seno de las Organizaciones Públicas y Privadas"**.**

Las teorías con las que se va a abordar la investigación son las que han desarrollado los investigadores Manuel Castells, Peter F. Drucker y los Laudon, quienes han aportados teorías importantes que pudieran servir de referencia para interpretar y analizar, y los cuales son teóricos mundialmente aceptados y reconocidos tanto en el campo de las TICs, como en el campo de la gerencia moderna. En este sentido Laudon y Laudon en su libro *"Sistemas de Información Gerencial"* (2012) definen que la seguridad y el control son las prioridades más importantes en el negocio de la actualidad.

> La seguridad se refiere a las políticas, procedimientos y medidas técnicas que se utilizan para evitar el acceso sin autorización, la alteración, el robo o el daño físico a los sistemas de información. Los controles son métodos, políticas y procedimientos organizacionales que refuerzan la seguridad de los activos de la organización; la precisión y confiabilidad de sus registros, y la adherencia operacional a los estándares gerenciales (p. 293)

Esta investigación es de tipo histórico/documental y por lo tanto vamos a manejar obras elaboradas por conocidos teóricos; además se procederá a investigar fuentes documentales a fin de recoger información o datos en el contexto donde se desarrolla la problemática estudiada. Esta investigación se podrá realizar en el tiempo señalado, y aborda el periodo de tiempo desde el 2011 hasta el 2016 en la empresa Gandalf Comunicaciones, C.A. con presencia en Venezuela, se dispone de fuentes y documentos; usando medios electrónicos e impresos, y la tecnología del internet; por otro lado, el autor de esta investigación es un profesional de ingeniería en telecomunicaciones egresado de la Universidad José Antonio Páez que posee la formación teórica y los conocimientos necesarios, en tanto que presta sus servicios en la empresa Gandalf Comunicaciones, C.A, así como también cuenta con amplia

experiencia en las áreas de las telecomunicaciones, específicamente en el área de las redes de comunicaciones, todo lo referente a configuración de *routers* y *switches*, enlaces de microondas, enlaces satelitales, gerencia y planificación de proyectos y energía solar fotovoltaica, y cuenta con experiencia en el área de las telecomunicaciones, el cual le ha permitido poner en práctica las teorías y conocimientos que adquirió en sus estudios de pregrado, y las experiencias que ha desarrollado le han permitido conocer más acerca de las tecnologías de la información y las comunicaciones, a nivel profesional y personal, los cuales gracias a la maestría ha podido obtener más conocimiento e información de las mismas. Por lo tanto, se afirma que la investigación es factible, en tanto que se cuenta con los recursos necesarios para su ejecución.

Esta investigación tiene un enfoque operativo y tecnológico, en tanto que la gestión de la seguridad de la información, las TICs y la gerencia moderna en la organizaciones y en la empresa Gandalf Comunicaciones, C.A., son importantes para todas las operaciones de estas mismas, se excluyen los enfoques políticos, culturales y educativos debido a que no pertenecen, a las áreas de las TICs, ni al estudio de la gerencia. Esta investigación se justifica o es importante porque su resultado servirá de herramienta o podría ser un recurso teórico para que la empresa Gandalf Comunicaciones, C.A., solucione el problema de la gestión de la información en la gerencia, como un valor agregado prioritario, y de esta manera favorecer su competencia en el mercado, favoreciendo la mejora continua en la empresa.

Por todo lo anteriormente señalado se considera necesario e importante elaborar y presentar a la consideración de la comisión coordinadora de la maestría en gerencia y tecnología de la información de la Universidad José Antonio Páez, la propuesta de esta investigación, que podría ser una herramienta teórica para el gerente moderno Venezolano y para la empresa Gandalf Comunicaciones, C.A., así como también, podría abrir una nueva vertiente en el estudio de la seguridad de la información, y para que otros investigadores del área de la gerencia y la gestión de la seguridad de la información, aborden esta problemática de relevancia para la competitividad de las organizaciones.

1.2.Objetivos de la Investigación

1.2.1. Objetivo General

Investigar la gerencia y el problema de la seguridad de la información en las organizaciones modernas (Caso de Gandalf Comunicaciones, C.A.)

1.2.2. Objetivos Específicos

1.2.3. Identificar las situaciones de riesgo y potenciales amenazas que podrían afectar la seguridad de la información como valor agregado prioritario en el seno de la organización Gandalf Comunicaciones, C.A.

1.2.4. Describir las herramientas tecnológicas necesarias para el control y prevención de los riesgos, en pro de la seguridad de la información, y acerca de cómo afectan la toma de decisiones gerenciales en las organizaciones modernas.

1.2.5. Analizar la confiabilidad, integridad y disponibilidad de la información en la infraestructura de las TICs en la empresa Gandalf Comunicaciones, C.A.

1.3. Importancia o Justificación de la Investigación

Los aspectos y teorías que se abordaran en esta investigación, son relevantes ya que podrían servir para que la empresa Gandalf Comunicaciones, C.A., cuente con una herramienta teórica sobre la importancia que tiene la gestión de la seguridad de la información como valor agregado prioritario en las organizaciones modernas, así como también se aborda la problemática de que las organizaciones modernas al no contar con suficiente información acerca de la gestión de la seguridad de la información corren riesgos, y se les hace difícil aplicar herramientas gerenciales que les permitan solucionar los problemas en materia de la seguridad de la información.

El autor de esta investigación considera relevante los aspectos concernientes a la gestión de la seguridad de la información como valor agregado prioritario de la gerencia de las organizaciones modernas, porque las TICs son cada vez más usadas para el apoyo y automatización de todas las actividades de las empresas. En relación a la gerencia moderna, las organizaciones en Venezuela y en la empresa Gandalf Comunicaciones, C.A., podrían obtener importantes beneficios, entre los que caben mencionar la mejora de sus operaciones y funciones de cada uno de sus departamentos, la llegada a una mayor cantidad de clientes, la optimización de sus recursos, la apertura a nuevos mercados, y contar con herramientas de TICs que permitan brindar a los clientes un servicio de mejor calidad y una comunicación más fluida, no sólo con sus empleados sino también con sus proveedores. Es decir, una efectiva gestión de seguridad de la información les permite a las empresas lograr aumentar considerablemente su eficiencia y su competitividad en el mercado nacional y extranjero, en tanto que esta investigación podría ser un aporte o herramienta teórica de relevancia para la empresa Gandalf Comunicaciones, C.A.

La investigación se podría considerar importante para el desarrollo de la nación y de la sociedad porque con los constantes avances y masificación que han experimentado las tecnologías en éstas últimas diez décadas en el desarrollo de internet, han dado una gran revolución en el seno de la sociedad actual, la cual se ve en la necesidad de actualizarse con respecto a la gestión y seguridad de los sistemas de información dentro las TICs. La investigación podría considerarse original debido a que podría abrir estudios en el área de la gerencia y de la seguridad de la información, para que otros investigadores de estas áreas puedan utilizar la información recabada en ésta investigación como antecedentes o bases teóricas para la apertura de otras investigaciones en las áreas de la seguridad y gestión de los sistemas de información.

La investigación podría contribuir a solucionar, prevenir o resolver los problemas presentes o futuros en forma teórica en el área de seguridad de la información, en la empresa Gandalf Comunicaciones, C.A., las TICs, y la gerencia, así mismo podría ayudar a comprobar los niveles de seguridad de la información en la empresa Gandalf Comunicaciones, C.A.

La metodología de la investigación, el cual es bajo la modalidad histórico/documental, se considera pertinente y adecuado a la problemática y al objeto de estudio que se aborda en esta investigación, en tanto que se trata de una problemática que requiere enfoques teóricos, operativos y tecnológicos, basado en la ciencia, y en pro de la creación del conocimiento, sin tomar en consideración los enfoques políticos o educativos, ya que como se ha mencionado anteriormente, no son acordes a las áreas de estudios de las tecnologías de la información y la comunicación, y el estudio de las ciencias gerenciales, se podría considerar, que al presente y en el futuro, las organizaciones modernas cada día van a necesitar de investigaciones afines a estas, porque el estatuto del valor de la información va a evolucionar, y cada día serán más necesarios los niveles de protección, salvaguarda, disponibilidad y cuidado de la información, y la gestión de la seguridad de la información debe tener siempre, un paso adelante en ventaja de las amenazas y los riesgos.

1.4. Limitaciones y Factibilidades del Proyecto

Esta investigación de tipo histórico/documental es un estudio acerca de la gerencia y el problema de la seguridad de la información en las organizaciones modernas (Caso de Gandalf Comunicaciones, C.A.), en el periodo de tiempo desde el año 2011 hasta el año 2016 considerando teóricos importantes como por ejemplo Manuel Castells, Jeimy Cano, Peter Drucker y Laudon y Laudon quienes son reconocidos a nivel mundial por sus aportes a la ciencia por que han escrito importantes teorías como lo son *"La función de seguridad de la información" (*Jeimy Cano; 2014), *"La ciudad informacional: tecnologías de la información"* (Manuel Castells; 2014), *"Su visión sobre la administración, la organización, la economía y la sociedad"* (Peter Drucker; 1996), *"Los Desafíos de la Gerencia para el Siglo XXI"* (Peter Drucker; 2002) y *"Sistemas de información gerencial"* (Laudon y Laudon; 2014).

En tanto que la empresa Gandalf Comunicaciones, C.A., es importante para la nación debido a que integra una parte de la producción tecnológica, mercados, flujos comerciales y financieros que aportan tecnologías a la sociedad Venezolana aportes como por ejemplo la información, comunicación, nuevos empleos en el territorio nacional, y el autor de esta investigación labora en esa empresa por lo tanto existe factibilidad humana.

La tesis correspondiente a ésta investigación va a ser presentada en el año 2017 y es factible debido a que se cuenta con los recursos necesarios para llevar a cabo dicha investigación, y es una investigación documental, que consiste en la recolección de información, fundamentos, aspectos importantes y análisis, por lo tanto, la investigación es viable.

De acuerdo a lo mencionado en los párrafos anteriores, la investigación tiene enfoques principalmente tecnológicos y gerenciales en la seguridad de los sistemas de información en las que se encuentran las TICs y se excluyen los enfoques políticos, culturales y religiosos debido a que no tienen ningún tipo de relación con la gestión de la seguridad de la información porque son áreas diferentes y no tratan nada que tenga relación con la investigación. El autor de esta investigación es un profesional en telecomunicaciones con experiencia en el área de la seguridad de la información y también en áreas como redes de comunicaciones, sistemas satelitales y de microondas, gerencia de proyectos y sistemas informáticos. La investigación podría ser una herramienta teórica para Gandalf Comunicaciones, C.A., ya que aborda los aspectos importantes referentes a los riegos que conlleva no implementar un sistema de gestión de la seguridad de información en las TICs que manejan las organizaciones modernas.

El automatismo intensivo de las tecnologías de la información y comunicaciones como patrimonios para generar, almacenar, transferir y procesar la información, se han desarrollado de forma exponencial en los últimos años y se han convertido en un componente necesario para la actividad de la sociedad de hoy día. La sociedad ha alcanzado una gran dependencia respecto a la administración apropiada de la información, por lo que las aplicaciones informáticas son cada vez más importantes, así como también los requerimientos de seguridad son cada vez mayores y esenciales en las operaciones de las organizaciones modernas, asegurar la información en las empresas requiere de instalar una cultura de seguridad y realizar una adecuada combinación de conceptos, tecnologías, metodologías, estándares, herramientas de gestión y recursos humanos capacitados, por medio de la aplicación de métodos gerenciales en los departamentos de TICs de la organización.

CAPITULO II
MARCO TEORICO

La información actualmente se ha convertido en un activo distinguido para las organizaciones modernas en Venezuela, y éstas se apoyan en la seguridad de la información para su conservación y resguardo. Debido a la evolución constante de las TICs, las cuales exigen un mayor esfuerzo para garantizar la seguridad de la información en las organizaciones modernas ante los constantes ataques y amenazas que en la actualidad atentan contra la seguridad de la información, las cuales dichos ataques son más avanzados con la evolución de las tecnologías por lo que la privacidad de los datos personales, comerciales y financieros de las personas son vulnerables a cualquier tipo de ataques o amenazas, por ese motivo las organizaciones modernas deben contar con un Sistema de Gestión de Seguridad de la Información, con el objetivo de poder establecer y mantener un gobierno de seguridad en los departamentos de TICs en las organizaciones modernas, organizado a las necesidades y objetivos estratégicos de la empresa, compuesto por una estructura organizacional con roles y responsabilidades que debe llevar a cabo el gerente, así como también un conjunto de políticas, procesos y herramientas, que le permitan gestionar de la mejor forma los riesgos que puedan atentar contra la confiabilidad, integridad y disponibilidad de la seguridad de la información en la empresa.

2.1.- Antecedentes de la Investigación

Cristian David Macen Rojas, realizó una investigación titulada *"Políticas de Seguridad de la Información"* (2014); y en ella enfocó la relación que existe con respecto a la ausencia de las políticas de seguridad en los departamentos de TICs en las organizaciones, el cual en la actualidad dicha ausencia puede ocasionar graves efectos para las operaciones de las organizaciones.

Cristian menciona en su investigación y coloca como ejemplo el ataque que sufrió la empresa Ebay, en el que intrusos enviaron de forma fraudulenta correos a sus 55 millones de usuarios para solicitarles que confirmaran sus datos a través de un portal o sitio web de Ebay, igualmente falso, para una comprobación técnica, por ese motivo pocos clientes sospecharon que se tratase de un fraude. Por ese motivo y situación toda organización debe contar con políticas de seguridad de la información. En la investigación se analizan los riegos de la seguridad de la información, se dan a conocer los aspectos culturales y técnicos para el manejo de la información, así como también explica el desarrollo de las políticas que se deben llevar a cabo para garantizar una gestión efectiva de la seguridad de la información.

De acuerdo a Cristian Macen, citado por la Dirección de Tecnología Informática de la Universidad Distrital José de Caldas, se refiere a *"Políticas para la Seguridad de la Información como un manual de seguridad de la información"*, que formaliza su compromiso con el proceso de gestión responsable de la información, que tiene como objetivo garantizar la integridad, confiabilidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales (p. 20). Cristian Macen refleja la importancia que deben tener las políticas de la seguridad de la información, donde las organizaciones elaboren un manual que contempla todos los procedimientos y políticas de seguridad que se deben llevar a cabo ante cualquier situación de fallas o problemas que se presenten, el cual el mismo manual debe ser elaborado por el gerente del departamento de TICs conjuntamente con su equipo de trabajo, luego de haber realizado un estudio previo sobre las amenazas y vulnerabilidades en los sistemas de información en la organización.

Tania Del Lourdes Guevara Huilcarema, en su investigación titulada "*Modelo de Gestión de Seguridad para la Corporación Financiera Nacional Basado en Gestión de Riesgos" (2013)*; en donde se enfatiza en el análisis y evaluación de riegos, adquiriendo así de esta forma importantes requerimientos de la organización en proporción a la seguridad de la información; en la cual se basó su investigación. Explica de igual forma técnicas de identificación, evaluación y tratamiento de riesgo, así como también la integración que tiene la gestión de riesgos con otras áreas a nivel gerencial. Tania comenta un dato importante sobre la gestión de riesgos de la información, por lo que cita lo siguiente:

> Una vez se ha delimitado la gestión de riesgos de seguridad de la información, inmediatamente se procede a analizar y evaluar los riesgos, a este proceso la norma lo denomina Valoración del Riesgo; si la valoración de los riesgos resultante satisface las necesidades de la organización y/o cumple con las especificaciones de los criterios de aceptación del riesgo establecido en el primer proceso, se procede a dar tratamiento a los riesgos identificados, caso contrario, los procesos uno y dos se repiten iterativamente hasta llegar a un nivel aceptable de riesgo (p. 12).

Claramente Tania en su investigación enfatiza la importancia que representa la gestión del riesgo de la información y lo vital que es la valoración del riesgo, el cual va a determinar el grado de riesgo que tiene la información y hasta qué grado es aceptable el mismo para la organización, en el que como ya hemos conocido la información es un activo de gran importancia para las organizaciones, por lo que determinar el nivel del riesgo de la información es un dato muy importante para las organizaciones actuales.

El Instituto Nacional de Ciberseguridad en su publicación titulada *"Ciberseguridad en la identidad digital y la reputación online"* (2016); menciona que la **identidad digital corporativa** sirve a las empresas para diferenciarse en internet, y debe estar basada en una estrategia de comunicación sólida dirigida a alcanzar una posición a través de su página web, las redes sociales y todo tipo de comunicaciones con clientes y proveedores. Además, la **reputación online corporativa** calcula la valoración que realiza el público de una organización a través de sus perspectivas sobre el buen o mal uso de los medios que ofrece internet. Por este motivo, para la organización de la actualidad es también necesario vigilar las redes para observar el impacto que tienen las comunicaciones y corregir las posibles fallas o conflictos. La publicación analiza los riesgos de Ciberseguridad tanto para la identidad digital corporativa como para la reputación online, como por ejemplo: la suplantación de identidad, la fuga de información o las publicaciones difamatorias. También se revisa el marco legal y distintas recomendaciones preventivas y reactivas para hacer frente a los posibles ataques. En ésta publicación se cita:

> Cada vez son más las organizaciones (tanto públicas como privadas) que gestionan de forma profesional su identidad digital corporativa y su reputación en Internet, desde la perspectiva de la prevención frente a posibles problemas, como en la reacción y mitigación en caso de incidentes (p. 07).

Lo que da a conocer que en la actualidad, las organizaciones modernas están considerando con más importancia la situación de la seguridad en los sistemas de información que son los activos más importantes dentro de la organización.

Gabriela Agostini en su investigación titulada *"El Dominio del Saber y la Información como Factores de Gerencia y Competitividad en el Seno de las Naciones Latinoamericanas (Caso Venezuela)"* (2016), en ella se encamino a desarrollar unos de los principios operativos para implementar efectivamente las TICs en los procesos gerenciales, dentro de los cuales se encuentra uno de los principios que trata sobre la seguridad de la información y es el que mencionara a continuación:

> Tercer principio: sentido de urgencia informacional de toma de decisiones. Cada cargo requiere y usa información a diario, diferente tipo de información, información es información a distintos eslabones. La gerencia de la organización debe delimitar y conocer qué cargo domina cual información, y cuáles son los medios para lograr el acceso oportuno a lo que el colaborador requiere, es importante erradicar la burocracia de las organizaciones y fomentar la gerencia de liderazgo horizontal, de esta manera se distribuyen las responsabilidades de forma efectiva y eficiente. (p. 128).

