ANÁLISIS E IDENTIFICACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA, DIRIGIDO A LAS ORGANIZACIONES EN COLOMBIA, QUE BRINDE UN DIAGNÓSTICO GENERAL SOBRE LA IMPORTANCIA Y MEDIDAS NECESARIAS PARA PROTEGER EL ACTIVO DE LA INFORMACIÓN.

YINY DAYAN PEÑUELA VASQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
FUSAGASUGA
2018

ANÁLISIS E IDENTIFICACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA, DIRIGIDO A LAS ORGANIZACIONES EN COLOMBIA, QUE BRINDE UN DIAGNÓSTICO GENERAL SOBRE LA IMPORTANCIA Y MEDIDAS NECESARIAS PARA PROTEGER EL ACTIVO DE LA INFORMACIÓN.

YINY DAYAN PEÑUELA VASQUEZ

Monografía de investigación para optar el título de especialista en seguridad informática

Director:
ING. JUAN JOSÉ CRUZ GARZÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
FUSAGASUGA
2018

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del jurado

_____
Firma del Jurado

Fusagasugá, 28, Febrero, 2018

DEDICATORIA

Dedico mi proyecto especialmente a Dios, por permitirme cumplir con mi objetivo y darme la fuerza para continuar a pesar de las dificultades, a mi familia por su apoyo continuo en especial a mi hermano John que me dio el impulso para cumplir con esta meta y no dudar de mis capacidades, a mi esposo Fabio por su ánimo y entrega, buscando siempre cumplir con nuestro proyecto de vida y nuestros sueños.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia UNAD por la oportunidad de crecer académicamente, a los profesores que me brindaron el apoyo oportuno, sabiduría y las herramientas para lograr este objetivo.

Agradezco también a mi asesor de proyecto Juan José Cruz Garzón, por brindarme sus conocimientos y apoyo, y a todas las personas que de una u otra manera aportaron en el desarrollo de este proyecto.

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

Hoy en día la seguridad informática se ha convertido en un elemento fundamental en las organizaciones dado el avance constante de la tecnología, convirtiendo la información en un activo fundamental es por esto que la siguiente monografía consiste en realizar un análisis del estado actual de la seguridad informática en las organizaciones de Colombia, dado que en la actualidad es muy significativo recocer la importancia de la seguridad de la información siendo la información uno de las activos más importantes en las organizaciones, además se brindara un diagnostico general sobre la importancia y medidas necesarias para proteger el activo de la información, buscando que las organizaciones Colombianas identifiquen que es necesario la implementación de un Sistema de Gestión de la Seguridad de la Información SGSI en cada empresa sin importan su tamaño o el servicio que presten.

Se tendrán en cuenta los análisis e informes presentados por las empresas de antivirus más grandes del mundo Kaspersky, Symantec, McAfee, ESET y Norton, además teniendo en cuenta reportes realizados por la ONU, la ISO, la Asociación Colombiana de Ingenieros de Sistemas (ACIS) y también para contextualizar se tendrá en cuenta informes del Ministerio de Tecnologías de Información y las Comunicaciones de Colombia y la policía nacional de Colombia.

INTRODUCCIÓN

Debido a la globalización y el avance de la tecnología, la información ha tomado un papel muy importante en cualquier organización, la tecnología avanza diariamente y todas las organizaciones se han visto en la necesidad de adaptarse y sistematizar su información por medio de sistemas de información que a su vez se encuentran en computadores y estos computadores en redes, que por su puesto tienen acceso a internet, es por esto que en todo el mundo se presentan ataques informáticos a diario mediante diferentes tipos, lo que puede llevar a daño en la información, perdida etc., que conlleva a un gran problema ya que en la actualidad la información se ha convertido en uno de los activos más importantes de las organizaciones y al verse afectada puede causar daños económicos muy grandes.

La falta de conocimiento, falta de cultura en seguridad informática, la falta de colaboración en las empresas, además del poco entendimiento sobre este tema y por supuesto la baja inversión presupuestal de las organizaciones en seguridad han sido los motivos principales por el que las organizaciones no le han tomado importancia a la implementación de políticas de seguridad; debido a esto se realizara un análisis e identificación del estado actual de la seguridad informática, dirigido a las organizaciones en Colombia, que brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información.

1. TITULO

ANÁLISIS E IDENTIFICACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA, DIRIGIDO A LAS ORGANIZACIONES EN COLOMBIA, QUE BRINDE UN DIAGNÓSTICO GENERAL SOBRE LA IMPORTANCIA Y MEDIDAS NECESARIAS PARA PROTEGER EL ACTIVO DE LA INFORMACIÓN.

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA.

La seguridad informática tiene su origen en la necesidad de proteger la información en vista de que esta ya no se manejaba solo en papel, sino que se hacía de forma electrónica, antiguamente la seguridad se prestaba de manera física actualmente es necesario y primordial el soporte informático. Es así como se vio en la obligación de normalizar o estandarizar la seguridad informática ya que la información se convirtió en uno de los activos más importantes de las organizaciones, por esta razón La International Organization for Standardization e International Electrotechnical Commission ISO/IEC, se ha convertido en la organización encargada de estandarizar y normalizar la gestión de la seguridad de la información en cualquier organización.

Actualmente las Normas de la serie ISO 27000 son las encargadas de estandarizar, pero estas tuvieron su origen en la norma británica BS7799 cuya entidad normalizadora fue BSI (British Standards Institution) en 1995, esta norma se dividió en dos partes la BS 7799-1 la guía de buenas prácticas y la BS7799-2 de 1998 siendo la primera no certificable y la segunda dio origen al SGSI (Sistema de Gestión de Seguridad de la Información) la cual era certificable.

Dichas normas se revisaron en 1999, para que en el año 2000 la norma BS7799-1 pasara a ser la norma ISO 17799 sin cambios importantes, ya en el 2005 la BS7799-2 se publicó como la ISO 27001 esta con algunos cambios, ya para ese momento algunas empresas se encontraban certificadas con la Norma BS7799-2.

Para el 1 de julio de 2007 la norma ISO17799 fue denominada como ISO 27001:2005. Y en marzo de 2005 la BSI público una nueva norma BS7799-3:2006 que se encargaba de la gestión de riesgo de los sistemas de información.

Estas normas fueron el pilar inicial para las normas que usamos en la actualidad que son de la seria ISO/IEC 27000 siendo la ISO/IEC 27001 la única norma certificable.

En la actualidad cualquier organización que desee cumplir con los niveles adecuados de seguridad informática debe cumplir con la certificación ISO 27000.
Las normas utilizadas actualmente por las organizaciones para cumplir con los estándares son las siguientes:

- ✓ La norma ISO/IEC 27000 fue publicada en 1 de mayo de 2009, es básicamente la introducción a los SGSI con una descripción del ciclo PDCA.
- ✓ La norma ISO/IEC 27001 fue publicada el 15 de octubre de 2005, que cuenta con los requisitos del SGSI, esta es la única norma que es certificable.
- ✓ La norma ISO/IEC 27002 fue publicada el 1 de julio de 2007, es la guía de buenas prácticas para los controles de seguridad informática.
- ✓ La norma ISO/IEC 27003, fue publicada el 1 de febrero de 2010, se basa en el diseño, implementación, procesos, aprobación y planes en marcha del SGSI.
- ✓ La norma ISO/IEC 27004 fue publicada el 15 de diciembre de 2009, establece la efectividad del SGSI.
- ✓ La norma ISO/IEC 27005 fue publicada en 15 de junio de 2008 con una segunda edición el 1 de junio de 2011, para la gestión de riesgo de la seguridad de la información, con el enfoque de gestión de riesgos.

Cumpliendo con estas normas las organizaciones logran aplicar el SGSI, garantizando en gran medida la seguridad de la información, es necesario que las organizaciones cumplan con todas normas, leyes o estándares internacionales con el fin de salvaguardar y mitigar las vulnerabilidades a los que está expuesto el bien de la información.

2.2 FORMULACIÓN DEL PROBLEMA.

¿POR QUÉ ES IMPORTANTE ANALIZAR E IDENTIFICAR EL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA DIRIGIDO A LAS ORGANIZACIONES EN COLOMBIA, QUE BRINDE UN DIAGNÓSTICO GENERAL SOBRE LA IMPORTANCIA Y MEDIDAS NECESARIAS PARA PROTEGER EL ACTIVO DE LA INFORMACIÓN?

2.3 DESCRIPCIÓN DEL PROBLEMA.

En la actualidad tanto en Colombia como en el mundo la seguridad informática se ha convertido en un elemento muy importante en todas las organizaciones, considerando el papel que tiene la información; ya que esta se ha convertido en un activo muy importante, es allí donde radica la importancia de protegerla, esta información puede ser encontrada de distintas forma ya sea en papel, almacenada electrónicamente, a través de correo electrónico, en videos, grabaciones, o en cualquier medio digital etc. Es así que a través de cualquiera de estos medios la información se puede ver amenazada o vulnerada. En la antigüedad la seguridad principalmente era física ya que la mayoría de la información se encontraba en

papel, pero en la actualidad la prioridad está en el soporte informático y la seguridad lógica, ya que las organizaciones cada día más dependen de sus sistemas de información y estos son cada vez más vulnerables.
Los delitos informáticos han tenido un gran aumento a nivel mundial, incluyendo Latino América, esto se debe en gran medida a la necesidad en las organizaciones de adquirir nuevas tecnologías de la información, y a la falta de conocimiento sobre cómo deben protegerse de estos delitos. Por otra parte, no sería necesario proteger la información si no existiera quien la necesite o quien pague por conseguirla, es por esto que debemos tener en cuenta el mercado negro de la información, que busca obtener bases de datos con información personal para distintos fines.

Se han presentado muchos ataques informáticos en donde los atacantes consiguen obtener información confidencial, que han traído con ello costosas pérdidas económicas, legales o incluso en su imagen, es allí donde se ve la necesidad de derribar algunos mitos y aclarar algunos conceptos sobre la importancia de la seguridad informática para las organizaciones en Colombia, ya que entre más claridad se tenga sobre el tema se genera más conciencia de que todos tenemos algo que ver en el manejo y seguridad de la información dentro de una organización.

Es por esto que se plantea analizar e identificar el estado actual de la seguridad informática, dirigido a las organizaciones en Colombia, que brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información, con el fin de contextualizarnos e identificar en que radica esa importancia y como a través de los años ha tomado más fuerza tanto en grandes, medianas y pequeñas empresas, siendo hoy en día un punto fundamental en el desarrollo de las mismas y más aun siendo la información uno de las bienes más preciados en este momento en todas los organizaciones, es allí donde radicara el valor de este análisis.

3. JUSTIFICACION

Desde el inicio de la globalización, la informática se ha constituido en un factor importante en las organizaciones por aspectos como el internet, las redes sociales, las nuevas tecnologías de la información y nuevos sistemas de información, donde las empresas deben manejar su información convirtiéndose esta en uno de las activos más preciados, es así como las organizaciones le deben prestar más atención a la seguridad de la información, ya que aunque se debe estar a la vanguardia en las tecnologías de la información en este mundo globalizado también se debe avanzar y conocer la importancia de la seguridad informática, es necesario estar consciente de los riesgos con que se cuenta, las amenazas y vulnerabilidades que se puedan tener y reconocer que la seguridad no es un juego y más aún cuando se trata de la información de nuestras organizaciones.

Es muy peligroso ignorar los riesgos y las amenazas que se presentan cada vez con más frecuencia en la actualidad, algunos de estos pueden ser accidentales por desconocimiento del mismo personal de la empresa, por negligencia o pueden ser provocados siendo ataques directos al sistema que pueden buscar robar información o dinero a través de transferencias financieras, manipular datos, esto puede suceder en cualquier entidad sea pública o privada, negocios, hospitales, colegios, e incluso el gobierno que depende en gran medida de su presencia en línea.