El tercer principio del sentido de urgencia informacional establecido por Gabriela, en la toma de decisiones claramente expresa que la gerencia debe estar al tanto de aclarar qué cargo dentro de la organización presenta o maneja mayor influencia en determinada información y cuál sería la misma, con el propósito de lograr que se cumplan con todos los requisitos necesarios, por lo que es indispensable eliminar el trámite de procesos centralizados y descentralizados en las organizaciones y promover más el liderazgo gerencial en equipo para

cumplir de forma más precisa con las metas propuestas. El manejo y uso adecuado de la información no necesariamente debe estar basado en procesos administrativos burocráticos en la cual el único con permisos sea la gerencia, algunos cargos en los departamentos, podrían tener accesos a determinada información, así como también podrían tener restricciones a otra información. Es una función de la gerencia, disponer que cargos o departamentos en la empresa manejarán o tendrán acceso a cuales informaciones, incluyendo las que el mismo gerente necesita para la toma de decisiones, esto sería parte de un plan de protección interna de la información. El acceso efectivo de los empleados a la información, está relacionado con un conjunto de técnicas o metodologías para realizar una búsqueda, encontrar, categorizar, alterar o modificar y tener disponibilidad y acceso a la información que se encuentra dentro de un sistema de información en la empresa, con herramientas de las TICs como repositorios, bases de datos, archivos etc. El acceso a de los empleados a la información involucra muchos aspectos relacionados con la seguridad y la confidencialidad de la información de la empresa, el objetivo principal de los accesos a la información por parte de empleados internos, es garantizar el uso efectivo de la información usando la menor cantidad de recursos, como por ejemplo, el recurso del tiempo.

2.2.- Bases Teóricas

Según Laudon, las empresas modernas deben disponer de sistemas de información basada en las TICs, porque para este autor los sistemas de información son esenciales para realizar las actividades comerciales diarias, así como para lograr los objetivos de negocios estratégicos. Sectores completos de la economía serían casi inconcebibles sin las inversiones sustanciales en los sistemas de información (2ed., 2012).

> Las empresas de comercio electrónico como Amazon, eBay, Google y E*Trade simplemente no existirían. Las industrias de servicios de la actualidad —finanzas, seguros y bienes raíces, al igual que los servicios personales como viajes, medicina y educación— no podrían operar sin los sistemas de información. Asimismo, las empresas de venta al detalle como Walmart y Sears, además de las empresas de manufactura como General Motors y General Electric, requieren los sistemas de información para sobrevivir y prosperar. Al igual que las oficinas, los teléfonos, los archiveros y los edificios altos y eficaces con elevadores fueron alguna vez la base de los negocios en el siglo XX, la tecnología de la información es la base para los negocios en el siglo XXI (p. 44).

Por lo cual significa que cada vez hay una dependencia mayor entre la habilidad de una organización de usar la tecnología de la información y su experiencia para poder implementar estrategias corporativas y lograr los objetivos colectivos. Para Laudon y Laudon las actividades comerciales siempre van buscar de manera continua mejorar la validez de sus transacciones para poder obtener una mayor rentabilidad de sus productos, algo que es común en los mercados de las organizaciones modernas. Las tecnologías de información y comunicaciones, en la actualidad son uno de los instrumentos más importantes que tienen disponibles los gerentes, para de esta forma conseguir grandes niveles de eficiencia y productividad en las transacciones comerciales y operaciones de la organización, dato que deben tomar muy enserio las organizaciones, especialmente al tener que ajustarse a las permutaciones en las prácticas de negocios y el comportamiento gerencial.

Manuel Castells en su libro *"La ciudad informacional. Tecnologías de la información, estructuración económica y el proceso urbano-regional"* (2014), estudia la correlación existente entre las nuevas tecnologías de la información y comunicaciones; y los procesos regionales en el extenso contexto de la transformación histórica dentro de la cual surgen y desarrollan las tecnologías de la información y comunicaciones. El objetivo principal que expone Castells en ésta investigación es centrarse en el levantamiento de un nuevo modelo de una organización socio-técnica (que él la llama *modo de desarrollo informacional*), así como en una estructuración del capitalismo como órgano imprescindible para la organización económica de la colectividad de hoy día. Castells también analiza sobre la presencia de un acumulado de innovaciones que se han venido articulando auténticamente e incluyen al

capitalismo como un nuevo y moderno sistema social, a la información comprendida como el modo de desarrollo en el que la información suplanta a la mano de obra como elemento determinante y a las tecnologías de la información y comunicaciones como fuertes herramientas de trabajo en las organizaciones transnacionales. El fundamento teórico en el que se basa, es que las corporaciones o empresas están organizadas en función de los conocimientos humanos constituidos por las relaciones de manufactura (acción ejercida por el hombre sobre la materia para obtener de ella un producto que le favorezca), práctica (acción de los seres humanos sobre sí mismos en el cuadro biológico y pedagógico para la bienestar de sus necesidades) y jurisdicción (relación de los seres humanos que sobre la base de la producción y de la experiencia impone la voluntad de unos individuos sobre otros por medio del uso potencial o real de la violencia) comprobadamente determinadas.

Manuel Castells (2014) en su investigación utiliza el conocimiento de modo de producción, el mismo hace un reseña existente en las movimientos sociales de manufactura que se dan dentro del marco de una sociedad para acceder a las necesidades de mayor importancia, y en el cual se expresa una diferencia notoria entre la adjudicación que termina sobrando y los objetivos que encontramos en el modo de producción capitalista y posteriormente lo diferencia del modelo de desarrollo, que vienen siendo las relaciones técnicas de producción, o en otras palabras, las definimos también como los procedimientos tecnológicas mediante los cuales la responsabilidad del trabajo funciona sobre determinados factores o elementos que van a permitir crear un beneficio en común.

Aquello que evidencia Castells es la presencia de nuevo paradigmas relacionados a las TICs, a medida que ha avanzado la ciencia y el desarrollo que nuevas técnicas y tecnologías de la información y la comunicación, y que ha originado nuevos modelos de desarrollos a nivel de empresas en el sector de la información, como se ha evidencia en el último siglo, esto es debido a la globalización y al avance de las TICs. Manuel Castells deriva de una aproximación muy interesante a las actuales transformaciones socioeconómicas de la sociedad occidental, en la que se exponen las características de la revolución tecnológica en curso y en la que se intenta formalizar las relaciones entre capitalismo, informacionalismo y cambio tecnológico. (p. 19).

Peter Drucker en su libro *"Los Desafíos de la Gerencia para el Siglo XXI"* (2002) ofrece crónicas relacionadas con las ideologías gerenciales con vertientes impulsadas a la globalización, y la disposición para tomar una ventaja y ser parte del cambio organizacional, y relacionado a el capital humano, y las relaciones humanas, como retos para aquellos que llevan a cabo roles gerenciales, y que tienen bajo su responsabilidad el cumplimiento de los objetivos de éxito en las empresas modernas, habida cuenta que la gerencia es el ente principal de decisiones en las empresas, y que de esta misma depende en gran parte y responsabilidad, el desarrollo de las naciones, tal y cual como lo establece el padre de la gerencia, Peter Drucker:

> El centro de una sociedad, es la institución, administrada como el órgano de la sociedad que está para producir resultados, y la administración es la herramienta específica, la función específica, el instrumento específico que capacita a la administración para que produzca resultados. (p. 57).

El aspecto teórico mencionado por Drucker nos explica que el gran reto para las organizaciones modernas se encuentra originalmente en la integración, la diversificación, la innovación, y la creación de nuevas y mejores estrategias a nivel tecnológicos que le permitan a las organizaciones asumir los cambios necesarios para seguir compitiendo en el mercado mundial, y desempeñarse siendo competitivos fácilmente en dichos mercados.

De forma que dicho de ésta manera, es necesario que las organizaciones modernas se desasgan de las antiguas ideas administrativas que se ofrecían a establecer estructuras y jerarquías, examinando solo resultados operativos, haciendo a las organizaciones débiles y reacios al cambio y/o actualización tecnológica, trayéndoles así resultados negativo y pérdidas económicas para dichas organizaciones transnacionales, la denominada gerencia vertical, por el contrario, la gerencia actual promueve a colaboradores o trabajadores del conocimiento más activos y participativos, y menos pasivos.

Por lo tanto se debe mantener al personal de la organización informados de los cambios más recientes a nivel interno y externo de la empresa, como por ejemplo la globalización, si es viable observarlos como grandes oportunidades para hallar el camino al éxito, pero para que esto sea posible, Peter Drucker en sus obras comenta algunos ejemplos que ayudan con el proceso, y a su vez contribuyen con la perfección continua y sistemática de la organización, como lo es aprender de los errores del pasado y tener una visión más real de los acontecimientos, que viene siendo el mejoramiento de la organización, lo cual se debe tener presente que debe realizarse paulatinamente, para no cometer errores, pero siendo persistente por supuesto, y por último, el aprovechamiento del éxito, es decir percibirlo como una gran oportunidad. También se debe pensar buscar el mantenimiento de la fuerza laboral, para asegurar el bienestar y la futura supervivencia de las organizaciones modernas en las economías desarrolladas, este desafío consiste en pensar más en la productividad de la práctica de los conocimientos de las personas, y no en la rentabilidad que logra la organización por medio de este trabajo, pues así, se eleva la productividad del trabajo cimentado en el conocimiento y de quien trabaja con él. La aparición de nuevas tecnologías y la tendencia a la globalización sobrellevan una serie de cambios que afectan a todas las organizaciones modernas y plantean nuevos retos a los empresarios, quienes deben analizar de forma muy detallada de cómo van a abordar éstos nuevos retos tecnológicos. Peter Drucker, hoy día es considerado uno de los grandes especialistas de la historia en la gerencia actual, en sus investigaciones presenta sus opiniones y juicios acerca la situación presente en la actualidad y que se presentara en un futuro inmediato, por supuesto que esas opiniones y juicios las realiza desde un punto de vista presente en varias perspectivas.

Este libro titulado "*Los Desafíos de la Gerencia para el Siglo XXI"* (2002), es un placentero diálogo entre dos continentes como lo son Oriente y Occidente en el que van naciendo todos los problemas, retos y desafíos a los que debe enfrentarse el empresario actual en un mundo que constantemente cambia y evoluciona en materia de tecnologías de la información y comunicación. Independientemente de todo prejuicio y por encima de cualquier tipo de ideologías, la actual convivencia de las tecnologías de la información y comunicación más avanzadas y con los valores humanistas tradicionales de nuestra civilización, exige una concentración serena pero recóndita acerca del presente y el futuro de las nuevas tecnologías. (p.200)

Peter Drucker también aborda teóricamente sobre la nueva revolución de la información y explica sobre la información que requiere el gerente y la información que éste debe proporcionar, así mismo, inspecciona la productividad de las personas que trabajan con el conocimiento y demuestra que para lograr un mayor rendimiento se necesitan cambios en las condiciones de los individuos, las organizaciones y cambios estructurales en el trabajo.

CAPITULO III
MARCO METODOLOGICO

El marco metodológico describe los procedimientos de metodología a través de los cuales la investigación se va a ejecutar, con el objetivo de abordar el objeto de estudio o problema de forma crítica, y de esta manera generar saberes y conocimientos que podrían ser de utilidad para otros proyectos de investigación.

3.1. Tipo y Diseño de Investigación

El tipo de diseño de la investigación es una investigación histórica/documental, apoyada en la información o estudio de antecedentes a nivel descriptivo. En éste sentido, ésta investigación tiene como título "La Gerencia y el Problema de la Seguridad de la Información en las Organizaciones Modernas (Caso de Gandalf Comunicaciones, C.A)" para la definición de las herramientas y políticas de seguridad que permitan proteger la información de las organizaciones, y que en la empresa Gandalf Comunicaciones, C.A se aborden las problemáticas que enfrentan en relación a la seguridad de la información. Situación bastante importante hoy en día, donde las nuevas tecnologías de la información y comunicaciones, se han integrado activamente en las organizaciones. Los planteamientos en ésta investigación, permiten al investigador, analizar, evaluar y proponer las herramientas o los lineamientos necesarios que contribuyan a reducir y los riesgos en la seguridad de la información.

Se trata de que la empresa Gandalf Comunicaciones, C.A tenga o cuente con herramientas teóricas basadas en TICs y en el estudio de la gerencia que permitan mejorar la gestión de la seguridad de la información, y de alguna manera, colaborar con soluciones teóricas a la problemática bajo estudio, que también podría servir de referencia para otras organizaciones modernas en Venezuela. La investigación documental es un proceso basado en la búsqueda, recuperación, análisis, critica e interpretación de datos secundarios, es decir, los

obtenidos y registrados por otros investigadores en fuentes documentales, ya sean impresas, audiovisuales o electrónicas, se trata de ampliar los conocimientos en el estudio mediante el uso de teorías desarrolladas por reconocidos teóricos, como por ejemplo Peter Drucker, Manuel Castells y Laudon y Laudon.

3.2. Técnicas e Instrumentos de Recolección de Datos

Una vez que se define el diseño del proyecto de investigación, es necesario especificar las técnicas o instrumentos que permitan recolectar los datos necesarios para poder cumplir con todos los objetivos que nos hemos planteado. De forma que para esta investigación se procederá a usar una técnica de observación indirecta, ya que se van a usar documentos, de modo que se van a analizar las teorías y las fuentes de investigadores teóricos de forma cualitativa, por lo que no aplica el uso de encuestas ni de cuestionarios, en tanto que se trata de una investigación de tipo histórico documental.

3.3. Procedimiento y Técnicas de Análisis de Datos

En atención al procedimiento y técnicas de recolección de datos, se utilizaran los documentos obtenidos de las fuentes teóricas para poder ampliar el conocimiento y teorías que podrían ser de utilidad a otros investigadores para la elaboración de sus investigaciones que tengan relación con el objeto de estudio o problemática que se aborda en esta investigación.

CAPITULO IV

LAS TICs Y COMO ABORDAR LAS POTENCIALES AMENAZAS QUE PODRIAN AFECTAR LA SEGURIDAD DE LA INFORMACION EN EL SENO DE UNA EMPRESA

4.1. Historia de la Seguridad de la Información.

Desde el inicio del ser humano, el mismo ha tenido la necesidad de resguardar y proteger con celo los conocimientos adquiridos, debido a la ventaja del poder que éste le producía a otros seres humanos o sociedades. Años atrás en la antigüedad el hombre crea las bibliotecas con el propósito de resguardar la información para luego transmitirla y para evitar que otras personas tuvieran acceso a ella, dando de esta manera las primeras muestras de protección de la información.

Investigadores como Sun Tzu en su libro titulado *"El Arte de la Guerra"* y Nicolás Maquiavelo en su libro titulado *"El Principe"*, ellos mencionan la significativa importancia que representa la información sobre los competidores y el completo conocimiento de sus intenciones a la hora de la toma de decisiones. En los años 1939 hasta 1945, en el desarrollo de la segunda guerra mundial se establecieron e implementaron la mayoría de los servicios de inteligencia en todo el mundo, esto con el único propósito para la fecha y dada la situación de conflicto que se vivía en ese momento, era con el fin de poder obtener suficiente información valiosa y confiable, creándose así de esta manera las primeras agencias secretas de espionaje. Posteriormente con el pasar de los años y con la constante evolución de las tecnologías de la información, que en la actualidad representa un crecimiento bastante significativo, el cuidado y resguardo de la información se ha convertido en un aspecto importante y fundamentalmente a considerar para el ser humano, las organizaciones o empresas y para las sociedades. Con dicha evolución de la seguridad en las tecnologías de la información en estos últimos años, tal tecnología se ha convertido en una carrera profesional totalmente nueva acreditada a nivel mundial donde se ofrecen muchas especializaciones en el área de los Sistemas de Gestión de Seguridad de la Información.

La seguridad de la información es un método que trata sobre las vulnerabilidades, riesgos, amenazas, análisis de espacios, prácticas y políticas de seguridad, que deben ser aplicados y puestas en práctica para evaluar el nivel de seguridad que presentan las tecnologías de la información, por parte de la gerencia en las organizaciones modernas, con el objetivo principal de elevar la confianza en el diseño, uso, almacenamiento, transmisión, disponibilidad, confiabilidad, recuperación y disposición de la información para los usuarios, clientes y proveedores.

Algunas fechas importantes en el desarrollo de la seguridad de la información son:

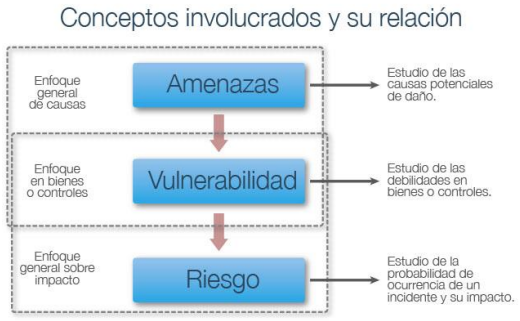
1. En el mes de Junio de 1942, un mensaje mal encriptado fue transmitido entre oficiales de la armada japonesa, el mismo fue interceptado por los enemigos y tuvo como consecuencia la destrucción de 4 portaviones japoneses, culminando así con el fin del dominio de la armada japonesa en el océano pacífico.
2. En el año 1988, Robert Morris, un joven programador, diseño un programa para que utilizando vulnerabilidades de UNIX, se transmitiera de un sistema a otro con gran velocidad infectando todos los equipos conectados a la red y poder sustraer información de los usuarios.
3. En Junio del 2005 un hacker logro tener un listado de más de 50 mil clientes en España, teniendo así acceso todos los datos personales de los clientes, como direcciones, correos, números telefónicos e incluso números de las tarjetas de crédito.
4. En Junio del 2010, VirusBlokAda emitió una alerta por todo el mundo que desencadeno una carrera a nivel internacional para rastrear el malware más sofisticado de computadoras llamado Stuxnet, el cual deja una nueva generación de amenazas cibernéticas.