Para contrarrestar esto es necesario identificar la importancia de la seguridad informática en las organizaciones derribar mitos y aclarar algunos conceptos, que permitan contextualizar la seguridad informática en Colombia.

Con la información viajando a través de diferentes redes del mundo se hace necesario proteger la información, es necesario que acá en Colombia se le dé la importancia que esto requiere, en base a lo anterior descripción el propósito de la presente es realizar un análisis e identificar el estado actual de la seguridad informática, dirigido a las organizaciones en Colombia, que brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información.

4. OBJETIVOS DEL PROYECTO

4.1 OBJETIVO GENERAL

Analizar e identificar el estado actual de la seguridad informática, dirigido a las organizaciones en Colombia, que brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información.

4.2 OBJETIVOS ESPECÍFICOS.

1. Identificar los elementos básicos acerca de la importancia de la seguridad informática en las organizaciones en Colombia.

2. Realizar el análisis e identificación del estado actual de la seguridad informática dirigido a las organizaciones en Colombia, basados en los informes emitidos anualmente por las más grandes empresas de antivirus, Kaspersky, Symantec, McAfee, ESET y Norton, además teniendo en cuenta reportes realizados por la ONU, la ISO, la Asociación Colombiana de Ingenieros de Sistemas (ACIS), el Ministerio de Tecnologías de Información y las Comunicaciones de Colombia y la policía nacional de Colombia.

3. Indagar la Importancia de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones colombianas.

4. Presentar el estado de la seguridad informática para las organizaciones en Colombia.

5. MARCO REFERENCIAL.

5.1 MARCO TEÓRICO.

5.1.1 Teoría general de sistemas. El biólogo Ludwig von Bertalanffy (1901-1972), es quien propuso la denominación “Teoría general de sistemas” para el este era el mecanismo de integración entre las ciencias naturales y sociales y ser el instrumento para la formación y preparación de científicos.

En 1925 Bertalanffy publico sus investigaciones con relación a los sistemas abiertos, pero fue en realidad en 1945 cuando termino la segunda guerra mundial que su investigación tomo importancia y a partir de este momento la “Teoría general de sistemas” fue acogida por el mundo científico hasta la actualidad.

La TGS se puede ver como la forma ordenada y científica de representación del mundo real ya que pretende la integración de diversas ciencias naturales y sociales, nos lleva además a analizar con el objetivo de buscar soluciones, ya sean problemas grandes o pequeños ya que se convierte en un lenguaje universal, con el fin de unir múltiples áreas o especialidades para que trabajen en un bien común, esto puede ser aplicado en cualquier contexto, es por esto de su importancia ya que se puede aplicar cualquier ámbito organizacional para la búsqueda de una solución en las empresas.

5.1.2 Sistema de gestión de la seguridad de la información. El sistema de gestión de la seguridad de la información SGSI, es sobre lo que se basa principalmente la norma ISO 27001 y es la gestión de la seguridad de la información en las empresas, que consiste en un proceso documentado y debe ser conocido por toda la empresa.

5.1.2.1 Información. Según Idalberto Chiavenato, información "es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones"[1]

[1] Del libro: «Introducción a la Teoría General de la Administración», Séptima Edición, de Chiavenato Idalberto, McGraw-Hill Interamericana, 2006, Pág. 110

Para Ferrell y Hirt, la información "comprende los datos y conocimientos que se usan en la toma de decisiones" [2]
Según Czinkota y Kotabe la información "consiste en datos seleccionados y ordenados con un propósito específico" [3]

Teniendo en cuenta los conceptos anteriores de distintos autores se puede indicar que la información es un conjunto de datos ordenados y seleccionados con un fin determinado y lista para su uso.

En la actualidad la información ha tomado una gran importancia ya sea para las organizaciones como a nivel personal, es por esto que se ve la necesidad de preservarla y asegurarla es allí donde toma importancia el SGSI, ya que este sistema permite a las empresas de una forma sistémica y ordenada implementar las medidas necesarias para asegurar la información a través de la norma ISO 27001, según esta norma el SGSI debe resguardar los principios fundamentales de la seguridad informática, la confidencialidad, integridad y disponibilidad.

5.1.2.2 Norma ISO 27001. La primera revisión de La norma ISO 27001 se publicó en 2005 que fue desarrollada en la base de la norma británica BS 7799-2, la última revisión se publicó el 25 de septiembre de 2013 siendo ahora su nombre completo ISO/IEC 27001:2013, esta norma brinda una metodología para la implementación del SGSI en cualquier tipo de organización o empresa, también permite que sea certificada, garantizando que la organización implemento el SGSI cumpliendo con esta norma.

La Norma ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información, es por esto que cada vez más empresas se certifican a nivel mundial.

La siguiente tabla emitido por ISO nos muestra el top de los 10 países con más certificaciones hasta el 2016.

[2] Del libro: «Introducción a los Negocios en un Mundo Cambiante», Cuarta Edición, de Ferrell O. C. y Hirt Geoffrey, McGraw-Hill Interamericana, 2004, Pág. 121.
[3] Del libro: «Administración de Mercadotecnia», Segunda Edición, de Czinkota Michael y Kotabe Masaaki, International Thomson Editores, 2001, Pág. 115.

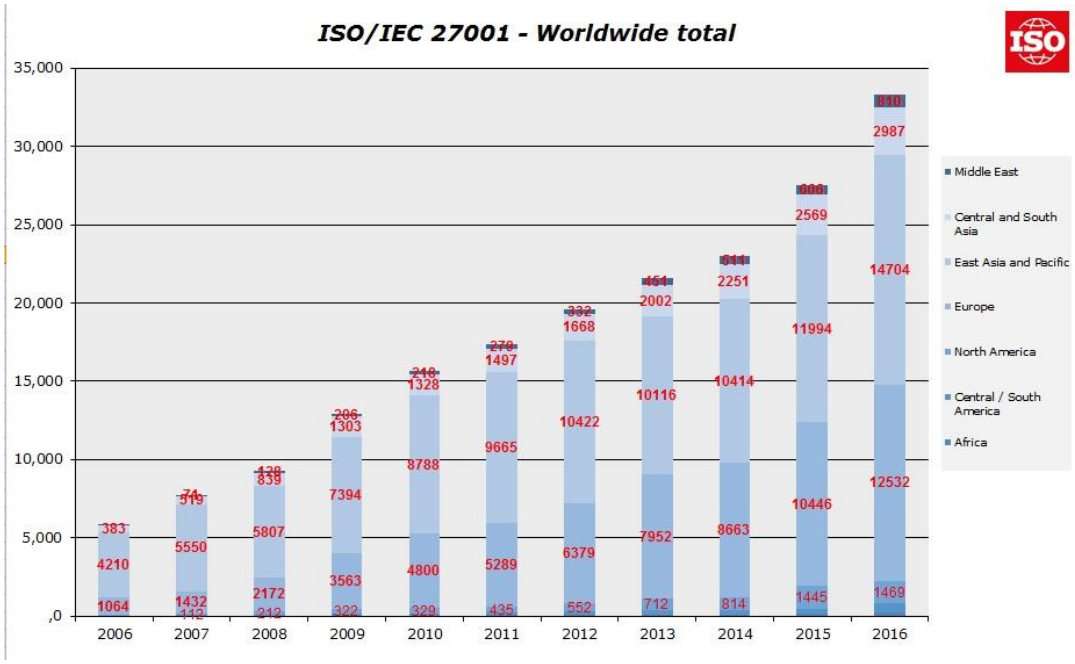
Tabla 1: El top de los 10 países con más certificaciones hasta el 2016.

Top 10 countries for ISO/IEC 27001 certificates – 2016		
1	Japan	8945
2	United Kingdom	3367
3	India	2902
4	China	2618
5	Germany	1338
6	Italy	1220
7	United States of Amerdica	1115
8	Taipei, Chinese	1087
9	Spain	752
10	Netherlands	670

Fuente: El portal de ISO 27001 en Español

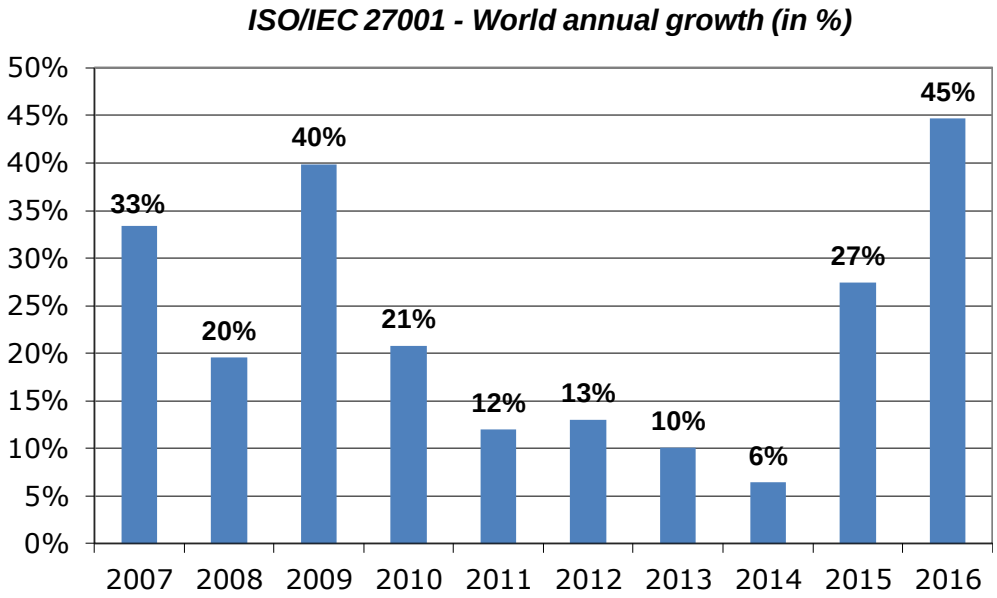
Allí se puede identificar que Japón es el país con mayor número de certificaciones con un total de 8945, seguido por Reino Unido con 3367, he india con 2902.

Figura 1: Total mundial



Fuente: El portal de ISO 27001 en Español

Figura 2: Crecimiento anual mundial



Fuente: El portal de ISO 27001 en español

En estas figuras se identifica el crecimiento anual en la cantidad de las certificaciones de la Norma ISO 27001 a nivel mundial. Según los datos entregados por ISO hasta el 2016 Colombia ha obtenido 163 certificaciones y 257 sitios[4].

La norma ISO 27001 se basa en la gestión de riesgos, identificar donde está el riesgo y tratarlo a través de medidas que son presentadas como políticas e implementarlas, es por esto y en vista que para implementarlo se gestionaran diversas políticas, ISO unió todo esto en dentro del SGSI que no solo trata de la seguridad de las TIC, sino que también tiene en cuenta la gestión de procesos, los recursos humanos, protección legas y física etc.

5.1.2.3 ¿Porque es importante la implementación de la Norma ISO 27001***?*** La implementación de la Norma ISO 27001 toma cada vez más fuerza debido a su importancia dentro de las organizaciones, permitiéndoles tener una mejor estructura ya que deben dedicar un poco de tiempo en la definición de sus procesos y procedimientos lo que les permitirá a futuro ahorrar tiempo de sus trabajadores ya que estos procedimientos no serán únicamente los referentes a la seguridad si no sus procesos en general, además les permitirá ahorrar dinero ya que con la implementación de la norma se identificaran los riesgos de seguridad evitando los posibles incidentes que se puedan presentar y de esta manera

[4] EL PORTAL DE ISO 27001 EN ESPAÑOL. {En línea}. {Consultado el 22 de Agosto de 2017} Disponible en: http://www.iso27000.es

ahorrar dinero, debido a que el costo de la implementación de la norma será menor al que puede llegar a tener en una emergencia de seguridad. Por otra parte, si sus clientes saben que la empresa está certificada en la norma les permitirá tener más confianza frente a sus competidores, además le permitirá cumplir con todas las leyes relacionadas con la seguridad como sobre la información personal, propiedad intelectual etc., ya que la norma le permite cumplir con todas ellas.