Por todo lo mencionado anteriormente, es muy importante estar al tanto del aparecimiento histórico de las tecnologías de la información y comunicaciones, para poder así entender la situación a la que nos enfrentamos actualmente en éste siglo XXI, por lo que resulta interesante conocer cuántos acontecimientos tuvieron que suceder para llegar hasta la tecnología de punta que hoy tenemos en nuestros hogares, oficinas y organizaciones, quiénes fueron las personas que idearon e inventaron los diversos desarrollos tecnológicos e incluso determinar hacia dónde se dirige la tecnología y por supuesto hacia dónde va la seguridad de la información. Por este motivo, fue indispensable perfeccionar los recursos tecnológicos con los que se contaba en determinada época, de tal manera que se mantuviera un excelente sistema de gestión de seguridad de la información. En hechos anteriores se tiene información de una serie de sucesos relevantes ocurridos en la historia de la seguridad de la información, en las que fueron surgiendo las primeras amenazas, riesgo y vulnerabilidades como los conocidos virus informáticos, que con la evolución de las tecnologías de la información y comunicaciones, se han vuelto más sofisticados y cada vez más difíciles de detectar. De Igual forma surge la necesidad de mantener un mayor nivel de seguridad de la información en las organizaciones modernas, producido por el avance en las tecnologías de la información. Acorde se perfeccionan los dispositivos de comunicación se tiene que ir perfeccionando la seguridad de éstas tecnologías, manteniendo siempre los principios fundamentales de la seguridad información (integridad, confidencialidad y disponibilidad), que son los pilares fundamentales o las bases en las cuales se sustenta la seguridad en las tecnologías de la información y comunicación.

4.2.Las Amenazas, Riesgos y Vulnerabilidades que podrían presentarse en los Sistemas de Información de una Empresa.

Las organizaciones modernas a medida que van creciendo van acumulando mucha información en sus bases de datos, pero al tener que acumular grandes cantidades de información de forma digital o electrónica, corren el riesgo de que la información sea vulnerable a distintos tipos de amenazas o ataques, esto ocurre debido a que los sistemas de información, gracias al internet, se interconectan entre sí por medio de las redes de comunicaciones, por lo que pueden generar grandes pérdidas económicas a la organización. Los riesgos en los sistemas de información se encuentran presentes cuando convergen las vulnerabilidades y amenazas, por lo que estos dos últimos elementos están cercanamente relacionados entre sí. Las amenazas a la seguridad de los sistemas de información pueden venir de cualquier parte, ya sea de forma interna o externa, pero siempre viene relacionada con el entorno de la organización.

Existen cuatro grupos de tipos de amenazas a la seguridad de los sistemas de información que son: Factores Humanos (accidentes, errores, entre otros.); Fallas en los sistemas de procesamiento de la información; Desastres naturales (terremotos, inundaciones, huracanes); y Actos malintencionados (virus informático, robo de información, denegación del servicio, sabotaje, entre otros). Las vulnerabilidades son una debilidad presente en las tecnologías de la información, por tal motivo se les consideran como características propias de los sistemas de información.



Interacción entre Amenazas, Vulnerabilidades y Riesgos

Figura 1

Actualmente en el mundo digital en el que vivimos, gracias a la evolución de las tecnologías de la información y comunicaciones, las amenazas, vulnerabilidades y riesgos de brecha en la seguridad de los sistemas de información ha aumentado de forma considerable. Así como ha aumentado la cantidad de información que circula cada día por la red, también se ha visto un aumento en el número de medios en los cuales la información es almacenada y luego transferida de manera ilegal sin la debida aprobación del propietario de dicha información. Contrariamente a la mayor conciencia sobre las amenazas, vulnerabilidades y riesgos a la seguridad de la información que encaran las organizaciones de todo el mundo, las brechas de seguridad están aumentando y amenazando seriamente la solidez de los negocios y la privacidad de sus clientes y proveedores. A pesar de que los gerentes y profesionales de las TIC tienen a su disposición una variedad de herramientas para soluciones de seguridad, los cibercriminales todavía atacan los sistemas de información y roban valiosos datos que pueden utilizar para fraude con tarjetas de crédito, robo de identidad y otras actividades maliciosas. Las organizaciones de cada uno de los diferentes sectores industriales continúan notificando de ataques a la seguridad de los sistemas de información y a los activos más sensibles y confidenciales de la misma.

Con la creciente reproducción de dispositivos móviles de almacenamiento como lo son las memorias USB y memorias micro SD involucran una gran amenaza, vulnerabilidad y riesgo para las organizaciones, ya que parte de los empleados se llevan información cuando cambian de trabajo, poniendo así en riesgo la imagen y la integridad de la misma. Pero, la mayoría de las organizaciones no son conscientes de este peligro ya que muchas sin tener los conocimientos previos, se colocan innecesariamente en riesgo al no considerar la potencial amenaza que supone para la seguridad de sus redes los ya citados dispositivos móviles de almacenamiento. En muchos casos, la falta de información y desconocimiento de los principios y procedimientos básicos de seguridad, por parte del personal de TIC y de la gerencia, son los principales motivos de las fallas de seguridad en lugar de la actividad maliciosa (aunque esto último no se puede ignorar). Pese a que el resultado final es regularmente el mismo: se pierde información inestimable y por tal motivo la organización pierde credibilidad, la confianza de sus clientes y proveedores, entre otros factores a considerar de igual importancia.

Por mas difícil que parezca, es realmente fácil que se produzca una vulneración de la seguridad de las redes de información de una empresa y es motivado porque los empleados colocan sus contraseñas sobre sus escritorios, olvidan portátiles o dispositivos de mano en lugares públicos o en sus vehículos. También mantienen sus dispositivos desbloqueados o encendidos (PC, celulares, tabletas) durante la hora del almuerzo o descanso, dejan sin atención las memorias USB con información empresarial y personal sensible o navegan por Internet desde sus casas mientras están conectados a sus redes empresariales. Las organizaciones deben tomar medidas preventivas de seguridad para evitar que ocurran estas fugas de información a sus empleados en materia de seguridad y barreras tecnológicas que impongan los gerentes de la organización. Es necesario hacer un mejor uso de las herramientas y comenzar a ver la seguridad como una inversión en lugar de como un gasto. Estas organizaciones deben poner en marcha un plan eficaz de políticas de seguridad empresarial y darlo a conocer a todos y cada uno de los empleados de la misma y no confiarse de su buena voluntad para cumplir este plan. Con la aplicación de una adecuada política de seguridad, las organizaciones pueden proteger satisfactoriamente sus negocios de daños financieros, legales y salvaguardar su reputación; y de esta forma limitar así el riesgo de que alguna persona o empleado descontento con la empresa desde algún lugar esté esperando pacientemente para infligir serios daños en la red de la empresa y robar información.

La empresa Akamai, líder mundial en servicios de redes de distribución en internet, publico un informe sobre los ataques DDoS contra aplicaciones web en el primer trimestre del 2017, en donde Martin Mckeay, experto principal en seguridad de Akamai cita la siguiente:

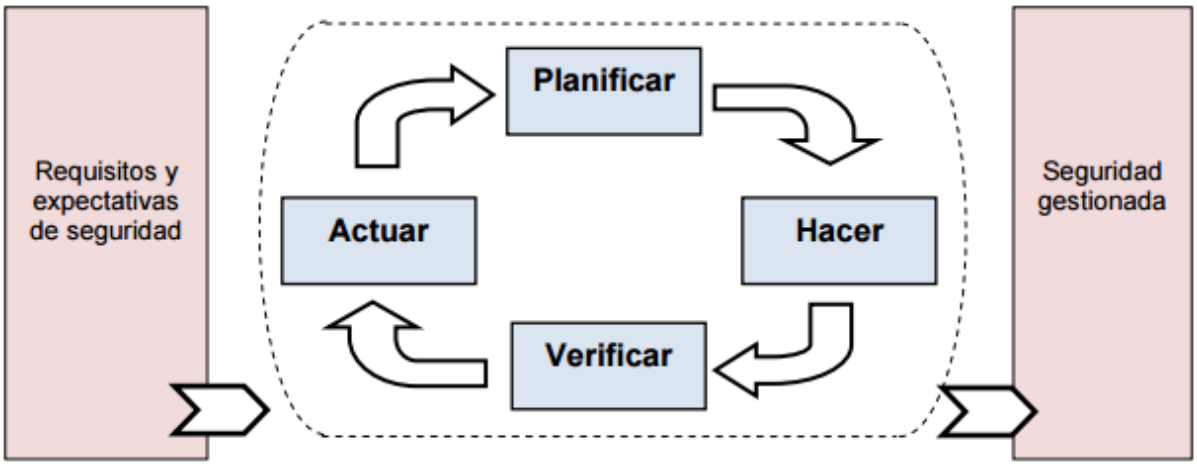
> Los atacantes indagan constantemente los puntos débiles en las defensas de una empresa y cuanto más común es una vulnerabilidad, más eficaz es su ataque y los hackers dedicarán más energía y recursos a ello. Eventos como la botnet Mirai, la explotación utilizada por WannaCry y Petya, el continuo aumento de ataques de SQLi y el resurgimiento del PBot demuestran que, los atacantes no solo migran a nuevas herramientas, sino que también vuelven a utilizar algunas antiguas, cuya eficacia está más que probada.

http://blog.segu-info.com.ar/2017/09/mini-botnet-logra-lanzar-ataque-ddos-de.html?utm_source=Segu.Info&utm_medium=twitter&utm_campaign=seguinfo&m=1

4.3 El dominio y manejo de la Gestión de la Seguridad de la Información como factor de éxito organizacional.

Un Sistema de Gestión para la Seguridad de la Información primero que nada lo definimos como principalmente un conjunto de métodos que permiten gestionar de forma eficiente el acceso a la información, teniendo como principal objetivo asegurar la confiabilidad, integridad y disponibilidad de los activos de información de la organización para así disminuir los riesgos, amenazas y vulnerabilidades a la seguridad de la información. Tenemos que tener en cuenta que toda información es un activo importante para **conseguir el éxito como factor principal y la continuidad** en el mercado de cualquier organización, ya sea pequeña, mediana o grande. Las organizaciones se enfocan en buscar mecanismos más eficaces y eficientes que les permiten asegurar y gestionar la seguridad de la información y de los sistemas que empapelan. Las normas de la familia ISO 27000, en este caso en particular la ISO 27001 es la norma que manifiesta cómo implementar de la forma más efectiva un Sistema de Gestión de Seguridad de la Información en una organización.

El Sistema de Gestión para la Seguridad de la Información se compone de cuatro procesos básicos:



Requisitos Generales para la Implementación de un SGSI

Figura 2

En una organización, el diseño, implantación y mantenimiento de un Sistema de Gestión de Seguridad de la Información, como factor de éxito organizacional, tiene **influencia en las necesidades, en los objetivos**, en los requisitos de seguridad, en los procesos de los trabajadores, en el tamaño y en la infraestructura de la organización. El diseño, implementación, dominio y manejo de éstos sistemas, representan un importante factor de éxito organizacional debido a que le permite a la organización conocer las amenazas, riesgos y vulnerabilidades a las que se encuentra sometida su información, así de ésta manera la organización puede integrar la Gestión de la Seguridad de la Información con el resto de los sistemas de gestión que ya existen en la organización y como aspecto importante también aumenta la confianza de sus clientes, proveedores y empleados, al igual que su imagen ante ellos, convirtiéndose así en un factor diferenciador frente a la competencia.

El convencimiento de los directivos de la alta gerencia en la organización, la creencia en la importancia del cambio tecnológico, la transmisión de la visión y objetivos perseguidos, el compromiso y cooperación por parte de todo el personal de la organización para el cumplimiento de los objetivos planteados, la alineación de los objetivos de todo el personal con los de la organización y la administración adecuada de la información y las tecnologías, son también uno de los factores de éxito más importantes, que bebe llevar a cabo el gerente del departamento de tecnologías de la información y comunicaciones de la organización, velar por el cumplimiento de las normas y políticas de seguridad, así como también brindar el adiestramiento necesario a todo el personal de la organización en conjunto con su equipo de trabajo. El factor de éxito en el dominio y manejo de la gestión de la seguridad de la información ha tenido hoy en día una orientación sistemática, el cual ha logrado una buena señal de las ventajas que se pueden aportar para la gestión de los sistemas de seguridad de la información. El uso de una orientación sistémica para la gestión de seguridad de la información ayudará a los gerentes de este campo a tratar ambientes complejos y dinámicos, y generará un efecto favorable sobre la colaboración dentro de la organización, generando una adaptación al cambio operativo, navegación de incertidumbre estratégica y tolerancia del impacto causado por factores externos.

Otro factor de éxito en la gestión de la seguridad de la información, aparte de factor tecnológico, el cual abarca equipos, software, aplicaciones, entre otros, también debemos mencionar y no menos importante el factor humano, el cual representa la interacción y la brecha entre la tecnología y las personas, para lo cual tiene un valor prioritario en el manejo y dominio de la gestión de la seguridad de la información. Si el personal que labora en la organización no entiende cómo utilizar las tecnologías, no aceptan las nuevas plataformas tecnológicas o no siguen las normas o políticas de seguridad para los sistemas de información, pueden salir graves problemas en la gestión de la seguridad de la información. Por este motivo es vital que el gerente del departamento de TIC, unido con su equipo de trabajo, dedique suficiente tiempo para explicar el uso de la gestión de la seguridad de la información al personal que labora en otros departamentos de la organización.

A continuación se mencionan algunos factores de éxito organizacional adicionales:

• Como principal objetivo a lograr es la concienciación del empleado por la seguridad.

• Realización de comités a distintos niveles (operativos, de dirección, entre otros.) con gestión continua de no conformidades, incidentes de seguridad, acciones de mejora, tratamiento de riesgos.

• Creación de un sistema de gestión de incidencias que recoja notificaciones continúas de los incidentes de seguridad por parte de los usuarios los cuales deben ser reportados y analizados.

• La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.

• La seguridad no es un producto, es un proceso.

• La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.

• La seguridad debe ser inherente a los procesos de información y del negocio.

4.4 Estrategias Gerenciales para el efectivo uso y manejo de las TICs

Las organizaciones modernas en su búsqueda para la mejora de sus productos tienen el objetivo de modernizar sus conocimientos tanto administrativos como tecnológicos y comprometerse con sus proveedores, clientes y usuarios, para lo cual las estrategias gerenciales representan un componente de interconexión entre estos métodos y el ambiente social que tienen un importante y significativo valor. Las estrategias gerenciales actualmente son una herramienta muy útil que la puede implementar cualquier gerente en una organización moderna para lograr el perfeccionamiento y fortalecimiento de las estrategias gerenciales, en consecuencia un gerente debe desarrollar políticas acordes a las exigencias de la organización y emplearlas para que las mismas sean triunfantes. Se definen a las estrategias gerenciales como las que impulsan el desarrollo a través de un procedimiento, en el cual se completan las primeras claves y políticas de una organización, constituyendo una secuencia y armónica de las actividades a realizar, con el objetivo de alcanzar un escenario factible y original con los recursos necesarios.

Observando la forma de cómo mejorar el potencial de las tecnologías de la información para gestionar el riesgo, se debe identificar a las personas más capacitadas para gestionarlo. El gerente de tecnología de la información debe aprovechar las tecnologías para agregar la gestión del riesgo en todas las operaciones del día a día que se presentan en la organización. Todo aquel personal que se encuentre bien capacitado, trabajara para introducir un idioma común para poder hablar acerca de la gestión del riesgo, por lo que trabajarán para ensamblar la administración del riesgo y el monitoreo de las decisiones en la cultura corporativa, en lugar de depender de procesos separados en cada departamento. Trabajaran en conjunto y de forma activa con los gerentes de otros departamentos y funciones de la organización para así lograr cumplir con los objetivos planteados con la colaboración, consenso y trabajo en equipo.

En las organizaciones modernas donde se ha establecido una comisión para la gestión de estrategias, el gerente del departamento de tecnología de la información puede ayudar a mejorar las capacidades para la toma de decisiones de ese grupo, proporcionando acceso oportuno a información relevante, facilitando una visión de buenas estrategias a nivel de la organización, y homologando los distintos temas para el buen uso de las TICs que abordan a cada uno de los departamentos. La función del gerente supone el intercambio de ideas. La manera en que la tecnología de la información y comunicación en la organización administre las estrategias debe ser consistente con los enfoques establecidos por la función de la gestión de las mismas. Pero al mismo tiempo, el equipo de trabajo del gerente del departamento de tecnología de la información y comunicación debe proporcionar la infraestructura y apoyo a las plataformas tecnológicas para medir y monitorear la aplicación; y el buen uso de las estrategias gerenciales que se estipularon en la organización en general, por lo que dichas estrategias de gestión no solamente trata de soluciones en materia tecnológica, sino también se trata de gerencia efectiva y liderazgo.

Un gerente que aplique estrategias gerenciales y promueva el uso adecuado de las TICs de manera eficiente y eficaz enfoca su atención a prestar más importancia a los siguientes factores:

- ✓ Identificar, evaluar, administrar e informar debilidades en los sistemas de información que amenazan la seguridad, privacidad y continuidad de la organización.
- ✓ El uso de la infraestructura tecnológica en toda la organización para ayudar a otros departamentos.
- ✓ Jugar un rol ejecutivo para asegurar que dicha estrategias gerenciales se consideren de manera apropiada y ayudar a los directivos a entender su importancia para la seguridad de la información en la organización y formular los planes de acción que se requieran.

La creciente necesidad de las estrategias gerenciales en los sistemas de información en forma eficaz y eficiente, obliga a los gerentes de tecnologías de la información a redefinir su función, en una que sea más creativa, proactiva, innovadora y estratégica. Cuando el equipo de trabajo busca orientación en temas cada vez más complejos sobre el ejercicio del poder a nivel corporativo, las estrategias gerenciales, el buen uso de la TIC y el cumplimiento de normas, hacen que el rol activo del gerente se hace cada vez más necesario e importante. Hoy en día las estrategias gerenciales cumplen una función más amplia, que exige una perspectiva más profunda y extensa de cómo el departamento de TICs puede evolucionar de sus obligaciones convencionales de proteger los activos de la organización, a una nueva responsabilidad estratégica de generar valor y mejorar la competitividad para la misma. Al realizar esto, los gerentes de TIC mejorarán el destino de toda la organización, de las personas de cada departamento, al igual que su propio crecimiento y desarrollo profesional. Para el uso efectivo y manejo de las TICs el gerente, junto con su equipo de trabajo deben diseñar e implementar un conjunto de políticas de seguridad de la información, medidas preventivas y herramientas que permitan proteger la información de la organización, por lo que se deben definir estándares y normas que permitan asegurar la misma.

La implementación de Políticas de Seguridad de la Información es un proceso que debe abarcar a toda la organización, por ende, debe estar avalado y contar con un fuerte apoyo de los directivos de la alta gerencia, ya que sin este apoyo, su implementación será más compleja e incluso puede fracasar. El gerente de TIC junto con su equipo de trabajo debe diseñar un manual de políticas de seguridad, normas y estándares como medidas preventivas y herramientas que permitan proteger la información de la organización. Entre los estándares que se pueden aplicar como herramientas se tienen las normas o estándares ISO 17799, ISO Serie 27000, COBIT, ITIL, LEY SOX y COSO que son los más utilizados y recomendados a nivel internacional para la seguridad de los sistemas de información.

Es importante mencionar que al momento en el que el gerente elabore el manual de seguridad y exponga en el mismo las políticas de seguridad de la información, se consideren los siguientes aspectos:

- Desarrollar un análisis de riesgos en los sistemas de información, para valorar las amenazas y vulnerabilidades en los activos y así adecuar las políticas a la realidad de la organización.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar a los gerentes en cada departamento, pues son ellos los interesados en proteger los activos críticos en su área.
- Monitorear periódicamente los procedimientos y operaciones de la organización, de forma tal, que ante cualquier cambio, las políticas puedan actualizarse oportunamente.
- Especificar de forma explícita y concreta el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Las organizaciones modernas de la actualidad al no implementar un sistema de gestión de seguridad de la información como estrategia gerencial, presentan varios riesgos que deben ser considerados por la alta gerencia de la organización, como por ejemplo disminuye la confianza de los clientes, usuarios y proveedores con respecto a la confiabilidad, disponibilidad y acceso a la información que maneja la organización, desmejora la eficiencia de las operaciones y procesos relacionados con la seguridad de la información no pudiendo obtener así de esta manera los conocimientos necesarios sobre las vulnerabilidades, amenazas y debilidades de la seguridad de la información en dicha organización y por último se presentarían perdidas y robos con los activos de información en la misma. Desde la perspectiva de la alta gerencia, un SGSI permite obtener una visión general del estado en que se encuentran los sistemas de información sin caer en detalles experimentados, además de poder observar las medidas de seguridad aplicadas y los resultados obtenidos, para poder con todos estos elementos tomar mejores decisiones estratégicas.

4.5 Análisis de los cambios que pueden afectar la seguridad de la información con la aparición de la nuevas TICs.

En la década los años 80 y principios de los 90 la Seguridad de la Información se concentraba en proteger los equipos de los usuarios, es decir, proporcionar seguridad a las computadoras y su sistema operativo. Esta seguridad lógica, entendida como la seguridad de los equipos informáticos para evitar que dejasen de funcionar correctamente, se centraba en la protección contra virus informáticos, pero luego con la evolución de las tecnologías de la información y las comunicaciones y con el uso globalizado del internet en las organizaciones, la seguridad de la información empezó a enfocarse en la conectividad de las redes de transmisión de datos, protegiendo así los equipos servidores accesibles públicamente a través de internet, controlando también la seguridad de éstos dispositivos de forma remota. Con los cambios constantes en la evolución de las tecnologías de la información y comunicaciones, la seguridad de la información se ve afectada con la aparición de nuevas amenazas, vulnerabilidades y riesgos en el que se vería expuesta y comprometida la información de la organización, la cual es importante para el desarrollo de las operaciones comerciales de la misma y que puede ser fácilmente robada gracias a la conectividad a internet sino se tienen aplicadas las medidas necesarias y políticas de seguridad a los sistemas de información.

En los últimos años una parte de los profesionales del sector de las tecnologías de la información y comunicaciones; y gerentes de dichos departamentos en las organizaciones modernas se han visto en la necesidad de mantenerse actualizados en todo lo relacionado a las tecnologías, ya que hoy día se encuentra un aspecto muy destacado y se trata del almacenamiento en la nube, el cual por medio de una combinación de tecnologías de la información y telecomunicaciones, el alojamiento de información en la nube permite a las organizaciones modernas establecer nuevas formas de trabajo.

Este tipo de servicio en la nube está muy relacionado a la movilidad e incluye ahorros económicos para los clientes y usuarios, pero pone en afectación el tema de la seguridad de la información, porque es un gran desafío para los gerentes de los departamentos de TIC ya que deben aplicar políticas de seguridad mas fuertes debido a que la información de la organización se encuentra en la nube y cualquier persona desde cualquier parte del mundo pudiera acceder a ella, si no está debidamente protegida dicha información. En la medida en que las TICs van evolucionando y cambiando, los profesionales y gerentes de TIC en las organizaciones modernas deben estar constantemente cambiando y actualizando las políticas de seguridad que han implementado, así como también los estándares internacionales que se implementan sobre seguridad de la información, cada día son mejorados e incluso se están desarrollando nuevos estándares.

Actualmente el desarrollo de las tecnologías de la información y comunicaciones se ha venido potenciando a nivel mundial, por lo que se han venido desarrollando herramientas que permiten una gran cantidad de recolección de información y también, el firmamento de registros y su administración en un entorno cada vez mas digital en el que con la interconexión, su disponibilidad se encuentra accesible a cualquier individuo, por ejemplo, la tecnología de la video vigilancia o sistemas CCTV, los cuales son una herramienta muy útil para prevenir delitos e incluso para esclarecerlos, pero se debe tener un dato muy claro, esta herramienta al utilizar las TIC como la conexión a internet y la misma no presente las políticas de seguridad establecidas e implementadas por el gerente, entonces la seguridad de la información se ve seriamente afectada con las nuevas TICs. Los cambios que afectan la seguridad de la información con la revolución tecnológica de hoy día y cada vez más en crecimiento, se ven reflejados en las organizaciones modernas de los sectores públicos y privados. Un ejemplo que se puede mencionar es la organización Gandalf Comunicaciones, C.A. una empresa del sector privado de las telecomunicaciones que se dedica a proveer servicio de internet, en la que a medida en que evolucionan las TICs, Gandalf Comunicaciones actualiza su plataforma tecnológica y políticas de seguridad, ya que al ofrecer servicios de internet, la misma debe salvaguardar su información financiera, la información personal de sus empleados y la de sus clientes, por lo que cuenta con personal capacitado que se encuentra constantemente buscando nuevas tecnologías en materia de seguridad, que sean aprovechadas

y a su vez innovadoras para la empresa y así fortalecer su tecnología en un mercado comercial cada día más globalizado y competitivo.

También la mayoría de las organizaciones modernas están colocando su información en la nube, lo que se llama Cloud Computing, como se mencionó en párrafos anteriores, en donde las organizaciones utilizan esta tecnología para ahorrar costos al migrar su información a la nube, como lo indica Cristian Aldama, director de desarrollo de negocio Cloud Computing de Oracle:

> Actualmente, las empresas son conscientes de que la transformación digital es vital para su continuidad y eso les ha llevado a tomar la decisión de avanzar en su transición a la nube. Una vez tomada la decisión de cambio, lo más importante es elegir un suministrador que ofrezca un portfolio amplio de soluciones, y a partir de ahí ejecutar el plan de implantación. Es un hecho que el modelo cloud permite obtener a empresas de cualquier tamaño ventajas imposibles de conseguir con el modelo tradicional. Contando con una plataforma Cloud completamente orquestada, las organizaciones podrán transformarse, competir y ganar.
>
> ***http://www.revistabyte.es/cloud-computing/toda-la-empresa-la-nube-especial-cloud-computing/***

Al hablar de seguridad cloud o seguridad en la nube los altos gerentes de las organizaciones se reúsan a competir por las soluciones que ofrecen estas nuevas tecnologías, por el motivo de la falta de cultura o educación tecnológica la cual debe ser dada a conocer por el gerente del departamento de TIC de la organización a la alta gerencia de la misma. Esto es muy común en organizaciones que carecen de una inversión en un personal calificado para ofrecer asesorías en el área de TIC. Las amenazas, riesgos y vulnerabilidades, siempre van a estar presentes en la nube de tal forma que la falta de seguridad afecta cualquier a cualquier dispositivo y aplicación tecnológica, por lo que para Guillermo Fernández ingeniero de WhatchGuard sobre su perspectiva de la seguridad de la información menciona:

> La protección de la información y el cumplimiento de la legislación son claves para cualquier empresa. En el caso del uso de soluciones Cloud con mayor motivo. Se ha de tener en cuenta dónde se aloja dicha información, así como qué medidas adopta nuestro proveedor para garantizar la protección adecuada de la misma. Delegar la seguridad en muchos casos no es recomendable por contar con soluciones compartidas y/o con servicios de seguridad limitados, que pueden poner en compromiso nuestra supervivencia.
>
> ***http://www.revistabyte.es/cloud-computing/toda-la-empresa-la-nube-especial-cloud-computing/***

En conclusión, cuando hablamos de seguridad de la información en cloud, es importante que el gerente de TIC aplique las políticas de seguridad más recomendables a las necesidades de la organización, para evitar pérdidas de información ante cualquier posible ataque, riesgo o vulnerabilidad que genere perdida o fuga de información y denegación de servicio que luego resulten en pérdidas costosas para la organización. José de la Cruz, director técnico de la empresa Trend Micro asegura lo siguiente:

> La seguridad y la opacidad en cuanto al tratamiento de los datos, es otro riesgo, según nuestro criterio y experiencia. Últimamente se están dando muchos casos de empresas afectadas por APT o ataques dirigidos que han conseguido extraer datos confidenciales de los servidores sin que los usuarios se dieran cuenta de ello. Los ataques son ahora dirigidos a víctimas específicas y debemos, además de aprovisionar nuestras máquinas con herramientas antimalware de última generación, protegernos de un modo especial si nuestra información está alojada en servidores remotos (nubes) que no vemos ni gestionamos nosotros. Por eso, una solución de protección mediante cifrado va a proteger nuestros datos forma personaliza y evitará también que se produzcan accesos que nosotros no queramos permitir. En Trend Micro apostamos por tecnologías innovadoras que aporten una seguridad inteligente y proactiva.
>
> ***http://www.revistabyte.es/cloud-computing/toda-la-empresa-la-nube-especial-cloud-computing/***

4.6 Acerca de cómo evaluar los sistemas de gestión de la seguridad de la información en las infraestructuras de TICs presentes en las organizaciones modernas.

Existe una gran necesidad de identificar de manera detallada como se encuentra la seguridad de la información en las infraestructuras de TICs que están en las organizaciones modernas, por tal motivo se debe realizar evaluaciones constantes que le permiten al gerente y empleados del departamento de TIC, identificar los puntos débiles y tomarlos en cuenta a la hora de elaborar e implementar un Sistema de Gestión de la Seguridad de la Información o mejorar el que ya se encuentra implementado. Para evaluar los sistemas de gestión de la seguridad de la información utilizamos la norma ISO/IEC 27001, la cual contempla la evaluación de los siguientes aspectos: La Organización de la Seguridad de la Información, Seguridad en la Gestión de los Activos, Seguridad en los archivos de RR.HH, Seguridad Física y Ambiental de la infraestructura y por último la Gestión de las Comunicaciones y Operaciones.

Durante la evaluación de los aspectos anteriormente mencionados, la norma ISO/ 27001 identificara medias de control, las cuales se consideran esenciales para mejorar la práctica de los sistemas de gestión de la seguridad de la información y son los siguientes: Documentación de la política de seguridad de la información, Adjudicación de responsabilidades para la seguridad de la información, Formación, entrenamiento y actualización propuesto por la gerencia de TIC para el personal del departamento de TIC, Relación de las incidencias de seguridad, Gestión de la continuidad de las operaciones en la organización, Derechos de la propiedad intelectual, Salvaguarda de todos los registros de la organización y Protección de los datos sobre la información personal. En estos últimos diez años, aproximadamente, se han venido desarrollando diversas metodologías para la evaluación de las infraestructuras de TIC con respecto a la seguridad de la información al interior de las organizaciones modernas y para revisar el estado que guarda la seguridad de la información en esa organización. Frente a las problemáticas de la seguridad de la información interna de los sistemas de gestión; en la actualidad se debe hacer una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de la organización en cuanto a la seguridad de la información que maneja.

Cada organización es diferente, para lo cual utiliza distintos tipos o categorías de evaluaciones de seguridad de la información para validar el nivel de seguridad de sus recursos de red, las cuales ayudan a describir las amenazas e identificar las vulnerabilidades a las cuales la seguridad de los sistemas de TI de las organizaciones se encuentran sometidos. Entre estas categorías incluyen auditorías de seguridad, evaluaciones de vulnerabilidades, hacking ético y pruebas de penetración.

Los dispositivos de las TICs son instrumentos que estructuran grandes cantidades de información, la cual puede ser confidencial para la organización moderna y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta; además pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de las actividades de procesamiento electrónico de la información y generar grandes pérdidas económicas a la organización. Esta información puede ser de suma importancia, y al no contar con ella en el momento preciso puede provocar retrasos sumamente costosos y perjudiciales para la organización. Al evaluar los sistemas de información, se debe verificar y constatar lo siguiente:

- Que no se tengan copias “piratas” o que, al conectarnos en red con otras computadoras y dispositivos, no exista la posibilidad de transmisión de virus.
- Que se hayan implementado procesos físicos y lógicos para la protección del hardware, así como a las instalaciones de ingreso al área o departamento de TIC. Contemplando las situaciones de incendios, sabotajes, robos, catástrofes naturales, entre otros.
- Implementación de dispositivos para garantizar la seguridad lógica del software, la protección de los datos e información, procesos y programas, así como la restricción de usuarios no autorizados al acceso de la información.

En Gandalf Comunicaciones, C.A., el gerente departamento de TIC, junto con su equipo de trabajo, se encuentran en todo momento evaluando los sistemas de gestión de seguridad de la información de la empresa e incluso innovando con las nuevas tecnologías que se adecuen más a las necesidades de la organización, factor de mucha importancia y que el gerente se toma muy seriamente, debido a que es una organización que presta un servicio, el cual cada día con un mundo cada vez más globalizado, se ha convertido en un servicio necesario, en el que se le presenta bastante atención para poder brindar todas las garantías de seguridad de la información a los empleados, clientes y proveedores.

Es muy importante elegir un modelo de evaluación para los sistemas de gestión de seguridad de la información en las infraestructuras de TIC, para así conocer los peligros potenciales y **de qué forma dichos riesgos, amenazas y vulnerabilidades pueden afectar a la información confidencial y los sistemas de información** de la organización. Posteriormente, también hay que evaluar **la probabilidad de que ese peligro potencial se convierta en una realidad.** Es importante que, a partir de ese modelo de evaluación, tanto la gerencia del departamento de TIC, como la organización sean capaces de:

- ✓ Evaluar los riesgos relacionados con confidencialidad, integridad y disponibilidad.
- ✓ Determinar criterios que definan qué se entiende por riesgo aceptable.
- ✓ Estimar los diferentes niveles de riesgo y sus consecuencias asociadas.
- ✓ Determinar si los riesgos son aceptables o si requieren una acción siguiendo criterios de aceptabilidad previamente definidos.
- ✓ Valorar los costos de la eliminación de riesgos.

4.7 La necesidad vital de las organizaciones de proteger la información y asegurarse que sea precisa, disponible, confiable, autentica e integra.

La necesidad de proteger la información para Hernández, F. (2011) es:

> La información, los procesos, los diversos sistemas y las redes que la soportan activos importantes del negocio. La definición, el logro, el mantenimiento y la mejora de la seguridad de la información pueden ser esenciales para mantener la competitividad, el flujo de caja, la rentabilidad, el cumplimiento legal y la imagen comercial. (P. 44)

Para las organizaciones modernas de hoy día que pertenecen al sector público y privado, sufren constantemente amenazas y ataques de seguridad a sus sistemas de información, los cuales provienen de distintos orígenes como espionaje electrónico, fraude electrónico, negación del servicio, entre otros aspectos, por lo que estos ciber ataques como se conocen a nivel mundial se han vuelto cada vez más sofisticados y ésta es la necesidad de las organizaciones de mantener e implementar sistemas de gestión en la seguridad de la información, para que la misma siempre sea precisa, confiable, autentica, integra y se encuentre disponible para los usuarios que trabajan dentro de la organización y para los clientes a los cuales se les brinda un servicio, ya que la misma depende del éxito de la organización a nivel operacional y comercial.

Proteger la información es proteger el funcionamiento adecuado de la organización, sobre todo en casos de fallo en la transmisión o almacenamiento de datos. De igual manera, la protección de la información permite evitar pérdidas financieras provocadas por la desaparición de archivos, bases de datos, balances financieros, entre otros. Una Política de Seguridad debe ser la guía a seguir por la organización para asegurar sus activos, debe tener unos objetivos básicos que fundamentalmente serán garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información, así como también debe cubrir, en la medida de sus posibilidades, con todos los aspectos que pudieran poner en peligro la información, sin olvidar las medidas de seguridad física.

Para que la información procesada por un sistema de información sea valiosa y tenga relevancia en los procesos de toma de decisiones, tanto en niveles operativos como gerenciales, debe ser precisa, autentica, confiable, integra y estar disponible en todo momento, porque para una organización, el costo de tomar decisiones sobre la base de información incorrecta, incompleta o que no presente alguna de los aspectos mencionados anteriormente, puede representar un gasto de mucho dinero para la organización. La necesidad de proteger y asegurar la información, así como también sea oportuna y confiable constituye una herramienta robusta, esencial e importante a nivel gerencial dentro de la organización. El conocimiento completo de la situación en la cual se trabaja, permite identificar fortalezas, debilidades, vulnerabilidades y amenazas que permiten enfrentar desafíos, así como analizar los diferentes escenarios o caminos que se pueden tomar; en esto radica la importancia de contar con información real, precisa, confiable, autentica y disponible en el momento en que se requieren, de lo contrario no son útiles en los procesos de toma de decisiones gerenciales.