Otros beneficios que se pueden tener en cuenta serían: aumentar la seguridad de los productos tecnológicos que poseen y que puedan llegar a adquirir, reduce los riesgos frente al manejo de la información ya que los riesgos y controles son permanentemente revisados, las auditorías externas permitirán identificar las posibles debilidades de SGSI y lo que se debe mejorar, si se implementa la norma en caso de presentarse un incidente se puede garantizar que su negocio siga.

5.2 MARCO CONCEPTUAL.

5.2.1 Seguridad informática. Ya que la tecnología a incursionada cada vez más nuestras vidas, nos permite informarnos, entretenernos, relacionarnos, comprar, vender, trabajar, aprender etc., ayuda al mejor funcionamiento de las empresas y organizaciones, así mismo nos volvemos más vulnerables, es por esto que es necesario ser responsables con el uso de esta tecnología desde donde estemos, por esto es preciso conocer y aprender sobre los riesgos a los cuales estamos expuestos, para poder tomar las medidas necesarias de protección es allí donde surge este concepto de seguridad informática que es básicamente las practicas que llevamos a cabo para proteger y resguardar el funcionamiento de los computadores o equipos electrónicos y la información que contengan. Podemos decir que Seguridad informática es la investigación, normas, procedimientos, métodos, técnicas y las políticas de protección de los datos que nos permita que el sistema de información pueda estar seguro y confiable, cuyo objetivo es garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que se encuentre en estos sistemas de información.

Como nos expone el libro seguridad informática de la editorial Editex S.A por más medidas de seguridad que se apliquen siempre tenemos un margen de riesgo, es por esto que es necesario conocer muy bien el sistema, sus componentes, y posibles peligros para determinar las medidas que se pueden implementar para contrarrestarlos.[5]

[5] AGUILERA LOPEZ. Seguridad informática: Madrid: Editex, S.A, 2010. 240 p

Se debe tener claro que todos los elementos que hacen parte del sistema de información pueden ser afectados por cualquier falla de seguridad que se pueda presentar, se puede hablar de daños a la infraestructura física, así como a la información almacenada, ambos factores son muy importantes y pueden ocasionar grandes pérdidas a las organizaciones o empresas que se puedan ver afectadas.

Tenemos dos tipos de seguridad según nos expone el libro Seguridad informática de la editorial Editex:

- Activas: que son esencialmente un conjunto de medidas con el objetivo de evitar o reducir los riesgos.
- Pasivas: que son fundamentalmente las medidas que se toman luego de ya producido el daño para intentar minimizarlo.

Para que un sistema de información se encuentre de alguna manera seguro sabiendo que nunca estará 100% seguro, es que cumpla con las propiedades de Disponibilidad y accesibilidad, integridad, confidencialidad, responsabilidad y confiabilidad de la información.

Según el Autor Javier Areitio en su libro seguridad de la información plantea que la disponibilidad y accesibilidad debe ser solo para uso autorizado, teniendo la información puntual y con prontitud para los usuarios que la puedan requerir, la disponibilidad protege los datos de un posible borrado no autorizado o de la utilización de estos de forma no autorizada además dice que la disponibilidad puede llegar hacer un factor muy importante en la organización.

Es por esto que en la mayoría de las organizaciones se cuentan con niveles de usuarios para determinar las funciones especificar y así saber a qué tipo de información puede acceder.

El Autor plantea que la integridad de datos es la garantía de que la información no haya sido alterada por usuarios no autorizados se pueden identificar dos formas de integridad una la integridad de datos, que es como ya se dijo la de garantizar que los datos no hayan sido alterados y la integridad del sistema, que es esencialmente cuando el sistema realiza la función que se desea.

La confidencialidad de datos y de la información del sistema según este mismo autor es principalmente que la información privada no se rebele a autores no permitidos.[6]

[6] AREITIO, Javier. Seguridad De La Información: Redes Informática y Sistemas de Información. Madrid: Paraninfo S.A, 2008. 567 p.

Esto es muy importante dentro de una organización ya que en caso de que este falle puede causar pérdidas irreparables como por ejemplo la pérdida de la confianza de los clientes ya que se pueden perjudicados sus datos.

Otro objetivo muy importante es La responsabilidad a nivel individual, nos dice el autor que este es un requisito de la política de la organización para poder tomar medidas de forma individual por parte de la organización.
Por ultimo habla de La confiabilidad, que es elementalmente la garantía de que los objetivos anteriores se cumplan y que todas las medidas implementadas para proteger el sistema y la información sean confiables.

5.2.2 Vulnerabilidades. Se refiere a una serie de características que puedan llevar a sufrir algún daño, es sinónimo de debilidad, es decir que esta propensa a sufrir algún daño y tendrá dificultades para recuperarse posteriormente.

A medida que aumente el uso de tecnología también aumentan las Vulnerabilidades, con base en el informe sobre "el fraude financiero: la amenaza que a las empresas les gustaría prevenir a toda costa" de Kaspersky Lab el 60% de las empresas en admitió al menos un incidente de seguridad informática, también menciona que la perdida de dinero debido a ataques cibernéticos es un tema que debe ser tenido en cuenta ya que muchas empresas van un paso atrás y no se están tomando medidas para protegerse.[7]

Las vulnerabilidades están directamente relacionadas con las amenazas, sino existe una amenaza no existe una vulnerabilidad.

5.2.3 Amenazas. Es principalmente la posibilidad de que ocurra algún evento que pueda causar un daño, en la seguridad informática, estas amenazas serian directamente a algún elemento de la red de información, o específicamente donde se encuentre la información, estas amenazas pueden ser de origen interno u origen externo, un ejemplo de las amenazas de origen externo puede ser un evento natural o un ataque de alguna persona externa, un ejemplo de una amenaza de origen interno puede ser causado por el mismo personal de la organización que comete una negligencia. Hay amenazas como los virus que son muy difíciles de controlar y por esto es tan necesario prevenirlas para lograr contrarrestarlas o minimizar los daños ya que una amenaza surge debido a una vulnerabilidad.

[7] INFORME SOBRE FRAUDE FINANCIERO KASPERSKY NOVIEMBRE DE 2015. {En línea}. {Consultado el 12 de Septiembre de 2017} Disponible en: https://latam.kaspersky.com/about/press-releases/2015_kaspersky-lab-publica-informe-sobre-el-fraude-financiero-la-amenaza-que-a-las-empresas-les-gustaria-prevenir-a-toda-costa.

5.2.4 Delito informático. Delitos relacionados con los computadores, como robo, fraudes, falsificaciones, estafa, etc. Son conductas ilícitas, en Colombia cada año va en crecimiento el número de delitos informáticos según el último estudio de Symantec 4 de cada 10 usuarios de internet son víctimas de delitos informáticos, además según David Kummers, especialista en seguridad de redes de Certicámara en Colombia los daños por cibercrimen en el año pueden alcanzar 917.000 millones de pesos esto incluye no solo la perdida sino el reparar el daño. La ventaja con la que cuenta Colombia actualmente es que es uno de los países que más rápido ha adoptado la regulación para evitar los delitos.[8]

5.2.5 Tipos de delitos informáticos. Las Organización de las Naciones Unidas ONU define tres tipos de delitos informáticos:

- Fraudes cometidos mediante manipulación de computadoras.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos computarizados.

Dado los cambios en la sociedad, la digitalización de la información y globalización de las redes informáticas, además notando en riesgo de que se cometieran delitos cibernéticos y la necesidad de proteger las tecnologías de la información en búsqueda de prevenir hechos que afectaran la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y redes de información siendo los principios fundamentales de la seguridad informática, En el año 2001 se firmó en Budapest el convenido “Convenio de Ciberdelincuencia del Consejo de Europa”

Título I - Delitos contra la confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos.

- Art. 2: Acceso ilícito
- Art. 3: Interceptación ilícita
- Art. 4: Interferencia en los datos
- Art. 5: Interferencia en el sistema
- Art. 6: Abuso de los dispositivos

Título II - Delitos informáticos.

- Art. 7: Falsificación informática
- Art. 8: Fraude informático

Título III - Delitos relacionados con el contenido.

[8] CIO AMERICA LATINA {En línea}. {Consultado el 15 de noviembre de 2017} Disponible en: http://www.cioal.com/2016/09/08/delitos-ciberneticos-en-colombia/

- Art. 9: Delitos informáticos relacionados con la pornografía infantil.

Título IV - Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

- Art. 10: Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. [9]

En la legislación colombiana la ley 1273 de 2009 se tipifico y clasifico los delitos informáticos relacionados con el manejo de los datos personales, apropiarse de patrimonio de terceros a través del uso de la tecnología esta ley modifico el código penal. Ver Marco Legal.

5.2.6 Virus Informático. En 1983 surgen los virus y el Dr. Fred Cohen le dio el nombre de "Virus informático" que se trata básicamente de un programa que tiene la facultad de copiarse y cumple con ciertas acciones, cuando un archivo está infectado por un virus, esta copia las líneas de código infectadas al código original del programa, por consiguiente, coda que el archivo o programa se ejecuta el virus se activa.

Inicialmente el virus no tenía la propiedad de difundirse en los computadores conectados a internet o una red, pero con los años los programadores lograron que así fuera. En 1884 se hizo pública la existencia de los virus a través de la publicación de la revista estadounidense "Scientific American", los virus fueron evolucionando en 1986 se creó el virus "Stoned" que dañaba definitivamente el sistema operativo, lo que ocasionaba la pérdida total de la información, en 1989 nace el virus "Dark avenger" que causaba un daño lento al sistema operativo; viendo la necesidad de contrarrestar estos virus en 1988 IBM comercializo en primer antivirus, siendo la creación de antivirus un gran negocio durante el siglo XXI, ya los virus se volvían cada vez más dañinos, ocasionando daños no sola al software sino al hardware como por ejemplo a los discos duros. En 1999 con el uso del programa Outlook se le da cabida a la creación de virus a través de correos electrónicos, ocasionando daños económicos, en el año 2000 nace el famoso virus llamado "I love you" siendo para esa época el virus que más perdidas económicas causo a las empresas de software.

A través de los años han ido avanzando la creación de virus que no solo pueden causar daños, sino que además se encargan de bombardear con publicidad que se ha convertido en un negocio muy rentable en la actualidad.

[9] CONVENIO SOBRE LA CIBERDELINCUENCIA. {En línea}. {Citado el 26 de Septiembre de 2017} Disponible en: http://www.cienciaspenales.net/files/2016/10/1.-CONVENIO-DEL-CONSEJO-DE-EUROPA-SOBRE-CIBERDELINCUENCIA.pdf

5.2.7 Antivirus. Los antivirus son programas informáticos cuyo propósito es detectar virus y eliminarlos antes o después de que ingresen al sistema, además de otros programas que puedan llegar a perjudicar, el antivirus debe estar correctamente configurado para que logre cumplir con su propósito, este puede ser una solución que minimiza los riesgos pero no es definitivo es muy importante mantenerlo actualizado, en la actualidad existen múltiples antivirus, que buscan minimizar los riesgos y cada vez son más efectivos ya que son direccionados a las necesidades específicas, ANTIVIRUS HEURISTICOS, ANTISPYWARE, ANTISPAM etc.

5.2.8 Riesgos informáticos. Según la Organización Internacional de Normalización ISO define riesgo tecnológico como: "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños".

Teniendo en cuenta la definición anterior de riesgos informáticos es muy importante que las organizaciones tomen las medidas necesarias para evitas esas amenazas o vulnerabilidades en la búsqueda de minimizar los riesgos que se puedan presentar.