En Gandalf Comunicaciones los directivos de la empresa y la gerencia del departamento de TIC se encuentran constantemente verificando el buen funcionamiento de la implementación de las políticas a los sistemas de gestión de seguridad de la información, porque la empresa, se preocupa por brindar la mayor seguridad a los sistemas de información en la conectividad de los dispositivos internos de la empresa y de la transmisión de la información a los clientes, como se mencionó anteriormente, Gandalf Comunicaciones ofrece servicios de internet por medios inalámbricos, por tal motivo para la empresa es muy importante mantener la seguridad de la información en sus enlaces de servicios de internet inalámbricos. En empresas que prestan un servicio, como lo es en este caso que es un servicio de telecomunicaciones, es muy importante mantener la seguridad de la información y que la misma siempre esté disponible, sea confiable, integra y autentica para los usuarios, clientes y proveedores; y la misma se convierte en una ventaja competitiva en el mercado frente a otros proveedores como la competencia.

CAPITULO V

LA GERENCIA Y LAS HERRAMIENTAS TECNOLÓGICAS PARA EL CONTROL Y PREVENCIÓN DE LOS RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN

5.1 La aplicación e implementación de estrategias gerenciales que son fundamentales para la solución de los problemas teóricos relacionados a la información.

Mediante las estrategias gerenciales se pueden equiparar las fortalezas y debilidades; se construyen prioridades, se diseñan planes, se alinean y utilizan los recursos de manera eficiente, se coordinan, ejecutan y examinan actividades, se determinan las operaciones, se formulan y evalúan los proyectos. La planificación es un proceso gerencial, de naturaleza racional, diseñada para promover resultados esperados. La estrategia gerencial tiende a ser prescriptiva, normativa, a convertirse en algo administrativo, predecible, cuantificable y controlable, por ende muy importante dentro de las organizaciones modernas.

La gerencia en las organizaciones modernas demanda asumir nuevos retos y los grandes cambios que suceden en el entorno, hacen que se asuman nuevas estrategias y modelos de gerencia. Actualmente existe lo que denominamos la globalización tecnológica, la cual abre caminos a los nuevos avances tecnológicos, la innovación se puede conocer y adquirir en un corto tiempo, gracias a las telecomunicaciones y sistemas de tecnología de la información, cada día las distancias se acortan y se forma una red de naciones interconectadas globalmente, los recursos que proporcionan la globalización son: internet, telefonía móvil a alta velocidad como 4G, VoIP, televisión en alta definición HD, entre otros, de esta manera las barreras de la distancia se vencen para estar cada día en un mundo cada vez mas conectado y comunicado. Las estrategias gerenciales son una búsqueda considerada por un plan de acción que le permita a la organización desarrollar una ventaja competitiva en el mercado, y la multiplique. Aplicar estrategias gerenciales en una organización, y luego implementarlas, es un proceso dinámico, complejo, continuo e integrado, que requiere de mucha evaluación y ajustes.

Realizar, aplicar e implementar de estrategias gerenciales en los Sistemas de Información dentro de cualquier organización moderna, tiene simplemente la finalidad de asegurar el ajuste entre los objetivos estratégicos de la misma y la información necesaria para soportar dichos grandes objetivos. Como consecuencia se genera una planificación de sistemas que cubren a toda la organización por lo que se debe tener en cuenta una serie de conceptos, en cuanto a planificación de estrategias. En carácter similar a la Estrategia del Negocio, la Estrategia de Tecnologías de Información, como solución a los problemas de la misma, es el resultado de una serie de decisiones gerenciales sobre su alcance, competencias y manejo, como lo es: El Alcance de la Tecnología de la información está asociado con decisiones gerenciales que determinan el tipo de tecnologías que se utilizarán (tecnologías orientadas a objetos, arquitecturas cliente/servidor, manejo de imágenes, robótica, multimedia, entre otros.), Las Competencias Sistémicas identifican las tipologías y fortalezas de las tecnologías de la información que serán críticas para la creación y extensión de estrategias gerenciales (disponibilidad, accesibilidad, confiabilidad, integridad y desempeño), Las decisiones gerenciales con respecto manejo de la Tecnología de la Información permiten también determinar el alcance de la propiedad sobre la tecnología, así como posibilidades de alianzas o sociedades.

Otro componente que se encuentra en las estrategias gerenciales de las TIC, tiene mucho que ver con su Infraestructura y Procesos de Tecnología, los cuales tienen tres manuales interrelacionados: La Infraestructura Tecnológica de la organización, en donde se especifican todas las prioridades y políticas que permiten la integración de aplicaciones tecnológicas, Los Métodos relacionados con el desarrollo de aplicaciones tecnológicas, con su administración y con la operación de ellas; y por último Las Destrezas, experiencias, competencias, compromisos, valores y normas del personal encargado de entregar productos y servicios de tecnología de excelente calidad para los usuarios, clientes y proveedores.

K. Laudon y J. Laudon en su libro *"Sistemas de Información Gerencial"*, explican

> Hay cuatro estrategias genéricas, cada una de las cuales se habilita a menudo mediante el uso de tecnología y sistemas de información: liderazgo de bajo costo, diferenciación de productos, enfoque en nichos de mercado y fortalecimiento de la intimidad con los clientes y proveedores. (P. 96).

Algunas organizaciones modernas, ya sean del sector público o privado, se enfocan en una de estas cuatro estrategias o se enfocan en las cuatro, dependiendo de cuál les arroje mejores resultados de acuerdo a sus necesidades, en la organización Gandalf Comunicaciones, la misma se he enfocado en el fortalecimiento de la intimidad con los clientes y proveedores, en el que se preocupa por mantener una relación de constante atención con los clientes, asegurándose siempre de atender los requerimientos de los clientes y presentarles la solución ante fallas del servicio lo más rápido posible, ya que esto los clientes valoran mucho estas acciones de la organización y sienten que la misma se preocupa por brindarles un buena atención y un excelente servicio.

5.2 Las Tecnologías de la Información y Comunicaciones como una de las principales e importantes herramientas para garantizar las operaciones, la gerencia y el servicio a los usuarios en las organizaciones.

Las Tecnologías de la Información y las Comunicaciones (TICs), en la actualidad son una herramienta gerencial de gran importancia, entrega un aporte de manera positiva al perfeccionamiento y la aptitud de las organizaciones modernas. Las TICs incrementan el importe de las actividades operacionales y a nivel gerencial, así como también permite a las organizaciones conseguir mejoras competitivas, permanecer en el mercado y centrarse en su negocio. Para que la implementación de nueva tecnología proyecte resultados positivos hay que cumplir varios requerimientos: como tener un conocimiento profundo de los procesos de la organización, planificar detalladamente las necesidades de tecnología de la información e incorporar los sistemas tecnológicos gradualmente, empezando por los más básicos.

Un aspecto importante que se debe considerar es que antes de agregar un nuevo dispositivo tecnológico en la organización, el gerente debe estar al tanto de las operaciones de la organización debido a que se ha determinado que muchas de las veces, el fracaso no es debido al software ni a los sistemas, sino al simple hecho de que las personas no poseen suficientes conocimientos sobre sus propia empresas o sus procesos empresariales. Las Tecnologías de la Información y la Comunicación han reformado nuestra manera de trabajar y gestionar recursos, por lo que se han convertido en un mecanismo fundamental para hacer que el trabajo sea más beneficioso: moviendo las comunicaciones, apoyando el trabajo en equipo, realizando análisis estratégicos, y promocionando sus productos en el mercado. El buen uso de las TIC permite a las organizaciones modernas de la actualidad producir más cantidad de productos y servicios, más rápido, de mejor calidad, y en menos tiempo y le ayudan a la competitividad.

La automatización de las Tecnologías de la Información y Comunicaciones en la gerencia de las organizaciones tiene los siguientes objetivos:

- Profesionalizar la gerencia en las organizaciones.
- Dar mayor transparencia a la información proporcionada por la organización moderna.
- Optimizar los patrimonios disponibles para una gerencia más eficiente y eficaz.
- Implementar prácticas gerenciales más modernas y eficientes que permitan la solución de problemas relacionados a la seguridad de la información.

En los últimos tiempos las Tecnologías de la Información y Comunicación han venido evolucionando de forma bastante significativa, la cual se ha visto motivada a una gran variedad de factores de los que se pueden mencionar los grandes desarrollos tecnológicos que permiten que los gerentes puedan manejar la información en tiempo real, lo que a su vez permite ser mucho más profesional a la hora de tomar decisiones en los distintos métodos productivos dentro de las organizaciones modernas.

Ramón Acosta, profesor de EADA (Operaciones y Sistemas de la Información) en el articulo web titulado ***"Aplicaciones de las tics en las empresas: Las Tecnologías de la Información y la Comunicación (TIC) están presentes en muchos y vanados campos de la actividad humana: medicina, ingeniería, industria, ámbito científico, en el mundo artístico y por supuesto, en la empresa en general"*** *menciona lo siguiente:*

> Podemos decir que las TIC se han convertido en imprescindibles para las empresas, por muchas razones. Son herramientas para mejorar y optimizar procesos, para agilizar operaciones y las actividades empresariales, ya sea para poder capturar los datos de una manera rápida y segura (aplicación operativa) o para poder procesar estos datos, y convertirlos en información de análisis (aplicación táctica) y por tanto, ayudar a la toma de decisiones (aplicación estratégica).

http://blogs.eada.edu/2012/07/05/tecnologias-informacion-en-empresa

En los países donde sus industrias se encuentran bastante desarrolladas, los mismos obtienen buenos resultados en sus actividades económicas debido a la aplicación de las Tecnologías de Información y Comunicación (TIC), las cuales como se afirma en el artículo anterior, son herramientas que manifiestan el apoyo los distintos procesos económicos, políticos y sociales de cualquier sociedad que haga uso de ellas, tomando en consideración que las mismas, no sólo se restringen al área de la información y de la comunicación, sino que aportan con otros patrocinios que requieren los ciudadanos. Como ejemplo de lo mencionado anteriormente en Venezuela en estos últimos años las organizaciones modernas públicas y privadas han informado de un gran avance en el desarrollo sobre el uso de las TICs en la vida cotidiana, por lo que la utilización de las Tecnologías Información y Comunicación inmerso en la globalización ha fijado el inicio para el mejoramiento de los métodos gerenciales, ocasionando grandes cambios en la organización moderna. Esta transformación tecnológica ha impactado en varios países suramericanos, demostrándose que la utilización de las TIC genera importantes ventajas competitivas comercialmente.

En el entorno gerencial es incuestionable el uso de las TIC como herramientas electrónicas de comunicación, como por ejemplo celulares, computadores, sistemas de información automatizados, software, internet, correos electrónicos, videoconferencias, entre otros, tienen el objetivo de agilizar las actividades operacionales de la organización en cada uno de sus departamentos y se obtiene como resultado un incremento de producción en los servicios y del volumen de información, lo que ha generado mayor complejidad en el ejercicio de la gerencia. Independientemente de las limitaciones de la infraestructura, socioeconómicas y culturales que se presenten, se ha comenzado a iniciar el uso de las TIC en los métodos gerenciales de las organizaciones modernas, por lo que los profesionales universitarios y los que se desempeñen como gerentes deben prepararse cada vez más para asumir nuevos retos y desafíos en una era de constante revolución tecnológica, con el objetivo de realizar cambios y mejoras en las organizaciones, considerando las TIC como herramientas estratégicas gerenciales que serán aplicadas para cumplir con los objetivos planteados y lograr mayor impactos en los resultados.

5.3 Las políticas de seguridad de la información como herramientas de la gerencia para administrar y controlar eficientemente la gestión de un sistema de información.

Las políticas de seguridad de la información representan una importante herramienta que servirá para garantizar el buen funcionamiento de los métodos gerenciales, para contribuir con su eficiencia, optimizar los sistemas de información internos y garantizar la calidad en la gestión, con el objetivo de asegurar la información en las organizaciones. Dichas políticas de seguridad tienen como objetivo los lineamientos de compromiso en el plano de la Tecnología de la Información y las Comunicaciones, a los usuarios en la utilización de la misma, a fin de que se cumplan con las políticas de una manera clara, precisa, transparente y lo más cercano a la realidad, ocasionando así una progresión de servicios de hechos y formas de comunicación dentro de la organización, así como también busca identificar y minimizar los riesgos, amenazas y vulnerabilidades a los que se muestra la información en sus procesos de actividades comerciales, al tiempo que implanta una cultura de seguridad en los usuarios, se ve una reducción de costos operativos y financieros a la vez que se certifica el cumplimiento de las obligaciones contractuales, regulatorios y legales vigentes en dichas políticas de seguridad.

La alta gerencia de Gandalf Comunicaciones, evidencia su compromiso con la seguridad de la información a través de la herramienta como la definición de políticas de seguridad e implementación de un Sistema de Gestión de Seguridad de la Información, el cual respalda a mantener la integridad, confidencialidad, autenticidad y disponibilidad de los activos de la información, lo cual permitirá administrar y controlar eficientemente la información. Las políticas de información que implementa la gerencia del departamento de tecnologías de la información y comunicaciones en Gandalf Comunicaciones, es un compromiso por brindar un servicio de excelente calidad para nuestros clientes, proveedores y personal, por éste motivo las políticas de seguridad de la información son una herramienta y guía para la constante búsqueda de que como organización se le quiere entregar a nuestros usuarios y trabajadores.

La gerencia del departamento de tecnologías de la información y comunicaciones de Gandalf Comunicaciones, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos y amenazas, la valoración de la disponibilidad y confidencialidad de su información y aún más la de sus clientes. Así, Gandalf Comunicaciones se compromete a desarrollar, implantar, mantener y mejorar continuamente su Sistema de Gestión de Seguridad de la Información (SGSI) con el objetivo de la mejora continua en la forma en que prestamos nuestros servicios y en la forma en que tratamos la información de nuestros clientes. Por tal motivo, es política de la información en Gandalf Comunicaciones lo siguiente:

- Se establece anualmente objetivos con relación a la Seguridad de la Información.
- Cumplir con los requisitos legales, contractuales y del negocio.
- Realizar actividades de formación y concienciación en materia de los procesos de Seguridad de la Información para todo el personal.
- Desarrollar un proceso de análisis, gestión y tratamiento del riesgo sobre los activos de información.
- Se establecen los objetivos de control y los controles correspondientes para mitigar los riesgos detectados y posibles amenazas.
- Se establece la responsabilidad de los empleados en relación a: Reportar las violaciones a la seguridad; preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política, y cumplir las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.

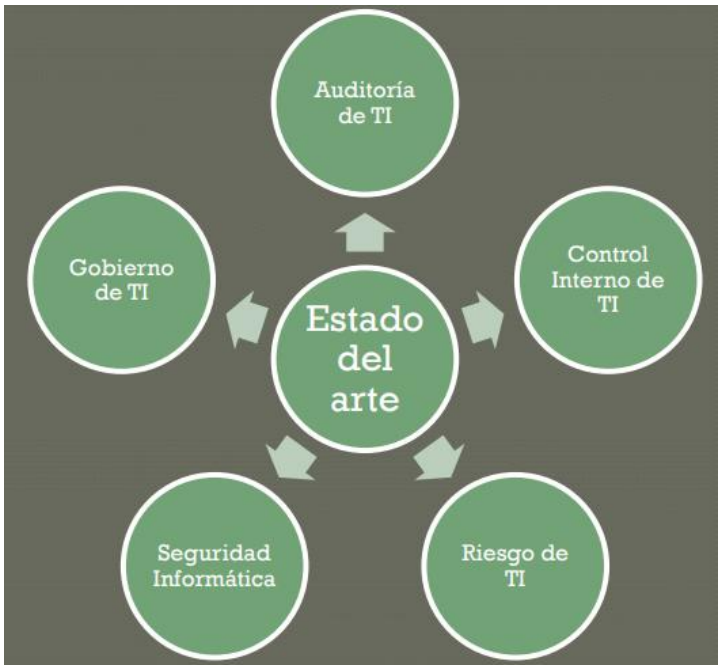
Laudon J. y Laudon K. en su libro titulado *"Sistemas de Información Gerencial"*, Capitulo 6, menciona la importancia del establecimiento de una política de información para la seguridad de toda la información en las organizaciones pequeñas, medianas y grandes modernas de la actualidad y citan lo siguiente:

> Toda empresa, ya sea grande o pequeña, necesita una política de información. Los datos de su empresa son un recurso importante, por lo que no es conveniente que las personas hagan lo que quieran con ellos. Necesita tener reglas sobre la forma en que se van a organizar y mantener los datos, y quién tiene permitido verlos o modificarlos.
> Una política de información es la que especifica las reglas de la organización para compartir, diseminar, adquirir, estandarizar, clasificar e inventariar la información.
> La política de información establece procedimientos y rendiciones de cuentas específicos, identifica qué usuarios y unidades organizacionales pueden compartir información, en dónde distribuirla y quién es responsable de actualizarla y mantenerla.
> Tal vez escuche que se utiliza el término gobernanza de datos para describir muchas de estas actividades. La gobernanza de datos es promovida por IBM y se encarga de las políticas y procedimientos para administrar la disponibilidad, utilidad, integridad y seguridad de los datos empleados en una empresa, con un énfasis especial en promover la privacidad, seguridad, calidad de los datos y el cumplimiento con las regulaciones gubernamentales. (P.230)

Para Gandalf Comunicaciones, la implementación y gestión de las políticas de seguridad de la información se han convertido en una herramienta fundamental e importante en la gerencia del departamento de tecnologías de la información y comunicaciones debido a que gracias a éstas políticas de seguridad han permitido la evaluación y posterior calificación de riesgos, amenazas y vulnerabilidades en los sistemas de información, así como también a identificar los objetivos de seguridad y componentes para lograra cada uno de los objetivos planteados.

5.4 El estado del arte en materia de gestión de seguridad de la información para las organizaciones modernas.

El estado del arte en el entorno de las operaciones en las organizaciones modernas, se trata del desarrollo y utilización de la última tecnología de punta que implementan las organizaciones modernas actualmente, para la fabricación de sus productos y mejoras en la calidad de los servicios que brindan a sus clientes y proveedores. El estado del arte lo aprovecha el gerente de tecnologías de la información y comunicaciones para tener una referencia ante una actitud crítica frente a lo que se ha realizado y lo que faltaría por realizar para mejorar la gestión de seguridad en las tecnologías de la información y comunicaciones.