Según la norma ISO 27001 el riesgo es el resultado de realizar un análisis de los riesgos y el análisis de riesgos en un proceso cuyo objetivo es obtener un valor que nos permita la toma de decisiones con respecto a seguir o no con el proceso.

Se pueden presentar distintos tipos de riesgos:

- Riesgo calculado: este se define de acuerdo al cálculo de la vulnerabilidad y el impacto que puede producir esto con el fin de tomar una decisión.
- Riesgo residual: este se define al momento de haber disminuido el riesgo, al aplicar medidas correctivas reales o simuladas.
- Umbral de riesgo: es el valor que se establece como referencia en la toma de decisiones para comparar con el calculado del riesgo.
- Riesgo intrínseco: Se define al momento en que se eliminan las acciones correctivas y preventivas.

Según la Norma ISO 27001 se debe tener en cuenta dos atributos del riesgo, restricción del riesgo y la propagación del riesgo.[10]

[10] EL PORTAL DE ISO 27001 EN ESPAÑOL. {En línea}. {Consultado el 22 de Agosto de 2017} Disponible en: http://www.iso27000.es/faqs.html#seccion1

5.2.9 Robo de información. Actualmente las empresas se encuentran expuestas a muchas ataques ya sean internos o externos que pueden crear gran pérdida de información que puede llegar a afectar económicamente a las organizaciones, es por esto de la importancia de proteger la información ya que los problemas no pueden llegar a ser solo técnicos, sino durante todo la transmisión de la información que puede ser por falta de cultura o conocimiento de la seguridad de la información, es allí donde los hacker o crackers pueden llegar a tomar poder la de información robándola o como es una práctica actual secuestrándola mediante el método de “ransomware” que es una práctica donde se secuestra la información de la organización y se pide a cambio una suma de dinero para lograr recuperarla.

5.3 MARCO LEGAL.

Es cada vez más común los ataques informáticos en Colombia lo que afecta la seguridad de la información en las empresas es por esto que se hace necesario en el país conocer y cumplir con la legislación relacionada con la seguridad informática.

Actualmente contamos con la legislación correspondiente a los derechos de autor:
Decisión 351 de la CAN: Se presenta para reconocer los derechos del autor y dar protección sin distinguir el tipo de arte.

Ley 23 de 1982: Esta ley es básicamente sobre los derechos de autor, presenta toda la regulación correspondiente a los derechos de autor en Colombia.

Ley 44 de 1993: Esta modifica la Ley 23 de 1982 y la ley 29 de 1944, se adicionan nuevas disposiciones como el soporte lógico (Software).

Ley 545 de 1999: Por la cual se aprueba “Tratado de la OMPI -Organización Mundial de la Propiedad Intelectual- sobre Interpretación o Ejecución y Fonogramas (WPPT)" que contempla los derechos de propiedad intelectual de los artistas cantantes músicos, los productores etc., que tengan responsabilidad de los sonidos interpretación o ejecución.

Ley 603 de 2000: Por la cual se modifica el artículo 47 de la Ley 222 de 1995.

Contamos demás con la legislación con respecto comercio electrónico y firmas digitales:

Ley 527 de 1999: esta ley reglamenta principal el acceso y uso de mensajes de datos y comercio electrónico y de las firmas digitales, esta ley se divide en dos partes, primero permite el uso de información o datos para el comercio electrónico, firmas digitales, mensajes de datos por medio escrito y digital, también permite la certificación de las personas naturales y jurídicas para realizar transacciones

electrónicas, pero además da reconocimiento legal a los documentos electrónicos como si fueran físicos y pueden ser parte de un proceso legal.

Decreto 1747 de 2000: por la cual se reglamenta la Ley 527 de 1999.
Resolución 26930 de 2000: "Por la cual se fijan estándares para la autorización y funcionamiento de las entidades de certificación y sus autores"[11]

También tenemos leyes de protección de datos personales:

Ley 1581 de 2012: Esta ley dicta disposición sobre la protección de datos personales. Se trata básicamente de reconocer el derecho que tiene toda persona de conocer, actualizar y rectificar los datos que se hayan recogido sobre cada una en bases de datos, así como reconocer el derecho constitucional referido en el artículo 15 de la constitución política de Colombia que se refiere principal al derecho a la intimidad y el artículo 20 que se refiere al derecho de informar y recibir información veraz.

Ley 1266 de 2008: en la cual se dictan disposiciones del hábeas data y se regula la información el manejo de la información que está contenida en las bases de datos especialmente financieras y crediticias.

Ley 1273 de 2009: Esta ley añade dos capítulos al código penal colombiano, el Capítulo 1: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas de informáticos, Capitulo 2: De los atentados informáticos y otras infracciones, esta ley está muy atada a la ISO 27000, lo que permite al país estar en la vanguardia en la legislación de seguridad informática.

CAPITULO. I

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva.

CAPITULO. II

[11] RESOLUCIÓN 26930 DE 2000. {En línea}. {Citado el 16 de Septiembre de 2017} Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5793

- Artículo 269I: Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos.
- Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:
- Artículo 58. Circunstancias de mayor punibilidad.
- Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:
- Artículo 37. De los Jueces Municipales.[12]

[12] LEY 1273 DE 2009. {En línea}. {Citado el 26 de Septiembre de 2017} Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

6. ESQUEMA TEMATICO

6.1 CAPITULO I: ELEMENTOS BASICOS ACERCA DE LA IMPORTANCIA DE LA SEGURIDAD INFORMATICA EN LAS ORGANIZACIONES EN COLOMBIA

La seguridad informática tiene sus inicios a principios de los años 80, que realmente fue el inicio de las redes informáticas, cuando se identificó que al tener varios equipos conectados en lugares diferentes eran más vulnerables, por esto surge la necesidad de que las personas conocieran como protegerse y se certificaran en buenas practicas, conocimiento común, valores y ética para la seguridad informática, viendo esta necesidad se forma (ISC) en 1989 Información Campo De La Seguridad que se encargó de estandarizar y certificar estas buenas prácticas de seguridad informática.

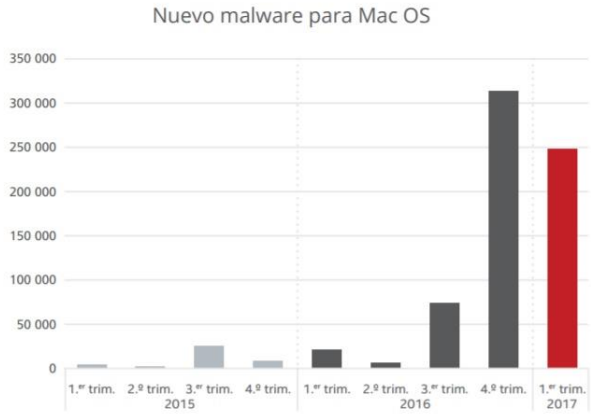
En 1983 surgen los virus y el Dr Fred Cohen le dio el nombre de "Virus informático" que se trata básicamente de un programa que tiene la facultad de copiarse y cumple con ciertas acciones, cuando un archivo está infectado por un virus, esta copia las líneas de código infectadas al código original del programa, por consiguiente, cada que el archivo o programa se ejecuta el virus se activa. Inicialmente el virus no tenía la propiedad de difundirse en los computadores conectados a internet o una red, pero con los años los programadores lograron que así fuera. En 1984 se hizo pública la existencia de los virus a través de la publicación de la revista estadounidense "Scientific American", los virus fueron evolucionando en 1986 se creó el virus "Stoned" que dañaba definitivamente el sistema operativo, lo que ocasionaba la pérdida total de la información, en 1989 nace el virus "Dark avenger" que causaba un daño lento al sistema operativo; viendo la necesidad de contrarrestar estos virus en 1988 IBM comercializo en primer antivirus, siendo la creación de antivirus un gran negocio durante el siglo XXI, ya los virus se volvían cada vez más dañinos, ocasionando daños no sola al software sino al hardware como por ejemplo a los discos duros. En 1999 con el uso del programa Outlook se le da cabida a la creación de virus a través de correos electrónicos, ocasionando daños económicos, en el año 2000 nace el famoso virus llamado "I love you" siendo para esa época el virus que más perdidas económicas causo a las empresas de software.[13]

A través de los años han ido avanzando la creación de virus que no solo pueden causar daños, sino que además se encargan de bombardear con publicidad que se ha convertido en un negocio muy rentable en la actualidad.

[13] AGUILERA LOPEZ. Seguridad informática: Madrid: Editex, S.A, 2010. 240 p.

Según el último reporte de amenazas cibernéticas de la firma de seguridad McAfee “incluso los Mac han dejado de ser invulnerables a virus y otras formas de malware”[14] esencialmente son afectados por el programa malicioso “adware” que busca principalmente mostrar publicidad mientras se navega por internet cuyo objetivo principal del atacante es obtener ganancias de la publicidad digital. Para el año pasado se registraron 460.000 programas maliciosos para Mac y para otras plataformas 630 millones de piezas de malware en especial para Windows y Android.

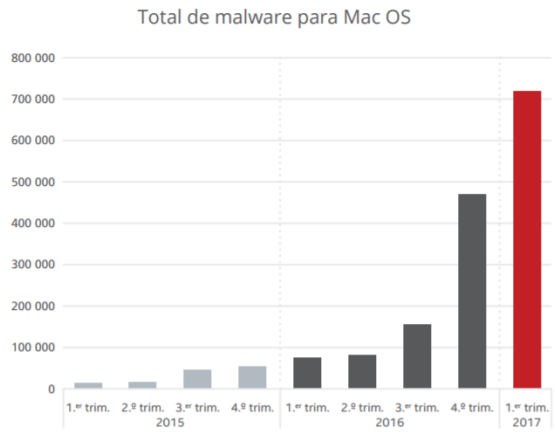
Figura 3: Nuevo malware para Mac OS



Fuente: McAfee Labs, 2017

[14] INFORME DE MCAFEE LABS SOBRE AMENAZAS JUNIO DE 2017. {En línea}. {Consultado el 12 de Septiembre de 2017} Disponible en: https://www.mcafee.com/es/resources/reports/rp-quarterly-threats-jun-2017.pdf

Figura 4: Total malware para Mac OS



Fuente: Mcafee Labs, 2017

Otra amenaza que tiene actualmente Mac es una pieza de “ransomware” que se distribuía a través del cliente de BitTorrent Transmission, este permite que los atacantes puedan secuestrar los datos del equipo y pedir dinero a cambio de liberarlos.

La seguridad informática ha tenido una evolución constante en las últimas décadas dado a la importancia que ha tomado la información en las organizaciones convirtiéndose en un don preciado; en los años 90 la seguridad física se centró en resguardar el bien físico, como los equipos y las instalaciones, evitando los posibles daños que podían sufrir los centros de cómputo, luego se dio lugar a la seguridad lógica que era entendida como proteger los equipos de cómputo y los sistemas operativos, esto solo desde el sentido puramente técnico entendido como que estos dejaran de funcionar correctamente, con la aparición de los virus se entendió que era necesario proteger la información almacenada y procesada, es así como se comprendió que era necesario generar restricciones para el acceso a la información y el manejo de la misma.

Posteriormente con la llegada del internet y la posibilidad de estar conectados se hace necesario para las organizaciones la conectividad a través de redes, ocasionando mayor vulnerabilidad en los sistemas de información y las redes de comunicaciones, lo que con lleva a la utilización de nuevos equipos como firewall para controlar la seguridad a nivel periférico.

Para ese momento los posibles atacantes no buscaban más allá de afectar un sistema mediante un virus o conseguir mostrar sus habilidades para acceder a algún sitio sin buscar ningún lucro, pero en la actualidad este perfil ha cambiado ya que lograron descubrir el valor que puede llegar a tener la información para una organización, es por esto que ya son grupos organizados con personal especializado en distintos tipos de ataques para obtener información, esto hace

que el concepto de seguridad informática cambie y evolucione hacia el concepto de seguridad de la información que permite generar políticas de seguridad aliadas con los planes estratégicos de las organizaciones.