Principales objetivos del Estado del Arte en la Gestión de la Seguridad de la Información

Figura 3

Los dispositivos y componentes de seguridad de la información, así como sus infraestructuras se deben ajustar para soportar los requerimientos de las actividades comerciales emergentes a nivel digital, y al mismo tiempo hacer frente a la situación de amenaza, riesgo y vulnerabilidad que cada vez son más avanzadas y frecuentes en sus ataques. Los gerentes y profesionales en seguridad de la información y comunicaciones deben comprometerse plenamente con las últimas tendencias de la tecnología para que permitan definir, alcanzar y mantener proyectos, políticas de seguridad y gestión de riesgos eficaces que permitan al mismo tiempo las oportunidades de negocio digital y gestionar los riesgos, amenazas y vulnerabilidades de los sistemas de información.

Los últimos 10 y más resientes avances tecnológicos identificados por analistas en materia de seguridad de la información son los siguientes:

- Agentes de Seguridad de Acceso a la Nube
- Detección Endpoint y Respuesta EDR
- Enfoques sin Firma para la Prevención Endpoint
- Análisis del Comportamiento del Usuario y de las Entidades EUBA
- Micro segmentación y Flujo de Visibilidad
- Pruebas de Seguridad para DevOps
- Soluciones de Orquestación del Centro de Operaciones de Seguridad dirigidas por Inteligencia SOC.
- Navegador Remoto
- Fraudes
- Servicios de Confianza Generalizados.

Determinados estudios han revelado que las organizaciones modernas aumenten en un gran porcentaje la adopción a nuevas tecnologías, que les permitan prepararse para la nueva era digital. Por este motivo CISCO presenta nuevas tecnologías que permiten a las organizaciones modernas virtualizar y asegurar sus sistemas de información, a través de su Digital Network Arquitecture, la cual le permite a CISCO detectar de manera más eficaz y rápida cualquier tipo de amenaza en materia de seguridad de la información. Las nuevas tecnologías que presenta CISCO en su publicación son las siguientes:

Visibilidad y control: Cisco Identity Services Engine (ISE) proporciona visibilidad y control de usuarios y dispositivos conectados a la red. ISE 2.2 ofrece una mayor visibilidad de las aplicaciones utilizadas en los terminales, incluyendo la detección de comportamiento anómalo. También proporciona un control más granular con la capacidad de definir sets de políticas "DEFCON" que permiten a los clientes ampliar su respuesta frente a amenazas que se reproducen continuamente.

Segmentación definida mediante software: Cisco TrustSec proporciona segmentación definida mediante software para aislar los ataques y restringir el movimiento de amenazas en la red. Esta segmentación dinámica consigue que los cambios en las políticas de seguridad se realicen un 98 por ciento más rápido frente a los métodos tradicionales, reduciendo un 80 por ciento los esfuerzos operativos. TrustSec 6.1 está ahora disponible a través de todo el portfolio de networking empresarial de Cisco y se integra con Cisco ACI. Con estas novedades, TrustSec permite la segmentación dinámica en cualquier lugar de la red, desde el extremo hasta el data center y el Cloud.

http://www.muycomputerpro.com/2017/02/26/cisco-virtualizacion-seguridad

5.5 La confidencialidad, integridad y disponibilidad como factores indispensables en la seguridad de la información de las organizaciones modernas.

Proteger la confiabilidad, integridad y disponibilidad de la información es factor importante e indispensable para la seguridad y gestión de los sistemas de información de cualquier organización actual, tal es el caso de Gandalf Comunicaciones que al pertenecer al sector de las telecomunicaciones y proveer servicios de internet, se encuentra siempre, la gerencia del departamento de TIC y todo su personal en la búsqueda de establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, de sus clientes, usuarios y proveedores a los cuales Gandalf Comunicaciones les ofrece servicios de internet.

Las organizaciones que obtienen la certificación de la norma ISO 27001, la cual promueve la confiabilidad, integridad y disponibilidad de la información, garantizan importantes aspectos en la gestión de los sistemas de seguridad de la información, como el personal autorizado para acceder a la información, que los procesos de la información sean los más precisos; y que solamente los usuarios o personal autorizado tengan acceso y a los activos en el instante que lo requieran y contribuye a fomentar las actividades de protección de la información en las organizaciones modernas, mejorando así su imagen y generando confianza frente a sus proveedores y clientes. Gran cantidad de las organizaciones modernas de la actualidad, se encuentran realizando los trámites necesarios para poder certificarse nacional e internacionalmente, esto con el objetivo de que la gerencia de los departamentos de TIC en las organizaciones les están dando mayor valor a mantener la confiabilidad, integridad y disponibilidad de la información por motivo de los actuales y recientes ataques a la información de empresas internacionales, los cuales los secuestran la información de los usuarios y posteriormente solicitan un pago de una alta suma de dinero a cambio de regresar dicha información a sus dueños legítimos, por esta razón las organizaciones ya están certificadas debido a que a nivel comercial les brinda mayor confianza a sus clientes y proveedores, en lo que respecta al aseguramiento de la información.

La empresa Proconsi recientemente mostro su nuevo y moderno Centro de Operaciones de Seguridad (SOC) el cual va enfocado en un principio a las pequeñas y medianas organizaciones con el objetivo de brindarles un control y monitoreo sobre posibles ataques o amenazas que pueden sufrir los sistemas de información en estas organizaciones e incluso el SOC también se encuentra diseñado para alertar al personal y gerentes de ciberseguridad en los departamentos de TIC en dichas organizaciones, de posibles vulnerabilidades que se encuentren presentando sus sistemas de gestión de seguridad de la información, es decir que se trata de un servicio que aportes soluciones para mantener la confiabilidad, integridad y disponibilidad de los sistemas de información.

El director del departamento de Sistemas y Ciberseguridad de Proconsi, Luis Angel Martínez, explico el objetivo principal y función que tiene el Centro de Operaciones de Seguridad, lo siguiente:

> Monitorizar la ciberseguridad en general, saber qué está ocurriendo por el mundo. Por ciberseguridad se entiende no solo cuando hablamos de ciberataque, sino que se pretende es buscar la integridad, la disponibilidad y la confidencialidad de la información, añadió el director de este departamento, quien resaltó que se intenta adelantarse a los posibles problemas que pueden tener los discos duros y en el hardware en general. El grado de madurez de implantación es muy bajo, y claro, los 'ransomware' van haciendo verdaderos estragos porque las empresas no están preparadas y hay que darse cuenta de que las ciberamenazas afectan a todas, desde el pequeño autónomo hasta la gran empresa.

http://www.lanuevacronica.com/proconsi-crea-un-departamento-para-detectar-ciberataques-contra-pymes

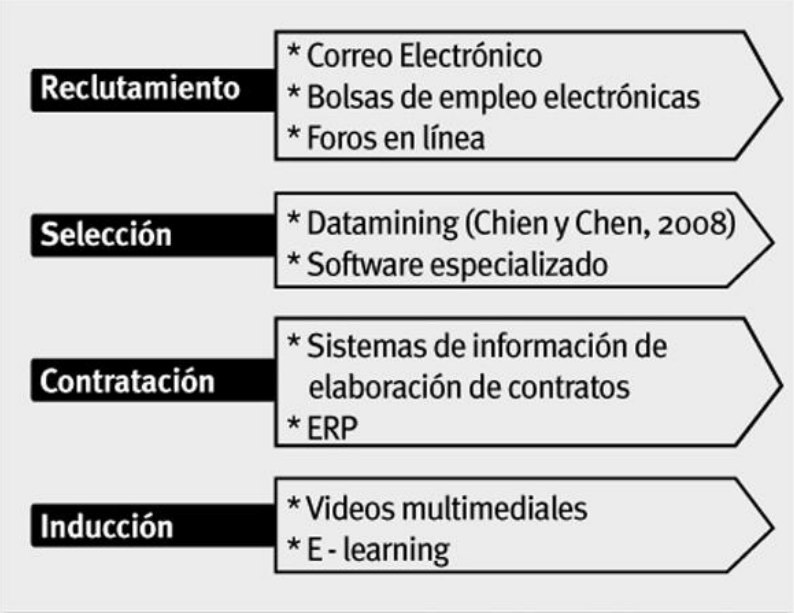
Junto a los principios o factores fundamentales en la seguridad de los sistemas de información, como lo son la confiabilidad, integridad y disponibilidad de la información, también hay que destacar otro factor fundamental y muy reciente en la seguridad de los, el cual es la Autenticación o Autenticidad, que permite controlar el acceso a la información con la verificación de cada usuario. Con lo anteriormente explicado se puede observar cómo se relacionan los diferentes factores en la seguridad de la información que son indispensables para las organizaciones modernas de la actualidad. De esta forma, la disponibilidad de la información pasa a ser en el primer componente de la seguridad, cuando existe éste, se puede situar la confiabilidad de la información como segundo componente, la cual es necesaria para poder conseguir la integridad de la información, pero a su vez también es necesaria para poder lograr la autenticación de la información. El elevado nivel de conectividad de personas en los sistemas de información que encontramos, hoy día, no sólo proporciona acceso a gran cantidad y variedad de fuentes de información de forma cada vez más rápida, sino que origina un aumento de los ataques a los sistemas de información.

En éste sentido y como anteriormente se ha mencionado, la confiabilidad, integridad y disponibilidad se han convertido en los tres principales factores de la seguridad en los sistemas de información, seguidos claro de la autenticidad como ultimo y mas reciente factor para la gerencia en los departamentos de TIC en cada una de las organizaciones modernas. En el departamento de TIC en Gandalf Comunicaciones, la gerencia de dicho departamento, esta consiente de la importancia que representan los factores de la confiabilidad, integridad y disponibilidad de la información, debidos a que son totalmente indispensables ya que es una organización de servicios que opera en el sector de las telecomunicaciones siendo un ISP, lo que obliga al gerente de TIC a cumplir con los factores fundamentales para poder mantener un servicio estable y sin fallas, lo podría generar grandes pérdidas económicas para la organización e incluso una mala reputación a nivel comercial frente a la futuros y nuevos clientes.

5.6 Las TICs como una de las herramientas más significativas que tienen actualmente los gerentes para salvaguardar los activos de la organización.

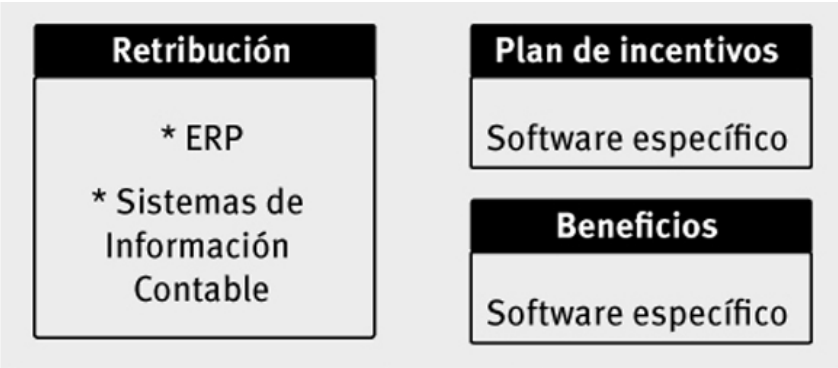
Las TICs en la gerencia de los departamentos de tecnologías de la información y comunicaciones en las organizaciones, se han convertido con el pasar de los años en una herramienta de gran poder interactivo en las distintas ramas del conocimiento humano. También las TICs en la actualidad constituyen un instrumento significativo para los gerentes que laboran en estos departamentos tecnológicos de las grandes y modernas organizaciones de la actualidad, debido a que gracias a la utilización de estas valiosas herramientas las cuales les ha permitido a los gerentes un importante y significativo ahorro de tiempo y recursos, al poder facilitar y acelerar los métodos de gestión, la toma de decisiones, ayudan a centrarse en las actividades u operaciones que agreguen valor y agilizar el contacto con los clientes y proveedores.

A continuación se mostraran algunas herramientas de las TICs que se utilizan actualmente en la gerencia de las organizaciones modernas:



Herramientas de las TICs para los Métodos de Ingreso de Personal

Figura 4

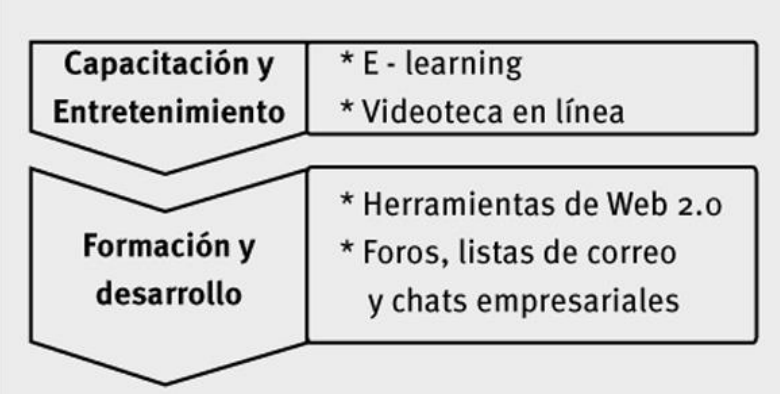


Herramientas de las TICs para los Métodos de Compensación
Figura 5

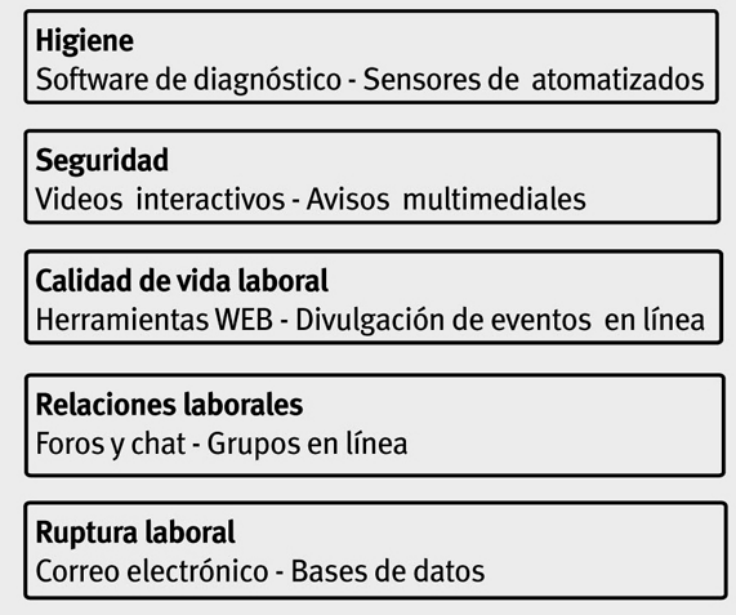
Entre el software específico para el soporte de los métodos de compensación se mencionan los siguientes:

- ✓ Softland Solucion Corporativa
- ✓ Microsoft Dynamics AX
- ✓ Factory Visual
- ✓ Midasoft
- ✓ Novasoft
- ✓ SAP

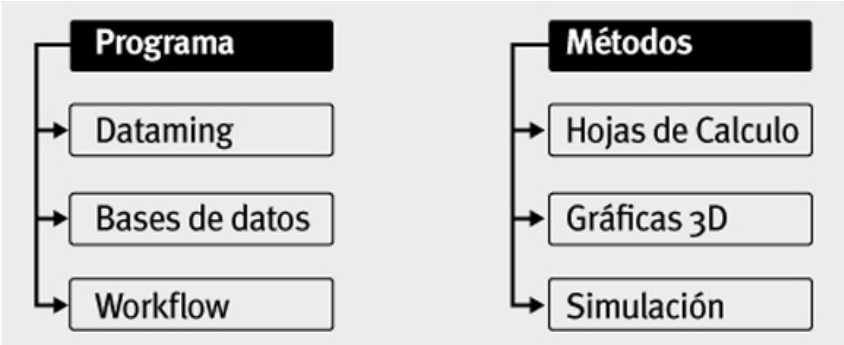
Solo por mencionar algún pero existen muchos software utilizados a nivel gerencial en las grandes organizaciones modernas de la actualidad y se han convertido en una herramienta muy utilizada.



Herramientas de las TICs para los Métodos de Adquisición de Conocimientos
Figura 6



Herramientas de las TICs para los Métodos con respecto a las Condiciones Laborales
Figura 7



Herramientas de las TICs para los Métodos de Evaluación
Figura 8

En Gandalf Comunicaciones, la gerencia ha aprovechado extraer al máximo provecho el uso adecuado de todas sus tecnologías actuales, es decir, gracias a las herramientas que han brindado las TICs, han identificado las ventajas para la correcta utilización de las tecnologías y su desarrollo en los métodos operacionales de la organización. Las TICs como herramienta gerencial para Gandalf Comunicaciones, ha constituido un instrumento tecnológico que le ha permitido mejorar el manejo de la información, por lo que se convierte en una herramienta indispensable y estratégica para así obtener ventajas competitivas en el mercado.

5.7 Similitudes y diferencias entre la seguridad de la información y la seguridad informática.

Para poder mencionar las similitudes y diferencias entre la seguridad de la información y la seguridad informática debemos saber cual es la definición de cada una, que aunque sus nombres sean casi iguales, realmente ambos conceptos no son lo mismo, sin embargo ambas definiciones en la gerencia y tecnologías de la información, se encuentran muy estrechamente ligados entre sí.

La Seguridad de la Información representa la ***confidencialidad***, la ***integridad*** y la ***disponibilidad*** de la información y los datos más importantes para la organización, como por ejemplo para Gandalf Comunicaciones, es la estabilidad del servicio de internet que le brinda a sus clientes y proveedores, el cual como ya sabemos, el internet se ha convertido en una tecnología de la información y comunicaciones cada vez más necesaria para las operaciones comerciales a nivel digital de las de las organizaciones modernas. La **Seguridad Informática** en cambio se fundamenta en asegurar que los patrimonios del sistema de información como los bienes activos (Computadores, Switches, Routers, Servidores, entre otros) y programas de software de una organización, sean manipulados de manera considerada, que para el caso de Gandalf Comunicaciones pues viene siendo todo su infraestructura tecnológica física. Como conclusión a estas dos definiciones queda claro que mientras la seguridad de la información constituye toda la información que mantenga ya sea en físico, electrónico o en cualquier otro estado en el que se encuentre y la seguridad informática se encamina en la protección de infraestructura tecnológica de la organización como (redes de comunicaciones, sistemas operativos, ordenadores, entre otros).