La globalización y el uso del internet han permitido que los delincuentes puedan operar desde cualquier país, multiplicando sus actividades delictivas a nivel mundial, el uso y el incremento de nueva tecnología disponible afecta a las victimas ya que no se cuenta con el respectivo conocimiento o información de cómo protegerse y los atacantes cuentan con mayor tecnología para realizar sus ataques.

Por otro lado, es cada vez más común el mercado negro de la información donde los atacantes buscan bases de datos con información personal que pueden comercializar lo que hace más atractivo el hecho de robar la información para obtener un lucro.

Según el informe sobre ciberseguridad de Norton 2016, el 35% "de la población mundial tiene como mínimo un dispositivo sin proteger y en el 2015 los cibercriminales lanzaron más de un millón de ataques web contra usuarios de internet por día." [15] Estos datos nos permiten realizar una mirada de cómo está avanzando a pasos agigantados la delincuencia informática y está tomando cada vez más fuerza debido a que se ha convertido en un negocio muy lucrativo y nos damos cuenta que no estamos preparados para contrarrestarlo.

Según el Informe sobre las amenazas para la seguridad en internet de 2017 de Symantec el año 2016 [16], se presentaron ataques fuera de lo normal entre ellos los ataques virtuales donde desfalcaron millones de dólares uno de los más importantes fue durante el proceso electoral de estados unidos donde se pretendió alterar dicho proceso grupos que fueron patrocinados por otros países interesados en intervenir, este informe además hace ver que las vulnerabilidades van más allá de un malware para llevarnos a estar vulnerables ante el espionaje o sabotaje.

Este informe es una prueba de que los ataques son cada vez más fuertes y con fines ambiciosos, lo que nos debe llevar a dejar atrás el miedo solo a los virus o malware, para llevarnos a aplicar políticas claras e efectivas en las organizaciones para contrarrestar cualquier tipo de ataque.

---

[15] INFORME SOBRE CIBERSEGURIDAD DE NORTON 2016. {En línea}. {Consultado el 11 de Septiembre de 2017} Disponible en: https://mx.norton.com/cyber-security-insights-2016

[16] INFORME SOBRE LAS AMENAZAS PARA LA SEGURIDAD EN INTERNET DE 2017 DE SYMANTEC. {En línea}. {Consultado el 11 de Septiembre de 2017} Disponible en: <https://www.symantec.com/es/mx/security-center/threat-report?inid=symc-home-page_ghp_to_security-center_threat-response.html
AGUILERA LOPEZ. Seguridad informática: Madrid: Editex, S.A, 2010. Pág. 9 y10

El centro de prensa de ESET da un resumen de los 10 incidentes más importantes hasta enero de este último año, uno de ellos es el ataque a DDoS (ataque distribuido de denegación de servicio) que afectaron a muchos sitios web entre ellos Twitter, Netflix, PayPal, Pinterest y PlayStation Network, otro fue a Tesco Bank la filial bancaria de la cadena de supermercados británica en noviembre de 2016 lo que ocasionó la perdida de dinero a cerca de 9 mil clientes; en junio de este mismo año un cibercriminal de apodo "Peace" hizo públicas más de un billón de contraseñas de LinkedIn, Twitter, Tumblr, VK y MySpace; otro de los incidentes presentados afecto a Yahoo! en septiembre con lo se denominó "la brecha más grande en la historia" donde la compañía perdió cerca de 500 millones de datos personales de sus clientes, en diciembre el jefe de segura de esta compañía informo que este no sería el único ataque que han recibido ya que según dijo en el 2013 mil millones de cuentas fueron afectadas con el robo de información personal. En octubre de 2016 los investigadores de ESET descubrieron un exploit kit llamado Stegano que se propagaba a través de banners publicitarios, a través de Internet Explorer que escaneaba los computadores buscando vulnerabilidad en Flash Player para explotarlas; en ucrania se presente un ataque en la industria energética en el mes de diciembre de 2016, a través de correos electrónicos con adjuntos maliciosos.

ESET también alerto sobre los ataques que apuntan a los Routers con contraseñas por defecto, que entre más dispositivos estén conectados los riesgos aumentan. Otro de los ataques que se encuentra en este ranking en el que se comprometieron base de datos del Departamento de Justicia EE.UU, los atacantes publicaron datos de 10 mil empleados del Departamento de Seguridad Nacional y de 20 mil empleados del FBI esto demuestra que las organizaciones gubernamentales están también expuestas a incidentes de seguridad, uno de los ataques más importantes que se presentó el año anterior fue contra la Comisión Filipina de Elecciones (COMELEC) donde a través de un acceso no permitido se perdió toda la información personal de los votantes de filipinas equivalente a más o menos 55 millones de personas.[17]

Uno de los ataques que han tomado más fuerza en el 2017 es el ransomware este consiste en el secuestro de información, los primeros brotes se presentaron en Ucrania, este ataque cifra el sector de arranque y se propaga automáticamente, las recomendaciones de los expertos es actualizar los sistemas operativos, soluciones de seguridad y educar a los usuarios, además es importante mantener siempre un Backup de la información; esta amenaza es una de las más preocupantes de los últimos tiempos, junto con denegar el acceso a datos y

[17] CENTRO DE PRENSA ESET {En línea}. {Consultado el 29 de Septiembre de 2017} Disponible en: http://www.eset-la.com/centro-prensa/articulo/2017/los-10-incidentes-seguridad-mas-importantes-del-ultimo-a%C3%B1o/4439

sistemas (con ataques de Denegación de Servicio Distribuido o DDoS) y el de infectar dispositivos que forman parte de la Internet (IoT).

En el último año casi la mitad de las empresas de Latinoamérica sufrieron una infección de malware siendo los correos electrónicos el medio más usado por ser masivo y económico.

Colombia no se queda atrás con respecto a estos ataques ya que según Camilo Gutiérrez especialista en seguridad informática de ESET solo el 36% de las empresas en Colombia realizan auditorias de seguridad, el 46,7% de las empresas en Colombia sufrieron algún incidente de seguridad durante el último año.[18]

El Ministerio TIC, el Centro Cibernético Policial CCP y colCERT, a través de la página de la policía nacional genera una alerta el día 12 de mayo de 2017 donde recomiendan a las entidades del estado para mayor seguridad actualizar sus sistemas operativos en las estaciones de trabajo y servidores, con el fin de mantener actualizados sus parches, esto debido a la filtración de una serie de exploit aplicables a las siguientes versiones de sistemas operativos: Windows: Xp, Vista, 7, 8, 10, 2000, 2003, 2008, 2012. Que afecta los servicios (tcp/445) SMB/ (tcp/139) NBT. También invitan a las entidades a realizar avances en la implementación de los modelos de seguridad y privacidad de la información, además dan una serie de recomendaciones como: no cliquear enlaces desconocidos en los correos electrónicos, no responder mensajes con información personal o financiera, tomar medidas de control contra malware, o cualquier software malicioso además de realizar las pruebas adecuadas de vulnerabilidad en los sistemas de información, también recomiendan realizar Backup periódicamente, mantener actualizados los antivirus y evitar ingresar a sitios web desconocidos.[19]

El vicepresidente de Planeación Estratégica de la Sociedad Internacional de Automatización, Yesid Yermanos asegura que en Colombia las fuerzas militares y la policía nacional están preparadas, pero a nivel general el país está en un nivel intermedio de riesgo, asegura que el 40% de las empresas de fabricación no han realizado evaluación de riesgos por ciberataques, además afirma que falta más inversión en el sector privado ya que no se han tomado en serio los daños que pueden causar los ataques cibernéticos o cualquier tipo de amenaza de seguridad informática. En este sentido es evidente que a nivel del sector público se está más

[18] CENTRO DE PRENSA ESET {En línea}. {Consultado el 29 de Septiembre de 2017} Disponible en: http://www.eset-la.com/centro-prensa/articulo/2017/los-10-incidentes-seguridad-mas-importantes-del-ultimo-a%C3%B1o/4439

[19] CSIRT-PONAL {En línea}. {Consultado el 15 de noviembre de 2017} Disponible en: https://cc-csirt.policia.gov.co

preparado, pero en el sector privado falta mucho para asegurar la seguridad informática en el país.[20]

Según la Encuesta Nacional de seguridad informática 2017 realizada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS)[21], con la participación de 128 encuestados, muestra los tipos de incidentes de seguridad que se presentan en las empresas de Colombia actualmente.

Figura 5: Tipos de incidentes.

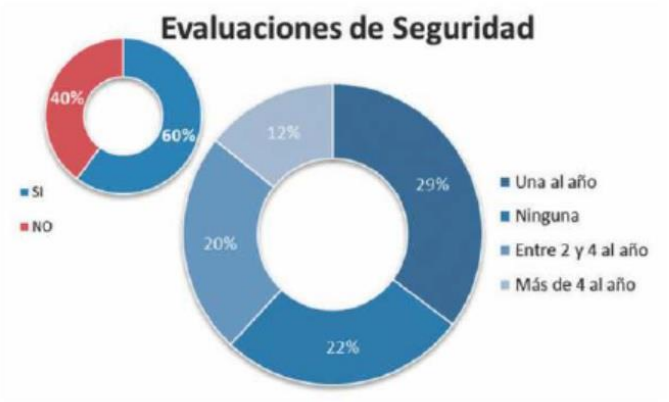
Fuente: Asociación Colombiana de Ingenieros de Sistemas (Acis)

Se identifica que el mayor ataque es de virus con un 43%, seguido por la instalación de software no autorizado 38%, en tercer lugar esta los Phishing con un 34%, seguido por Ransomware con un 20%.

[20] CARACOL RADIO {En línea}. {Consultado el 02 de octubre de 2017} Disponible en: http://caracol.com.co/radio/2017/06/09/nacional/1497042960_148590.html

[21] ENCUESTA NACIONAL DE SEGURIDAD INFORMÁTICA 2017 {En línea}. {Consultado el 02 de octubre de 2017} Disponible en: http://acis.org.co/revista143/content/encuesta-nacional-de-seguridad-inform%C3%A1tica-2017

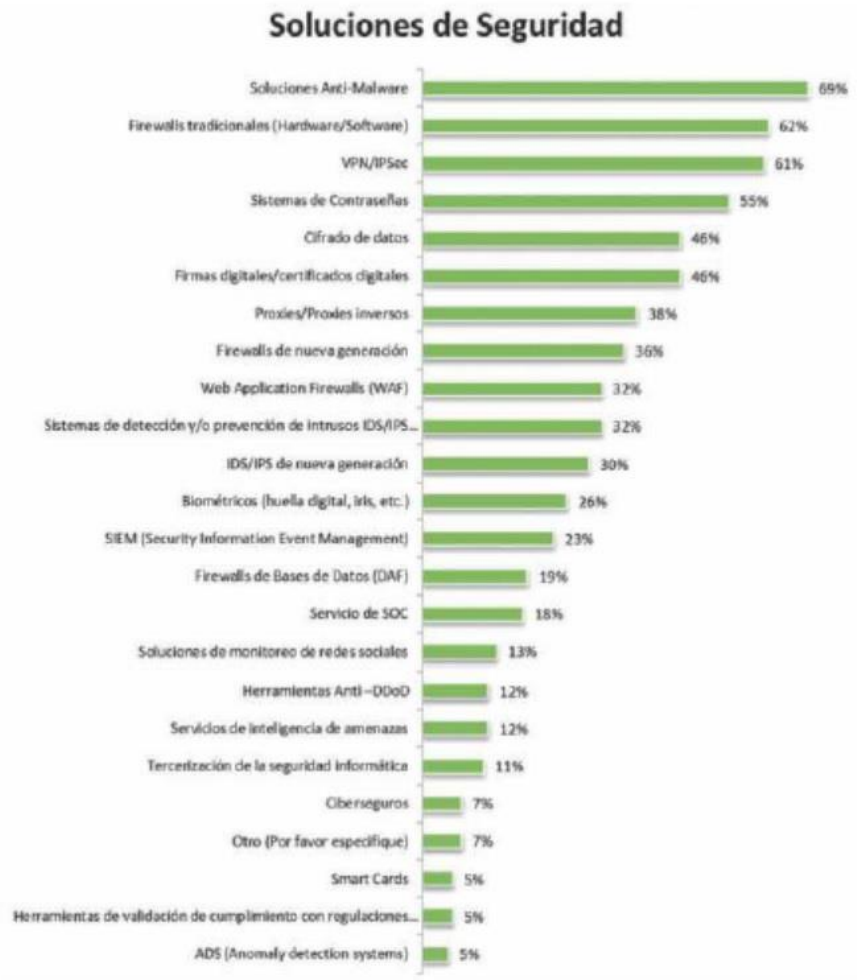
Figura 6: Evaluaciones de seguridad.



Fuente: Asociación Colombiana de Ingenieros de Sistemas (Acis)

Esta grafica nos muestra un panorama mucho mejor con respecto a la evaluación de seguridad, viendo que el 60% realiza evaluaciones de riesgo en las empresas contra un 40% que no lo considera necesario. Del 60% que realizan evaluaciones de riesgo e 29% lo hace cada año.
En esta misma encuesta nos muestran las soluciones de seguridad más utilizadas en las organizaciones encuestadas.

Figura 7: Soluciones de seguridad.

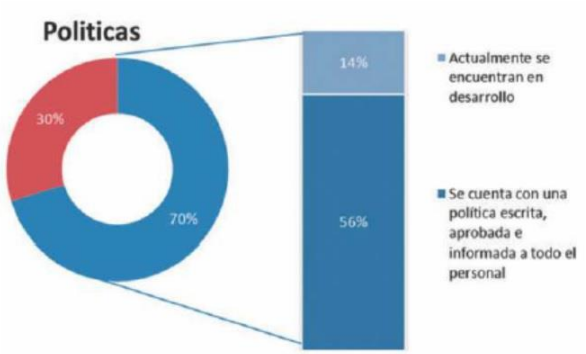


Fuente: Asociación Colombiana de Ingenieros de Sistemas (Acis)

En esta grafica se identifica que la solución más utilizada es el Anti-Marware con un 69%, seguido por los Firewalls tradicionales con un 62%, en un tercer lugar esta las VPN/IPSec con un 61%, en un cuarto lugar sistemas de contraseñas con un 55%, en menor escala se encuentra el cifrado de datos con un 46%, con lo que podemos identificar que las medidas o soluciones de seguridad que se utilizan actualmente son las comúnmente conocidas y más aplicadas en general.

Por otra parte, se muestra el panorama de la aplicación de políticas de seguridad en las organizaciones, donde el 70% de los encuestados afirman tener una política de seguridad en la empresa, frente a 30% indica no tenerla.

Figura 8: Política de seguridad.



Fuente: Asociación Colombiana de Ingenieros de Sistemas (Acis)

De quienes manifiestan tener una política de seguridad el 14% expone que actualmente se encuentra en desarrollo mientras que el 56% ya se encuentra aplicándola.

Se pueden identificar además unos obstáculos que se le presentan a la seguridad informática en las organizaciones.

Figura 9: Obstáculos a la seguridad.

Fuente: Asociación Colombiana de Ingenieros de Sistemas (ACIS)

Donde se identifica que el obstáculo más grande es la falta de cultura en seguridad informática, seguido del apoyo o colaboración entre áreas y poco entendimiento de la seguridad informática.

Se puede concluir frente a todo este análisis que las organizaciones en Colombia se ven enfrentadas cada día a nuevas tecnologías, que pueden por supuesto para mejorar el desarrollo de sus actividades y su rendimiento en general, pero también

se ven cada vez más expuestas a riesgos, por tanto se ven obligadas a tomar medidas de seguridad que permitan reducir sus riesgos, es por ello que aunque el panorama en general de la seguridad informática en Colombia no sea muy desalentador ya que se encuentra en un nivel medio en general, si genera una cierta incertidumbre con respecto a la importancia que se le está dando en general a la seguridad informática en las organizaciones, sobre todo aquellas empresas pequeñas pymes que no gastan gran presupuesto en su seguridad, ya que se ha analizado las empresas grandes o las empresas públicas que en su mayoría han implementado políticas de seguridad, pero las pymes son un blanco atractivo para los delincuentes ya que saben que estas empresas no invierten mucho presupuesto en su seguridad ya que por lo general no el mas de un 8% de su presupuesto, esto es realmente preocupante ya que las pymes en Colombia mueven alrededor de un 96% de la economía del país, y están siendo atacas anualmente alrededor de un 73% de las pymes en Colombia, a través de extraer información de sus correos electrónicos o redes sociales, ataques de Phising, no dejando atrás el robo de información internamente en las empresas donde los mismos empleados pueden robar la información, además con la tendencia actual de que los empleados puedan llevar sus dispositivos portátiles personales, para realizar trabajos y conectarse a la red y recursos corporativos conocido como Bring Your Own Device, o también con el incremento del tele trabajo a puesto más en vilo el tema de la seguridad de la información, por esta y muchas más razones es necesario que las pequeñas y medianas empresas reconozcan la importancia de la seguridad del información y generen más recursos para la implementación de políticas de seguridad en sus organizaciones, ya que los atacantes son inteligentes y sabrán donde atacar.

6.2 CAPITULO II: IMPORTANCIA DE LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LAS ORGANIZACIONES COLOMBIANAS

Basados en el Ítem anterior en el que se analizó el contexto en que se encuentra actualmente la seguridad informática y como ha tomado cada vez más importancia en el mundo, vemos que las organizaciones Colombianas no se pueden quedar atrás, teniendo en cuenta el análisis hecho en este documento, encontramos que las empresas grandes o multinacionales así como las empresas del estado están en alguna medida preparadas para los ataques que se les puedan presentar; en un contexto mundial vemos que su nivel de seguridad es medio, se puede identificar que permanentemente se están actualizando para ir mejorando la seguridad de la información en las organizaciones, esto teniendo en cuenta que nunca se está preparado en un cien por ciento y eso lo sabemos por los ataques que se realizan a diario a nivel mundial; la preocupación se presenta principalmente con respecto a la seguridad informática de las PYMES en Colombia, según lo que hemos podido analizar esto es algo que no podemos dejar de lado ya que como vimos anteriormente las PYMES mueven alrededor de un 96% de la economía del país, y son estas empresas las que más vulnerables se encuentran y esto por supuesto los atacantes los saben, y es necesario de manera urgente promover la implementación de políticas de seguridad informática en estas organizaciones por supuesto mediante la implementación de Sistemas de Gestión de la Seguridad de la Información (SGSI).

Se sabe que los obstáculos más grandes con que se cuentan es la falta de cultura en Seguridad Informática, la falta de colaboración en las empresas, además del poco entendimiento sobre este tema y por supuesto la baja inversión presupuestal de las organizaciones en seguridad.

No se debe desconocer que la información ha sido y será parte de la vida de los seres humanos y por consiguiente es un recurso fundamental en la organizaciones es allí donde parte la importancia de protegerla, aunque anteriormente este información se almacenada en papel, en la actualidad con el avance de la tecnología se encuentra almacenada principalmente en equipos tecnológicos por esta razón es muy importante que las organizaciones implementen un sistema que permita proteger la información, con controles que eviten los posibles intrusos que puedan llegar a causar daño que afecten los recursos de la empresa, por todo los anterior las organizaciones se ven de alguna forma obligadas a implementar el SGSI, que les permita gestionar los riesgos buscando salvaguardar la confidencialidad, integridad y disponibilidad de la información siendo estos los principios fundamentales de la seguridad informática.

De acuerdo a la información que maneje la organización se debe identificar qué tipo de información es, es decir si es publica si es privada y quienes pueden acceder a cada tipo de información, así también identificar a quien le puede interesar cada tipo de información, hackers, crackers, sniffers, curiosos, competidores, enemigos, delincuentes, rivales etc.

Actualmente los ataques son constantes es por esto que se necesita que todos los empleados de la empresa conozcan sobre la seguridad de la información y los encargados del manejo de la información tengan el conocimiento necesario, todos deben conocer que hay múltiples formas de acceder a la información, y que cualquier debilidad puede ser aprovechada por los delincuentes, ya que se pueden identificar múltiples tipos de ataques informáticos.

Lo que busca principalmente un SGSI es definir hacia dónde va la organización en materia de seguridad de la información, identificando los riesgos, para gestionar controles que permitan mantener la confidencialidad, integridad y disponibilidad de la información, basándose en la Norma ISO 27001 ya que esta es la norma que permite la certificación, aunque siempre hay que tener presente que nunca se puede garantizar el 100% de la seguridad, lo que se puede garantizar es minimizar los riesgos o el impacto que pueda llegar a tener el ataque en caso de que ocurra, también evaluar si las medidas fueron positivas.

Todas las organizaciones tienen objetivos principalmente con respecto a su negocio, pero es necesario que todos esos objetivos sean basados sobre el principio de la confiabilidad, como sabemos la información además de estar en los computadores, en la red etc., también se encuentra en las personas que trabajan en la empresa, así como también en la organización en si en la experiencia y demás particularidades que tenga es por esto que es importante el SGSI ya que allí se contempla todo esto, ya que permite mantener todos los riesgos controlados, muchas organizaciones piensan que implementar un SGSI es muy dispendioso y costoso, y solo es posible para grandes multinacionales o bancos, pero el beneficio que trae el SGSI es que es posible implementarlo de acuerdo a cada organización, incluso solo aplicando algunos principios, pero sin dejar de seguir los lineamientos principales, buscando siempre mejorar, basados en observar las medidas de seguridad aplicadas y el resultado obtenido, en la búsqueda de la toma de decisiones adecuadas de manera estratégica.

Se debe siempre tener en cuenta que todo el personal debe conocer el SGSI, además debe ser siempre documentado y este es requisito fundamental para garantizar la administración de la seguridad en una organización, siempre basados en el principio del ciclo de mejora continua PDCA (por las iniciales de Plan, Do, Check y Act),.

Otros beneficios de la implementación de un Sistema de Gestión de la Seguridad de la información son: mejorar la imagen de la organización, disminución del

impacto de los riesgos, mayor confianza por parte de los clientes, contar siempre con un plan de contingencia garantizando la continuidad de la organización, valor agregado a su organización, además del cumplimiento de la ley y las normas.

Lo que exige la norma principalmente es que se cumple con 4 actividades que compararemos en la siguiente tabla con el ciclo de mejora continua Plan, Do, Check y Act.:

Tabla 2: 4 Actividades Principales en el SGSI

	SGSI	CICLO DE MEJORA CONTINUA
1	Establecer el sistema.	Plan (planear o planificar).- En este primer paso se identifica aquello que se quiere mejorar, se recopilan los datos iniciales, se establecen los objetivos esperados y se planifican las actividades a realizar.
2	Implementar y operar el sistema.	Do (hacer o ejecutar).- Lo siguiente es ejecutar las actividades del plan hecho en el primer paso y documentar los resultados.
3	Mantener y mejorar el sistema.	Check (verificar).- Se comparan los resultados obtenidos versus los resultados esperados, que se definieron en el “Plan”.
4	Monitorear y revisar el sistema.	Act (actuar).- El ciclo “termina” haciendo los ajustes necesarios para que se logren, en la medida de lo posible, los objetivos planeados; se revisan las lecciones aprendidas y se reinicia el ciclo completo.