Seguridad Informática Vs Seguridad de la Información

Figura 9

Helena Rojas Valduciel en su artículo titulado *"Seguridad de la Información, Seguridad Informática y Ciberseguridad: ¿Son sinónimos?,* publicado el 20/04/2016, realiza un análisis sobre estos conceptos donde menciona las diferencias que se presentan entre la seguridad de la información y la seguridad informática en el que menciona lo siguiente:

> La **seguridad de la información** se orienta a proteger los activos de información sin importar su forma o estado, valiéndose de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, para la aplicación y gestión de las medidas de seguridad apropiadas en cada caso. Por tanto, abarca tanto a la seguridad informática, como la seguridad computacional y la ciberseguridad.
> La **seguridad informática**, se limita a proteger activos de información en formato digital y los sistemas informáticos que los procesan y almacenan, indistintamente si están interconectados o no.

https://infobyteabyte.wordpress.com/2016/04/20/seguridad-de-la-informacion-seguridad-informatica-y-ciberseguridad-son-sinonimos/

Ahora bien en cuanto a la similitud entre la seguridad de la información y la seguridad informática se menciona que ambas aéreas de las tecnologías de la información y comunicaciones tienen algo en común y es la protección de la información que representa un muy importante activo para las organizaciones, que debe ser salvaguardado ante posibles amenazas, riesgos y vulnerabilidades, ya sea que vengan de fuentes internas o externas.

CAPÍTULO VI

LA GERENCIA Y EL PROBLEMA DE LA SEGURIDAD DE LA INFORMACION EN LAS ORGANIZACIONES MODERNAS

6.1 La Evolución de las Tecnologías de la Información y la Comunicación en el seno de las sociedades globalizadas

La historia humana ha sido fragmentada, por muchos investigadores, en periodos identificados por una tecnología cada vez más imperiosa con el pasar del tiempo en factores como lo son el almacenamiento, la codificación, el cifrado, la autenticación y recuperación de información, por tal motivo la evolución de las tecnologías de la información y comunicaciones ha originado avances en el seno de las sociedades globalizadas, que tienen un mayor impacto en la vida cotidiana de dichas sociedades. En muchas ocasiones tendemos a olvidar que las tecnologías de la información y comunicación, aparte de tener contradicciones en la sociedad, también es resultado de las condiciones sociales y económicas del tiempo que se encuentre viviendo esa sociedad, por ésta doctrina las sociedades globalizadas funcionan como promotor en la toma de decisiones referentes a la innovación, difusión y generalización de las tecnologías de la información y comunicación.

La evolución de las tecnologías de la información y comunicación obtienen un territorio ubicado en el campo socioeconómico en esta era cada vez más globalizada que permite su perfeccionamiento en las sedes de investigación y Universidades de los gobiernos de cada país, como de igual forma su entrega a la sociedad y aplicación a su elaboración. La evolución tecnológica en los medios, canales y soportes de la información y comunicación de la actualidad se están originando en frente de nuestros ojos y se puede comprender en un conjunto más extenso de avances en la organización lucrativa de nuestra sociedad globalizada.

Sergio Roberto Matías Camargo, en su publicación titulada *"Las Tecnologías de la Información y La Comunicación. Enfoque Interdisciplinario"* explica como ha sido el enfoque evolutivo de las tecnologías de la información y comunicación en el modelo de desarrollo económico social, ha permitido la convergencia tecnológica de las TIC y cita lo siguiente:

> Un aspecto importante e innovador de las TIC es la convergencia tecnológica, es decir, en términos de la UIT, que las redes de la próxima generación (NGN) y su implantación permitirán disponer de una gran variedad de servicios de audio, vídeo, datos y voz en una sola infraestructura. La convergencia aportará a los usuarios la ventaja de contar con servicios más modernos en esferas como la educación, la salud, la administración pública, la agricultura y los sistemas de alerta en situaciones de catástrofe, entre otros, y que contribuirá al desarrollo social y económico, en especial en los países en desarrollo. (P. 69).

De igual manera Kenneth Laudon y Jane Laudon, en su libro *"Sistemas de Información Gerencial"* mencionan como la globalización de la sociedad tiene que ver o se encuentra estrechamente relacionado con los sistemas o tecnologías de la información y comunicaciones a nivel gerencial, dicen lo siguiente:

> El surgimiento de Internet para convertirse en un sistema de comunicaciones mundial ha reducido de manera drástica los costos de operar y realizar transacciones a una escala global. La comunicación entre el piso de una fábrica en Shanghai y un centro de distribución en Rapid Falls, Dakota del Sur, es ahora instantánea y prácticamente gratuita. Ahora los clientes pueden ir de compras en un mercado mundial, en donde obtienen información sobre precios y calidad de manera confiable, las 24 horas del día. Las empresas que producen bienes y servicios a escala global logran extraordinarias reducciones en los costos al encontrar proveedores de bajo costo y administrar instalaciones de producción en otros países. Las empresas de servicios de Internet, como Google y eBay, pueden replicar sus modelos de negocios y servicios en varios países sin tener que rediseñar su costosa infraestructura de sistemas de información de costo fijo. La mitad de los ingresos de eBay (así como de General Motors) en 2011 se originará fuera de Estados Unidos. En resumen, los sistemas de información permiten la globalización. (P. 11).

La revolución tecnológica y lo que conlleva sus derivaciones, junto con la convergencia de las tecnologías de la información y comunicaciones son un proceso globalizado que se ha venido convirtiendo en algo cotidiano en nuestras vidas al generar nuevos productos y servicios para la sociedad y también nuevas y mejores formas de gestión organizacional, siendo un punto importante en el desarrollo económico. En este siglo XXI, la sociedad de hoy en día es más complicada, sin embargo la misma debe ser formada con el propósito de que evolucione a mismo tiempo que lo hacen las tecnologías de la información y comunicaciones para llegar a transformarse en una sociedad del conocimiento.

José Félix Tezanos Tortajada, en su libro titulado *"Tendencias Científico-Tecnológicas Retos, Potencialidades y Problemas Sociales",* habla sobre la revolución digital en la que se a fundamentado en las tecnologías de la información y comunicación; y como han impactado en la sociedad, por lo que cita lo siguiente:

> A lo largo de la revolución tecnológica, muchas cosas han cambiado en nuestro entorno. No solo la productividad y los modos de producción se han visto espoleados, sino que todo el escenario ha cambiado radicalmente. El mundo se ha globalizado, internet ha creado una nueva infraestructura global imprescindible para el tiempo que vivimos. Nuevos sectores y actividades desconocidas han tomado mayor protagonismo económico, mientras que la sociedad ha visto desarrollarse en su seno tendencias y comportamientos que han roto con hábitos y modos de socialización que parecían inmutables. (P.108).

Evolución de las TICs

Figura 10

6.2 La información como un recurso de la gerencia moderna.

La información es un grupo de datos que ya previamente han sido establecidos y procesados que suministran nuevos y valiosos conocimientos acerca un proyecto, el cual permite la solución de fallas y toma de decisiones aprovechando la mejor información que se adapte a las necesidades de la organización. Gracias al desarrollo tecnológico, la información fue evolucionando y en la actualidad la misma ha dejado de estar en manos de una pequeña cantidad de personas para ser un conocimiento de muchos. La utilización de las nuevas tecnologías y especialmente la información como herramienta y recurso fundamental, se ha convertido en el medio más importante que el de los activos fijos y financieros de la empresa, ya que el valor de estos activos se ha visto limitado por la influencia que ha tenido la información.

El investigador Peter Druker en su libro titulado "*Su Visión Sobre la Administración, la Organización, la Economía y la Sociedad"*, dice la importancia que representa la información como herramienta de negocios para la alta gerencia, por lo tanto el autor cita lo siguiente:

> La información básica, información de productividad, información de competencia e información de asignación de recursos, con la finalidad de generar riquezas, y que la empresa continúe en marcha; ésta información permite dirigir la táctica. Para la estrategia la alta gerencia requiere información organizada del entorno. La estrategia debe basarse en información relacionada con los mercados, clientes y no clientes; la tecnología propia de la empresa y de la competencia, finanzas en el ámbito mundial y el ambiente económico mundial. Por lo tanto, el gerente tiene que estar informado, tanto de sus subordinados como de la red de su entorno, lo cual le permite reunir información de suma importancia, para dirigir la táctica y la estrategia de la organización. (P.56).

Peter Druker en lo citado anteriormente, señala la importancia que representa la información para la alta gerencia en las organizaciones modernas debido a los negocios originados en los mercados por la fluctuación de la economía mundial y este aspecto puede dar origen a que las empresas no tengan un crecimiento económico y productivo rentable por el simple hecho de que la gerencia no posea la información necesaria y actualizada.

Para que las organizaciones modernas, deban aprovechar al máximo la información que poseen, les corresponde operarla de una manera correcta y eficiente, de la misma forma como manejan los otros recursos que ya existen en la organización y es por esto que los gerentes deben entender que se presentan costos relacionados a la elaboración, distribución, seguridad, acumulación y recuperación de la información que se maneja en la organización. A pesar de que la información se localiza en nuestro entorno y alcance, se debe tener en consideración que la misma no es gratis, y su utilización es estratégica para colocar en un nivel de superioridad a la organización, frente a sus demás competidores en las áreas donde se desempeñe.

La información del mundo actual se encuentra transformando la economía, gracias a que la misma se ha convertido en un recurso estratégico para las organizaciones modernas que les permite registrar y ampliar los niveles lógicos en la toma de decisiones en su alta gerencia, por lo que para llegar a este nivel se debe contar con la debida información, de lo contrario la organización no alcanzara las expectativas deseadas en materia competitiva respecto a los negocios. Para las organizaciones modernas y la alta gerencia de la misma, la información juega un papel crítico e importante en la toma de decisiones, como ya se ha mencionado anteriormente, pero también se deben tomar en cuenta determinados atributos en la calidad de la información como por ejemplo que la misma debe suministrarse en el momento que sea necesario, debe ser reciente, suministrarse con frecuencia, debe estar libre de errores, poseer un amplio alcance y puede proporcionarse en la forma de documentos impresos, presentaciones, informes digitales, entre otros. En la estructura de la información presente en las organizaciones también son importantes la planeación y control de la información, en el que se requiere del reconocimiento de los cambios internos y externos de la organización, así como también analizar constantemente todas las operaciones que se realizan en la organización y capacidades de la misma para cumplir con las actividades que la definen.

6.3 La gestión de la seguridad de la información como valor agregado prioritario para la gerencia de las organizaciones modernas.

Con el objetivo de fortalecer la gestión de la seguridad de la información, es obligatorio que la gerencia de las organizaciones modernas establezca lineamientos a todo el personal de la organización para el uso adecuado de la información y se apliquen los métodos y prácticas para la protección de la misma. Actualmente la problemática existente en lo que respecta a la gestión de la seguridad de la información en las empresas Venezolanas, es que dichas empresas en la mayoría de los casos se presenta por una falta de información sobre las nuevas tecnologías, es decir, por la falta de conocimiento en cuanto a la importancia que tienen hoy día la seguridad de la información por parte de la gerencia de los departamentos de TICs en las empresas, ocasiona que a medida que evolucionan las tecnologías de la información y comunicaciones en un mundo cada vez más globalizado, los problemas de seguridad de la información en las empresas se agraven si las mismas no tienen la protección necesaria, por lo que en conclusión la problemática de la gestión en la seguridad de la información, se hace presente por la falta de estándares, políticas, formación y cultura de la seguridad en los sistemas de información.

Las empresas en Venezuela, algunas de ellas no todas cabe destacar, no mantienen actualizadas las políticas y los estándares de seguridad en los sistemas de información por parte de la gerencia y esto trae como consecuencia graves problemas de seguridad, pero también se encuentran empresas que la prestan la debida atención a la seguridad de los sistemas de información, como por ejemplo las organizaciones de la banca pública y privada en Venezuela, las cuales debido al servicio que prestan deben poseer un sistema de gestión de la seguridad de la información actualizado, debido a que en éstas instituciones se almacena gran cantidad de información sobre datos financieros de sus clientes la cual debe ser muy protegida. Empresas públicas y privadas que operan en el país como Proveedores de Servicio de Internet (ISP), también son organizaciones que se encuentran tomando conciencia en la gestión de la seguridad de la información y la importancia que tiene la misma como un factos esencial en la gerencia.

En la gestión de la seguridad de la información en Gandalf Comunicaciones, la gerencia y el personal del departamento de TIC siempre se encuentran en la búsqueda de la forma de proteger la información que es utilizada cada día en las actividades y operaciones que permiten adquirir los objetivos de la organización y así poder establecer objetivos y claves propias de seguridad, es decir, se debe buscar la formación estratégica para que cualquier esfuerzo contribuya al cumplimiento de objetivos y resultados de la misión. Como parte del valor agregado prioritario de la seguridad de la información, la gerencia debe participar en las diferentes acciones, como el estudio y aprobación de las políticas de seguridad, establecer y participar en las estructuras internas de la organización que permitan expresar su compromiso y liderazgo, autorizar auditorías y asignar personal altamente capacitado para el área de seguridad, con el fin de evitar problemas en la gestión de la seguridad de la información que parte de las empresas que operan en Venezuela, no lo toman en consideración por la falta de cultura informacional sobre la seguridad de la información.

Jesús Diez, gerente de Data Center y Seguridad de Level 3 en Venezuela, empresa de telecomunicaciones que opera en nuestro país como un proveedor internacional de servicios de internet para pequeñas, medianas y grandes empresas de telecomunicaciones, en su publicación a el diario El Mundo expresa la necesidad que presentan las empresas del país tomen conciencia de la importancia que tiene la seguridad de la información como un valor prioritario en la gerencia y cita lo siguiente:

> En muchas ocasiones, las organizaciones desconocen lo que les puede estar pasando, o simplemente no tienen como medir la magnitud de los hechos, lo que sigue es la elaboración de un estudio, tanto de la red interna de la organización, como también de sus políticas de seguridad y darle la debida importancia a nivel de presupuesto de TI (Tecnologías de la Información), esto con la finalidad de hacer las mejoras que correspondan a su infraestructura, equipos y personal calificado. Frente a un panorama de aumento vertiginoso del cibercrimen, Level 3 ha potenciado su ya poderosa infraestructura de red global y sus servicios gerenciados de seguridad con tecnologías líderes de detección y mitigación para garantizarles a sus clientes una capa avanzada contra estas eventuales agresiones.
>
> ***http://www.elmundo.com.ve/noticias/negocios/tecnologia/empresas-venezolanas-deben-prepararse-para-un-mayo.aspx#ixzz4qba2Ahjo***

En la gerencia del departamento de TIC en Gandalf Comunicaciones, dicho departamento posee herramientas tecnologías de seguridad como lo son DDos, Mitigation y Advance Security Testing, al igual que otras empresas que operan como ISP, con el objetivo de llevar y mantener un monitoreo constante de la seguridad de la información y evitar el ingreso de paquetes generados por intrusos por medio de ciberataques que puedan causar graves daños a los activos de información de la empresa y de sus clientes, sin embargo existen más herramientas tecnológicas de seguridad. La práctica arroja como resultado que el nivel de seguridad de la información aprehendido por medios técnicos es limitado e insuficiente por sí mismo por lo que las organizaciones modernas deberían tomar parte activa para conseguir una gestión positiva de la seguridad de la información. Esta gestión de la seguridad de la información debe estar liderada por la gerencia del departamento de TIC y se considera además los activos internos a clientes y proveedores de bienes y servicios.

Sistema de Gestión en la Seguridad de la Información

Figura 11

6.4 Últimos cambios y tendencias mundiales que se han generado en el área de la seguridad de la información

En los últimos años se han presentando importantes cambios y beneficios a nivel mundial que han traído las TIC a la gerencia de la seguridad de la información. En el que se destaca:

- ✓ La gestión de la seguridad de la información, permite a la gerencia poseer un soporte pueda respaldar a los altos directivos de la organización.
- ✓ Elaboración de un proyecto de inversión económica en el campo de la seguridad de la información, donde se refleje el resultado que arrojaría un golpe económico si se lleva a cabo el ataque a los sistemas e información.
- ✓ Presentar a través de un informe las soluciones para la mitigación ya sea de forma correctiva o preventiva ante las vulnerabilidades y ataques, para así, de esta manera la gerencia del departamento de TIC permita garantizar que la inversión resguarde la gran mayoría de las grietas de seguridad, junto con eficientes y eficaces controles de riesgo.
- ✓ Recolección de pruebas que para los casos que se presenten de fraude tanto a nivel interno o externo, permite a la gerencia entregar esa evidencia al departamento legal de la organización para que se preceda a abrir un proceso administrativo ya sea de manera interna si es el caso o judicial si también es el caso.
- ✓ Proyectar la inversión económica en materia de seguridad de la información con pruebas y cálculos si ocurre un ataque a los sistemas de información.

Es primordial para la gerencia de la seguridad de la información, tener claro el modelo de gestión que se realizara en el área de la misma, donde se tomaran en cuenta los costos y las consecuencias que pueda traer dicho patrón, por lo que sin importar el modelo de gestión que se implemente para una efectiva gestión, es necesario que la gerencia de TIC prepare una eficaz y segura gestión en la materia, debido a que es un activo de mucho valor para los objetivos de la organización y su mejora continua en las operaciones comerciales.

Las TIC han brindado beneficios y ventajas bastantes significativas en la gerencia de la seguridad de la información en las organizaciones modernas, porque les ha permitido reducir los costos con la implementación de políticas y estándares internacionales, así como también mejorando el control y acceso a la información. Las TICs han tenido un impacto positivo en la gerencia de las organizaciones modernas de la actualidad, ya que han aportado soluciones en la gerencia de los diferentes departamentos de la organización, como lo son RR.HH, Finanzas, Ingeniería, Ventas, TIC, Operaciones, entre otros, así como también las TICs han mejorado el acceso a las herramientas del conocimiento, han permitido la implementación de nuevos recursos tecnológicos que contribuyen a fomentar el desarrollo de las operaciones en las organizaciones modernas.

Ahora bien las TICs han traído a la gerencia innovación tecnológica, creación y construcción de nuevos métodos tecnológicos, así también las garantías de la implementación y posterior cumplimiento de políticas de seguridad en los sistemas de información, por lo que se han convertido en un elemento clave haciendo que las operaciones o actividades gerenciales dentro de la organización sean más beneficiosas en donde por ejemplo se aceleran de una forma más eficaz y eficiente las comunicaciones, se mantiene el trabajo en equipo, se gestionan de mejor forma las decisiones, se realizan análisis financieros y se promocionan los productos y servicios que ofrece la organización para sus usuarios, clientes y proveedores. En este sentido Paola Chocano, directora en la organización Consultoría de Career Partners, explica como los gerentes hacen uso constante de las tecnologías digitales o de las TICs en la actualidad para estar siempre conectados e informados sobre sus negocios y poder interactuar con aplicaciones web corporativas.

Paola Chocano, en una publicación titulada *"Herramientas digitales, cada vez más presentes en las oficinas de los altos ejecutivos"*, para el diario Gestión de Perú, cita lo siguiente sobre cómo han impactado las TICs en los altos ejecutivo o en la gerencia moderna

> Hoy en día los negocios están cada vez más digitalizados (como Uber, Netflix y Amazon). Por ende, el ejecutivo debe tener una visión para transformar su negocio a la era digital, pues no hacerlo podría sacarlo del mercado. La disminución de negocios de servicios presenciales, por el mayor uso de apps, así como la transición a canales digitales de cada vez más negocios, afectarán algunas características de lo que se busca en un alto ejecutivo", el alto ejecutivo debe contar con un perfil innovador, gestor del cambio, una visión digital y globalizada.

http://gestion.pe/empleo-management/herramientas-digitales-cada-vez-mas-presentes-oficinas-altos-ejecutivos-2188747

6.5 Los conocimientos y experiencias que deben dominar los gerentes en los departamentos de TICs para salvaguardar la información.

Los gerentes de los departamentos de tecnología de la información y comunicaciones, deben estar al tanto de que la organización cuente con el equipamiento necesario, el cual debe ser el más eficiente y eficaz en lo que se refiere a sus funciones. Por este motivo los gerentes que lideran los departamentos de TIC en las organizaciones modernas tienen que poseer amplios conocimientos en el área de la seguridad de la información, de igual manera deben estar actualizados sobre los últimos y más recientes avances tecnológicos en materia de seguridad para poder brindar excelentes asesorías a los gerentes de otros departamentos de la organización y realizar proyectos sobre tecnologías de la información y comunicaciones a futuro.

De acuerdo a los conocimientos y experiencias que deben dominar los gerentes de TIC en la seguridad de la información se tienen los siguientes aspectos:

- Diseñar, implementar y monitorear las estrategias de TICs
- Asesorar en la mejor implementación de los estándares internacionales de seguridad, de acuerdo a las necesidades de la organización.
- Definir, elaborar e implementar políticas y normas de seguridad de la información y comunicaciones, tanto lógica como física.
- Mantener la disponibilidad, confiabilidad e integridad de los sistemas de información.
- Manifestar las condiciones para la adquisición de dispositivos relacionados con las tics y la contratación de servicios tecnológicos sobres seguridad y telecomunicaciones.
- Respaldar la investigación, desarrollo y aplicación de nuevas tecnologías en seguridad de la información relacionadas a la continua mejora de capacidades y generación de ventajas competitivas para la organización.
- Elaborar y proponer actividades de capacitación y actualización dirigidas al mejoramiento continuo del personal que forma parte del departamento de TIC en relación a la seguridad de la información.

- Especificar las condiciones en las que se debe contratar personal especializado en la seguridad de las TICs.

- Establecer planes de contingencia ante posibles amenazas, ataques y vulnerabilidades a los sistemas de información y verificar su funcionamiento.

En otro sentido el gerente de TICs, gracias a su experiencia y conocimiento debe poder innovar al implementar nuevos productos y servicios, como estrategias y políticas de seguridad, software de última generación que ayuden a la seguridad de la información, permitiendo con la continua protección de los activos de la organización. La experiencia y los conocimientos le permiten al gerente aumentar el conocimiento con el personal del departamento de TIC, establecer normas y procedimientos que respalden el uso racional de la herramientas que permitan asegurar los activos de la organización, es decir, que los criterios de confiabilidad y seguridad de la información sean los más adecuados y convenientes para la organización.

Iván Darío Marrugo, socio fundador de la firma Marrugo Rivera & Asociados y abogado especialista en Derecho de Tecnologías en Seguridad de la Información y Protección de Datos personales y también auditor interno bajo la norma ISO 27001, junto con Andrés Felipe Contreras, consultor jurídico y abogado en derecho de las telecomunicaciones y nuevas tecnologías, en una publicación titulada *"Seguridad de la Información, pieza fundamental en la Gerencia Moderna"* hablan que con los conocimientos y experiencias adquiridas por los gerentes de TIC, los mismos pueden utilizar un Sistema de Gestión de la Seguridad de la Información, que se encuentra incorporado en los estándares internacionales de la familia ISO 27000, como una herramienta de dominio para salvaguardar la información de la organización, por lo tanto ambos autores de dicha publicación citan lo siguiente:

En el actual estado de desarrollo de la industria y el comercio, se evidencia como los esquemas de producción de bienes y servicios, los puestos de trabajo y los mercados en general, se energizan con modelos organizacionales en los que la alta gerencia de las compañías que quieren participar de dicho desarrollo, deben implementar sistemas de gestión de riesgo que respondan a la protección ponderada del activo empresarial más importante en la actualidad: **la información**. En relación con lo anterior, todos los niveles que participan en el flujo de datos dentro de la organización, deben auspiciar esfuerzos por mantener dinámicos y funcional, los diferentes modelos de gestión de seguridad de la información que se hayan implementado o se quieran implementar; siendo de suyo y apenas obvio, la importancia que tiene que la gerencia y los diferentes niveles directivos, participen en los procesos que de dicha gestión se desprendan.

http://www.digiware.net/?q=es/blog/seguridad-de-la-informacion-pieza-fundamental-en-la-gerencia-moderna

El dominio que obtienen los gerentes de TIC con sus conocimientos y experiencias para salvaguardar la información, ha resultado de gran utilidad para la gerencia de los sistemas de información y para la del resto de gerencias en las organizaciones modernas de la actualidad, debido a que le ha permitido incorporar importantes y grandes avances tecnológicos que traen excelentes beneficios competitivos y comerciales para las operaciones de los productos y servicios que ofrecen las organizaciones actuales.

6.6. La gerencia y el problema de la seguridad de la información en las organizaciones modernas.

Actualmente se ha encontrado que el problema de la seguridad de la información en las organizaciones modernas es la falta de gerentes que se encuentren capacitados profesionalmente en las áreas de gestión y seguridad de las TICs, es decir, que estén capacitados académicamente y presenten los conocimientos y experiencias necesarias para tales cargos. Otro problema que se observa es la falta de inversión tecnológica actualizada por parte de los directivos de las organizaciones, pero esto se debe a la falta de información sobre la importancia que representa la seguridad de la información para sus organizaciones. La solución al problema de la seguridad de la información en las organizaciones es gracias a la convergencia de dos factores, el primero es que la gerencia de los departamentos de TIC deben ser liderados por profesionales altamente capacitados en el área, y el segundo y no menos importante es la concientización, información y conocimiento sobre las seguridad de la información, un papel de importante responsabilidad que debe realizar la gerencia de las TIC.

Sid Deshpande, analista de la principal consultora Gartner, en una publicación titulada *"Seguridad de la Información: un 7% más en el 2017"* menciona algunos aspectos relevantes que debe considerar la gerencia de las TICs en la seguridad de la información por lo que cita lo siguiente:

> Mejorar la seguridad no es solo gastar en nuevas tecnologías. Viendo los incidentes globales de seguridad, esta área se ha convertido en un básico cada vez más importante. Las organizaciones deben invertir en posturas seguras centrados en la gestión de vulnerabilidades, segmentación de redes y administración de errores con sistemas de copias.
>
> ***http://www.muycanal.com/2017/08/21/seguridad-informacion-demanda***

Un ejemplo de dicha problemática fue el que se presento el 12 de Mayo del 2017, cuando un ataque producido por el virus WannaCry producía un cibersecuestro al encriptar la información en los documentos de los equipos de las organizaciones, en el que luego pedía un millonario rescate a los dueños de dicha información. Con ese ataque a la vulnerabilidad en la seguridad de la información grandes organizaciones quedaron paralizadas ocasionando grandes pérdidas de dinero. El ataque que afecto a grandes y reconocidas organizaciones como Movistar y Fedex, las cuales por la falta de concientización y mala gestión, los cibercriminales que ocasionaron el ataque, vieron una potencial vulnerabilidad y la supieron aprovechar, por esto la gerencia debe concientizar a todo el personal de la organización sobre la problemática de la seguridad de la información e indicarles cuál es el procedimiento a seguir para evitar pérdidas a la organización, los cuales dichos procedimientos se encuentran estipulados en las políticas de seguridad para implementar un Sistema de Gestión de Seguridad de la Información.

La universidad de Harvard en el año 2015, realizo una investigación en la que encontró que las organizaciones modernas admiten que presentan problemas en la gerencia y seguridad de la información, por lo que aconseja que lo mas optimo es que los altos directivos de la organización y la gerencia de TICs patrocinen un cuadro donde la gerencia de TIC pueda identificar e implementar las mejores estrategias en seguridad de la información y permita la solución a dicha problemática. En este sentido y a la falta de conocimientos en el tema por parte de la gerencia, Rober Artavia, presidente de Viva Trust y del consejo directivo de Incae, en una publicación titulada *"La Protección de los Datos es un asunto de la Alta Gerencia"* cita lo siguiente:

> Los gerentes de las empresas solo conocen generalidades de los sistemas y sus vulnerabilidades, mas no los riesgos directos creados por la tecnología para la privacidad y seguridad de su información.

http://www.elfinancierocr.com/tecnologia/Club_de_Investigacion_Tecnologica-Eset-Fortinet-Harvard-IBM-Deloitte-seguridad_0_956304380.html

CONCLUSIONES

Las organizaciones modernas, como el Gandalf Comunicaciones, actualmente, están tomando más conciencia sobre el tema de la seguridad de la información, gracias a los ataques recientes que han sufrido grandes empresas transnacionales. Con la aparición de nuevos riesgos, amenazas y vulnerabilidades, ha obligado a las organizaciones a solicitar personal altamente capacitado en la seguridad de la información, el cual les permita dar a conocer sobre las nuevas tecnologías, protocolos y estándares de seguridad disponibles que puedan ser implementados de acuerdo a las necesidades de la organización. El correcto uso de las políticas de seguridad de la información por parte de la gerencia de los departamentos de TIC, Gandalf Comunicaciones, ha dado como resultado grandes beneficios que han permitido incrementar la eficacia y eficiencia de los servicios que ofrecen la organización, permitiéndoles garantizar altos niveles de seguridad para sus sistemas de gestión de la información.

Hoy en día Gandalf Comunicaciones establece sus estrategias en base a la disponibilidad, confiabilidad e integridad de la información, la cual le permite una eficiente y efectiva toma de decisiones, que gracias a la seguridad de sus activos permite acceder a la información. Desde el punto de vista gerencial, es necesario que la gerencia de las TIC en las organizaciones y en en este caso Gandalf Comunicaciones, cuenten con las herramientas metodológicas más recientes y con un personal calificado en el área, para poder facilitar el desarrollo de innovadoras soluciones orientadas en la seguridad de las TIC y ofrecer los conocimientos necesarios para poder dominar todos los aspectos referentes a la seguridad de la información. Se pudo observar que Gandalf Comunicaciones, C.A. como organización moderna, cumple con los estándares de seguridad física en sus infraestructuras, así como también en lo que respecta a la seguridad lógica de sus sistemas de información, sin embargo hay que mejorar los actuales niveles de seguridad que Gandalf Comunicaciones, C.A. posee para el aseguramiento y gestión de los sistemas de información.

RECOMENDACIONES

Inspeccionar constantemente las últimas y más recientes actualizaciones de las versiones en los estándares internacionales de la Serie ISO 27000, avances en las TIC con el objetivo de garantizar la mejor aplicación de los sistemas de seguridad en los activos de información de las organizaciones modernas como el caso de Gandalf Comunicaciones, c.a. Es importante que la Gerencia del departamento de TIC, en la empresa Gandalf, mantenga actualizadas todas las políticas de seguridad de la información y hacerlas conocer a todo el personal que labora en la organización. También es importante que realice todos los pasos necesarios para poder obtener la certificación de seguridad de la serie ISO 27001.

La Gerencia de TIC en Gandalf, debe establecer un plan de contingencia con el procedimiento a seguir, que le permita a la organización continuar con las operaciones administrativas, comerciales, de ingeniería, entre otras, en el caso de que se presente algún tipo de problemas en la plataforma tecnológica y se vean afectada la seguridad de los sistemas de información de la organización. Es necesario que las políticas de seguridad de la información se incluyan los procesos o métodos de auditorías a los sistemas de información con iniciativa, supervisión y coordinación de la gerencia de TIC, como mediadas adicionales de seguridad de la información.

El personal del departamento de TIC en Gandalf Comunicaciones, junto con la gerencia de dicho departamento, clasifique e identifiquen los activos de información y determinar el nivel de importancia de cada activo para el correcto funcionamiento en la seguridad de los sistemas de información. El departamento de TIC en Gandalf Comunicaciones, debe utilizar aplicaciones avanzadas que les permitan analizar y proteger la información de cualquier tipo de amenaza, vulnerabilidad y ataque, así como también mitigar los mismos. La gerencia de TIC en Gandalf debe mantener actualizadas las estrategias y herramientas gerenciales para una mejor toma de decisiones en la información y seguridad de la misma.

7. Referencias Bibliográficas.

Agostini, G. (2016). *El Dominio del Saber y la Información como Factores de Gerencia y Competitividad en el Seno de las Naciones Latinoamericanas (Caso Venezuela), Valencia, Venezuela.*

Academia de Networking de Cisco Systems. (2004). (3era Ed.) *Guia del Segundo Año CCNA 3 y 4. Madrid, España.*

Baca, G. (2016). (1era Ed.) *Introducción a la Seguridad Informática. Cuidad de Mexico, Mexico.*

Burreta, E. (2015). *Transmisión de Información por Medios Convencionales e Informáticos*. *España.*

Cano, J. (2014). *La Fundación de Seguridad de la Información. Publicado por el periódico ISACA en el 2014*

Castells, M. (ed.2014). *La Ciudad Informacional: Tecnologías de la Información, Editorial Alianza, Madrid, España.*

Drucker, P. (1996). *Su Visión Sobre la Administración, la Organización, la Economía y la Sociedad, Grupo Editorial Norma, Bogotá, Colombia.*

Drucker, P. (2002). *Los Desafíos de la Gerencia para el Siglo XXI, Grupo Editorial Norma, Bogotá, Colombia.*

Giménez, J. (2014). (1era Ed.) *Seguridad en Equipos Informáticos, IC Editorial. Málaga, España.*

Hernández, F. (2011). *Desarrollo de un Modelo de Madurez para las Contingencias y Recuperación de la Información en las pequeñas y medianas empresas del sector salud en Venezuela. Caracas, Venezuela.*

Laudon, J. y Laudon, K. (2da. Ed.2012). *Sistemas de Información Gerencial 2da edición, Editorial Pearson, México.*

Lourdes, T. (2013). *Modelo de Gestión de Seguridad para la Corporación Financiera Nacional Basado en Gestión de Riesgo. Quito, Ecuador.*

Matias, S. (2011). *Las Tecnologías de la Información y La Comunicación. Enfoque Interdisciplinario. Bogotá, Colombia.*

Tezanos, J. (2016) *Tendencias Cientifico-Tecnologicas Retos, Potencialidades y Problemas Sociales. Madrid, España.*

Universidad José Antonio Páez (2014). *Manual para la elaboración, inscripción, presentación y defensa del trabajo especial de grado, trabajos de grado y tesis doctoral, San Diego, Valencia, Venezuela.*

8. Fuentes Electrónicas

http://www.revistabyte.es/cloud-computing/toda-la-empresa-la-nube-especial-cloud-computing/ (En Línea) [Consulta: 2017, Mayo 14]

http://blogs.eada.edu/2012/07/05/tecnologias-informacion-en-empresa/ (En Línea) [Consulta: 2017, Junio 23]

http://www.muycomputerpro.com/2017/02/26/cisco-virtualizacion-seguridad/ (En Línea) [Consulta: 2017, Julio 16]

http://www.lanuevacronica.com/proconsi-crea-un-departamento-para-detectar-ciberataques-contra-pymes (En Línea) [Consulta: 2017, Julio 26]

https://infobyteabyte.wordpress.com/2016/04/20/seguridad-de-la-informacion-seguridad-informatica-y-ciberseguridad-son-sinonimos/ (En Línea) [Consulta: 2017, Julio 31]

http://www.elmundo.com.ve/noticias/negocios/tecnologia/empresas-venezolanas-deben-prepararse-para-un-mayo.aspx#ixzz4qba2Ahjo (En Línea) [Consulta: 2017, Agosto 23]

http://gestion.pe/empleo-management/herramientas-digitales-cada-vez-mas-presentes-oficinas-altos-ejecutivos-2188747 (En Línea) [Consulta: 2017, Agosto 27]

http://www.digiware.net/?q=es/blog/seguridad-de-la-informacion-pieza-fundamental-en-la-gerencia-moderna (En Línea) [Consulta: 2017, Septiembre 01]

http://www.muycanal.com/2017/08/21/seguridad-informacion-demanda (En Línea) [Consulta: 2017, Septiembre 02]

http://www.elfinancierocr.com/tecnologia/Club_de_Investigacion_Tecnologica-Eset-Fortinet-Harvard-IBM-Deloitte-seguridad_0_956304380.html (En Línea) [Consulta: 2017, Septiembre 03]

http://blog.segu-info.com.ar/2017/09/mini-botnet-logra-lanzar-ataque-ddos-de.html?utm_source=Segu.Info&utm_medium=twitter&utm_campaign=seguinfo&m=1 (En Línea) [Consulta: 2017, Septiembre 10]