Fuente: El Autor

No necesariamente se debe cumplir con un listado de medidas, lo que se debe tener claro es que se debe preservar la seguridad de la información, y como se basa principalmente en el ciclo de mejora continua debemos garantizar que el sistema avance de lo contrario sabremos que no está bien implementado.

Tabla 3: Certificaciones ISO/IEC 27001 en Suramérica

ISO/IEC 27001 - Central / South America											
Year	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Country	18	38	72	100	117	150	203	272	273	347	564
Argentina	1	1	6	4	8	24	33	40	23	52	88
Barbados				1	1					0	1
Bolivia				1	1	3	1	1	1	1	6
Belize										1	1
Brazil	10	25	40	48	41	50	53	82	85	94	117
Chile	2	3	7	10	13	18	23	24	24	32	49
Colombia	**3**	**8**	**11**	**14**	**23**	**27**	**58**	**82**	**78**	**103**	**163**
Costa Rica			2	5	6	7	7	10	22	4	21
Cuba			1	1	2			0		0	0
Dominican Republic				1	1	2	3	4	3	4	8
Ecuador				1	1	1	3	5	7	6	11
El Salvador					1	1	1	1	1	1	4
Guatemala					1	1	1	2	3	2	5
Guyana				1	1			0		0	0
Honduras						1	1	0	1	0	5
Jamaica				1	1			0		0	10
Panama					1	1	2	1		0	2
Peru	1	1	2	6	9	5	7	9	12	22	32
Puerto Rico			2	2	2	2	2	2		0	2
Saint Lucia										1	1
Saint Vincent and the Grenadines										1	0
Trinidad and Tobago							1	1	1	1	2
Uruguay	1		1	4	4	7	7	8	11	21	28
Venezuela									1	1	8

Fuente: El portal de ISO 27001 en español

En esta tabla del portal de ISO 27001 nos muestra que hasta el 2016 Colombia ha obtenido 163 certificaciones y 257 sitios.

6.2.1 ¿CÓMO IMPLEMENTAR EL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA ORGANIZACIÓN?

La implementación de Sistema de Gestión de la Seguridad de la Información SGSI siempre debe cumplir con los siguientes pasos, hay que tener en cuenta que cada organización es diferente y cuenta con recursos y necesidades específicas, a continuación, se muestra la forma general de la implementación de un Sistema de Gestión de la Seguridad de la Información SGSI.

6.2.1.1 Planear. En este punto se debe analizar en entorno de la organización, se debe realizar el diseño del procedimiento que se va a realizar para la identificación de los riesgos y los controles que se van a tomar para gestionar estos riesgos.

- Creación de un plan de trabajo.
- Definir el alcance del SGSI.
- Definir la política de seguridad de la información para la entidad.
- Definir el inventario de activos de información.
- Definir el enfoque de análisis de riesgo.
- Metodología de análisis.
- Realizar el análisis de riesgo.
- Definir el plan de tratamiento del riesgo.
- Seleccionar los controles a implementar.
- Preparar la Declaración de aplicabilidad.
- Aprobación y gestión de recursos.
- Plan de tratamiento de riesgo.
- Definir conjunto de objetivos y métricas.
- Asignación y delimitación de responsabilidades.
- Implementación y puesta en marcha.
- Capacitación del personal.[22]

Basados en la norma ISO 27001 este paso puede tardar entre 6 meses a un año

6.2.1.2 Hacer. Es esencialmente la implementación del plan hecho anteriormente donde permita mitigar los riesgos y evitarlos, en esta fase es muy importante la

[22] EL PORTAL DE ISO 27001 EN ESPAÑOL. {En línea}. {Consultado el 22 de Agosto de 2017} Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

capacitación al personal de la organización buscando garantizar el éxito de la implementación de SGSI.

- Ejecutar el plan de tratamiento del riesgo.
- Documentar los controles.
- Implementar las políticas.
- Implementar entrenamiento.
- Gestionar la operación y los recursos.
- Implementar las respuestas a incidentes[23]

6.2.2.3 Verificar. Teniendo en cuenta que la implementación del SGSI requiere un seguimiento y control de todas las medidas implantadas, se debe realizar una serie de auditorías internas y externas que garanticen la correcta ejecución del SGSI.

- Verificar el inventario de activos de información.
- Realizar revisiones de eficiencia.
- Realizar revisiones del nivel de riesgo residual.
- Realizar la revisión interna del SGSI.
- Realizar la revisión por la dirección del SGSI.
- Registrar el impacto en el SGSI.[24]

6.2.2.4 Actuar. El SGSI exige actuar y mejorar, si se identifican amenazas, vulnerabilidades o riesgos es necesario actuar inmediatamente tomando las medidas necesarias preventivas y correctivas que garanticen la seguridad de la información de la organización.

- Implementar las mejoras identificadas.
- Tomar medidas preventivas y correctivas.
- Aplicar lecciones aprendidas.
- Comunicar los resultados.
- Garantizar el objetivo del SGSI.
- Revisar la Política de Seguridad, el Alcance del SGSI, los Activos de información, el Riesgo residual.[25]

[23] EL PORTAL DE ISO 27001 EN ESPAÑOL. {En línea}. {Consultado el 22 de Agosto de 2017} Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf
[24] EL PORTAL DE ISO 27001 EN ESPAÑOL. {En línea}. {Consultado el 22 de Agosto de 2017} Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf
[25] EL PORTAL DE ISO 27001 EN ESPAÑOL. {En línea}. {Consultado el 22 de Agosto de 2017} Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

Se debe tener en cuenta que la Norma ISO 27001 dice que se debe hacer, hacia donde se debe llegar con respecto a los objetivos que se tengan de seguridad, dice que se debe implementar, mas no el cómo, el cómo depende de cada organización de la gestión de riesgos que se realice, de los recursos con que se cuente, de las prioridades que se tengan; aunque cuenta con una lista de controles, no obliga a implementarlos de cierta forma, es flexible para que cualquier organización la pueda aplicar

Algo que se debe tener en cuenta y que muchas veces afecta al momento de tomar la decisión de implementar el Sistema de Gestión de la Seguridad de la Información, en especial en las pequeñas empresas como se sabe, es el costo, es claro que hay que realizar una inversión, pero como lo se ha analizado la organización define hasta dónde quiere llegar y como implementarlo, también depende del tamaño de la organización, la implementación se puede adaptar a los recursos con que se cuenten.

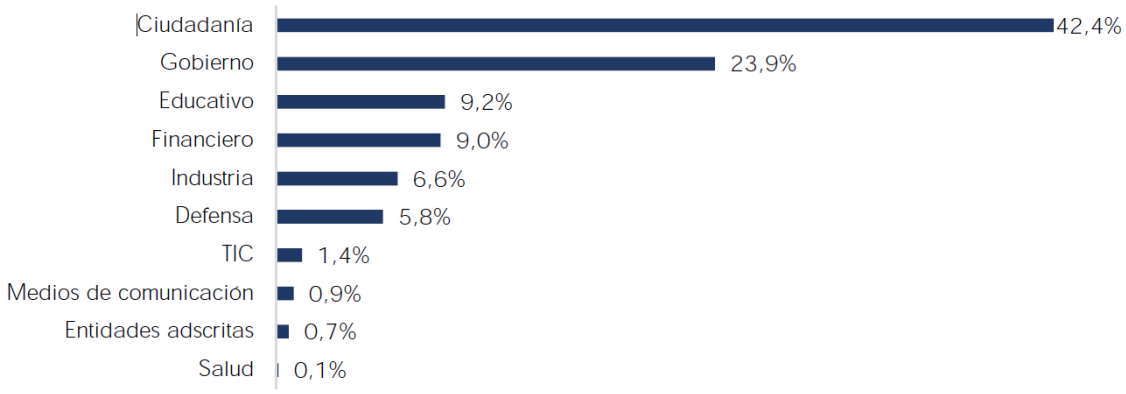
Teniendo en cuenta todo lo anterior se puede concluir que cualquier organización puede implementar su SGSI, lo que debe hacer o por donde debe empezar inicialmente es realizar una análisis del estado actual, identificar con qué recursos cuenta y que recursos necesita, luego de esto debe definir el alcance que depende de cada organización este debe ser muy claro y preciso, debe contar con un plan que por supuesto este plan lo da la misma norma que dice que se debe hacer, además debe haber un líder que se empodere del proceso y lo saque adelante, también se debe contar con una apoyo del personal operativo, ya que se debe contar con todas las áreas de la organización que apoyen en el proceso de identificación e implementación, además se iniciara con los riesgos donde se debe realizar una matriz de riesgos, el impacto de estos riesgos para su posterior gestión, algo que también se debe tener en cuenta para iniciar es buscar apoyo de los socios o empresas aliadas, para que compartan experiencias con respecto a la implementación del SGSI, allí se puede identificar cual es mejor forma de hacerlo y examinar las mejores alternativas

6.3 CAPITULO III: DIAGNÓSTICO GENERAL SOBRE LA IMPORTANCIA Y MEDIDAS NECESARIAS PARA PROTEGER EL ACTIVO DE LA INFORMACIÓN.

Como se ha analizado en los capítulos anteriores es claro que los ataques informáticos no disminuyen por el contrario cada vez son más organizados y más efectivos, es por esto que es necesario y muy importante que todas las organizaciones estén preparadas para contrarrestarlos, por esto es indispensable tomar medidas de protección para resguardar en lo posible el activo de la información.

Según el diagnóstico del CONPES 3854 en Colombia se ha vivido un crecimiento en la conectividad desde el año 2010 lo que por supuesto aumento los riesgos y vulnerabilidades

Figura 10: Sectores afectados en Colombia por incidentes digitales, 2015



Fuente: colCERT, 2015.

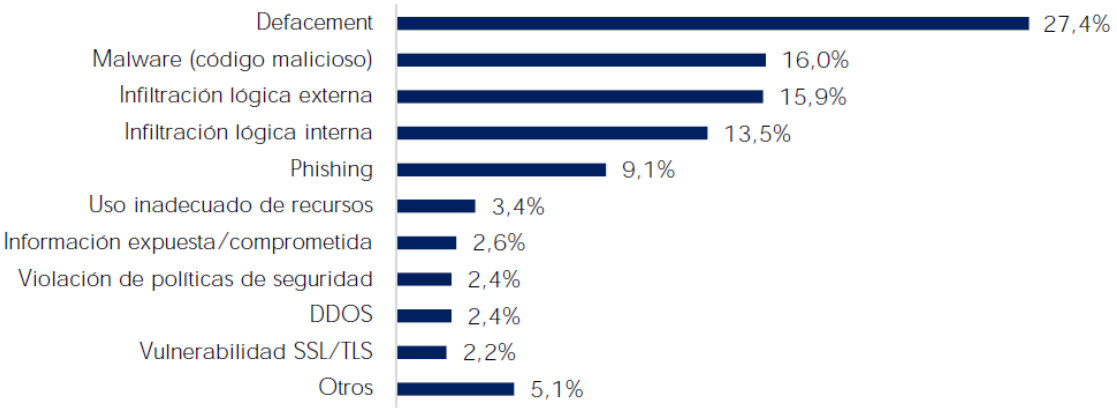
En la figura anterior podemos identificar que los ciudadanos son los más afectados con incidentes digitales seguidos por el gobierno y el sector educativo, es por esto que es tan importante ser conscientes de los riesgos de seguridad y tomar medidas al respecto, más aun sabiendo que Colombia no cuenta con una entidad encargada de la seguridad digital.

Figura 11: Incidentes digitales gestionados por CCP y CSIRT PONAL en el entorno digital en Colombia, 2015

Fuente: CCP y CSIRT PONAL, 2015

Dentro de los incidentes que vemos en la figura anterior se identifica el Defacement con un porcentaje de 34.4 % como uno de los incidentes más gestionados por la policía nacional, seguido por la estafa en compra y venta de productos o servicios por internet lo efectivamente evidencia que quienes más se ven afectados son los ciudadanos.

Figura 12: Incidentes digitales gestionados por el CCOC y el colCERT en el entorno digital en Colombia, 2015



Fuente: CCOC y colCERT, 2015.

En esta figura sigue siendo el Defacement con un 27.4 % el incidente digital más gestionado, como medida de protección se recomienda encontrarse siempre a la vanguardia de la tecnología en cuanto de protección de la información se trata, estar siempre informados sobre los avances que se tienen en cuanto a posibles ataques y como evitarlos, mantenerse siempre actualizados en los mecanismos de protección que se implemente en la organización. Además como se mencionó en el capítulo anterior es absolutamente necesario que todas las organizaciones implementen un Sistema de Gestión de la Seguridad de la Información (SGSI), para que de esta manera se tengan controlados los riesgos, y se cuenten con políticas claras del manejo de la información y su seguridad, además tener en cuenta que es necesario que todos en la organización conozcan el SGSI y lo apliquen totalmente, los recursos financieros para la implementación del SGSI no debe ser una excusa ya que como se mencionó este sistema nos dice que hacer mas no nos dice cómo hacerlo; es por esto que se puede adecuar a los recursos y necesidades de cualquier organización, así pues la recomendación más importante es la implementación del SGSI.

Es de suma importancia tener en cuenta que en la seguridad el recurso humano es muy importante, se debe contar con un proceso de capacitación y sensibilización del personal identificando sus roles y responsabilidad, hay que tener en cuenta que no es solo al personal que se encuentra en la actualidad en la

organización sino al momento de la vinculación o desvinculación, donde se deben tomar medidas como revisión de antecedentes, acuerdos de confidencialidad, firmas de paz y salvos etc., no olvidar el procedimiento de gestión y acceso a los sistemas de información, se deben validar los datos completos para ingresar a los sistemas, creación de usuarios y contraseñas.

No se debe dejar atrás la seguridad física y del entorno, tener el control del acceso áreas no autorizadas para evitar daños a la infraestructura, las instalaciones y por supuesto a la información, se debe identificar la ubicación de equipos que contengan información confidencial, aplicar controles para minimizar los riesgos de desastres naturales, amenazas físicas, daños por polvo, agua, descargas eléctricas, etc.

Tener en cuenta que al momento de retirar algún activo de la organización se debe contar con un procedimiento de autorización, en caso de mantenimientos preventivos se debe tener claro el procedimiento y los responsables.

Conjuntamente con las medidas mencionadas en los capítulos anteriores se recomienda al momento de actualizar o implementar nuevas aplicaciones tener en cuenta lo siguiente:

- Proteger los ambientes de desarrollo.
- Controlar el software adquirido.
- Restricciones en los cambios a paquetes de software.
- Realizar pruebas de seguridad de software.
- Cumplir con todas las leyes dispuestas para la protección de la información.
- Realizar copias de seguridad.

Hay otras alternativas para las organizaciones en Colombia que es adquirir servicios de CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad) o Centro de Operaciones de Seguridad o SOC, que cuentan con un grupo de expertos que se encargan de desarrollar medidas preventivas o correctivas al presentarse incidentes de seguridad en los sistemas de información, mediante el estudio de la seguridad en general de la organización y buscando o adecuando las mejores soluciones de seguridad, además de emitir alertas ante posibles vulnerabilidades.
Actualmente hay muchas empresas que prestan estos servicios en Colombia como Telefónica, Claro, CSIRT-CCIT, swatsecurityit, Ona Systems, entre otras. Entre los servicios que prestan son, avisos de seguridad, gestión de incidentes, gestión de vulnerabilidades, configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructura, auditorias y evaluaciones, búsqueda de vulnerabilidades.

Además hay que tener en cuenta que no solo se cuenta con la Norma ISO 27001 sino que además se cuentan con guías de buenas prácticas como por ejemplo el COBIT Control Objectives for Information and related Technology, que busca un mejor control y supervisión de los recursos de la tecnologia de la información, con una serie de procesos para mejorar la privacidad, los usuarios, Big data o detección de fraude, analítica preventiva y en general las buenas practicas dentro de la organización para el tratamiento de la información y las tecnologías de la información.

Se recomienda también a las organizaciones en Colombia que conozcan los mecanismos con que cuenta el estado o la policía nacional para brindar información importante y actualizada sobre posibles alertas o amenazas de seguridad, así como también los mecanismos con que cuentan para las denuncias o alertas de seguridad que se puedan presentar, ejemplo: El gobierno de Colombia cuenta con el Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT, que consiste en un grupo de expertos que se encargan de la gestión de incidentes de tipo cibernético entendidos como amenazas a las políticas de seguridad informática, para mitigar el riesgo y dar respuesta; mediante su página web se pueden consultar las alertas de seguridad que se han presentado de manera actualizada, además se encuentran los mecanismos que se pueden usar para denunciar ciberdelitos, reportar incidentes ya que tiene como responsabilidad la coordinación de la Ciberseguridad y Ciberdefensa Nacional, coordinando y asesorando no solo a entidades públicas sino privadas para responder ante incidentes informáticos.

También la policía nacional de Colombia cuenta con CSIRT-PONAL, que también es un equipo de respuesta a los incidentes de seguridad informática de la policía nacional, cuya función es prevención e investigación de los incidentes de seguridad informática; a través de su página web también se pueden consultar alertas y tips de seguridad, con boletines actualizados y recomendaciones para evitar ataques. De esta manera se puede contar con información actualizada y segura que permita estar atentos ante posibles ataques en las organizaciones.

Es muy importante contar con estos mecanismos que permiten de manera conjunta estar atentos ante cualquier amenaza a demás en caso de tener un ataque poder denunciar y combatir los ciber ataques de manera responsable.

Tabla 4: Tabla resumen de diagnóstico.

DATOS	
163	Certificaciones ISO 27001 hasta el 2016 en Colombia[26]
60%	Según Kaspersky las empresas admitieron que al menos ha tenido un incidente de seguridad. una encuesta global que incluyó a más de 5,500 ejecutivos de empresas y profesionales de 26 países, incluyendo Colombia[27]
4/10	Usuarios de internet han sido víctimas de delitos informáticos según Symantec.[28]
$917.000.000	A esto hacienden los gastos por daños a causa del Cibercrimen en el año no solo por la pérdida sino por la reparación, según David Kummers especialista en seguridad en redes de Certicamara[29]
460.000	Programas maliciosos para Mac[30]
630.000	Malware para Windows y Android[31]
35%	De la población mundial tiene como mínimo un dispositivo sin proteger.[32]
1.000.000	En el 2015 ataques web contra usuarios de internet por día.[33]
36%	De las empresas en Colombia realizan auditoria de seguridad según ESET.[34]
46,7%	De las empresas sufrieron algún incidente de seguridad durante un año, según ESET.[35]

[26] EL PORTAL DE ISO 27001 EN ESPAÑOL. {En línea}. {Consultado el 22 de Agosto de 2017} Disponible en: http://www.iso27000.es

[27] INFORME SOBRE FRAUDE FINANCIERO KASPERSKY NOVIEMBRE DE 2015. {En línea}. {Consultado el 12 de Septiembre de 2017} Disponible en: https://latam.kaspersky.com/about/press-releases/2015_kaspersky-lab-publica-informe-sobre-el-fraude-financiero-la-amenaza-que-a-las-empresas-les-gustaria-prevenir-a-toda-costa.

[28] INFORME SOBRE LAS AMENAZAS PARA LA SEGURIDAD EN INTERNET DE 2017 DE SYMANTEC. {En línea}. {Consultado el 11 de septiembre de 2017} Disponible en: <https://www.symantec.com/es/mx/security-center/threat-report?inid=symc-home-page_ghp_to_security-center_threat-response.html

[29] CIO AMERICA LATINA {En línea}. {Consultado el 15 de noviembre de 2017} Disponible en: http://www.cioal.com/2016/09/08/delitos-ciberneticos-en-colombia/

[30] INFORME DE MCAFEE LABS SOBRE AMENAZAS JUNIO DE 2017. {En línea}. {Consultado el 12 de Septiembre de 2017} Disponible en: https://www.mcafee.com/es/resources/reports/rp-quarterly-threats-jun-2017.pdf

[31] INFORME DE MCAFEE LABS SOBRE AMENAZAS JUNIO DE 2017. {En línea}. {Consultado el 12 de Septiembre de 2017} Disponible en: https://www.mcafee.com/es/resources/reports/rp-quarterly-threats-jun-2017.pdf

[32] INFORME SOBRE CIBERSEGURIDAD DE NORTON 2016. {En línea}. {Consultado el 11 de Septiembre de 2017} Disponible en: https://mx.norton.com/cyber-security-insights-2016

[33] INFORME SOBRE CIBERSEGURIDAD DE NORTON 2016. {En línea}. {Consultado el 11 de Septiembre de 2017} Disponible en: https://mx.norton.com/cyber-security-insights-2016

[34] CENTRO DE PRENSA ESET {En línea}. {Consultado el 29 de Septiembre de 2017} Disponible en: http://www.eset-la.com/centro-prensa/articulo/2017/los-10-incidentes-seguridad-mas-importantes-del-ultimo-a%C3%B1o/4439

40%	De las empresas de fabricación no realizan evaluación de riesgos por ciberataques.[36]
38%	Son ataque por instalación de software no autorizado.[37]
34%	Phishing[38]
20%	Ronsomware
60%	Realiza evaluaciones de seguridad.[39]
69%	Antimalware
62%	Firewalls
70%	Políticas de seguridad.
61%	De los obstáculos de seguridad es por falta de cultura.
40%	Falta de colaboración entre áreas.
35%	Poco entendimiento de la seguridad informática.
8%	Es el presupuesto que destinan las pymes para seguridad.[40]
96%	De la economía del país la mueven las pymes
76%	De las pymes son atacadas anualmente.
42,4	Siendo la ciudadanía el sector más afectado según CONCERT 2015[41]
23, 9%	Gobierno
34,4%	Defacement
15,4%	Estafa compra venta de productos o servicios por internet.

Fuente: El Autor

[35] CENTRO DE PRENSA ESET {En línea}. {Consultado el 29 de Septiembre de 2017} Disponible en: http://www.eset-la.com/centro-prensa/articulo/2017/los-10-incidentes-seguridad-mas-importantes-del-ultimo-a%C3%B1o/4439

[36] CSIRT-PONAL {En línea}. {Consultado el 15 de noviembre de 2017} Disponible en: https://cc-csirt.policia.gov.co

[37] CARACOL RADIO {En línea}. {Consultado el 02 de octubre de 2017} Disponible en: http://caracol.com.co/radio/2017/06/09/nacional/1497042960_148590.html

[38] ENCUESTA NACIONAL DE SEGURIDAD INFORMÁTICA 2017 {En línea}. {Consultado el 02 de octubre de 2017} Disponible en: http://acis.org.co/revista143/content/encuesta-nacional-de-seguridad-inform%C3%A1tica-2017

[39] ENCUESTA NACIONAL DE SEGURIDAD INFORMÁTICA 2017 {En línea}. {Consultado el 02 de octubre de 2017} Disponible en: http://acis.org.co/revista143/content/encuesta-nacional-de-seguridad-inform%C3%A1tica-2017

[40] ENCUESTA NACIONAL DE SEGURIDAD INFORMÁTICA 2017 {En línea}. {Consultado el 02 de octubre de 2017} Disponible en: http://acis.org.co/revista143/content/encuesta-nacional-de-seguridad-inform%C3%A1tica-2017

[41] COLCERT {En línea}. {Consultado el 15 de noviembre de 2017} Disponible en: http://www.colcert.gov.co

7 CRONOGRAMA

Tabla 5: Cronograma.

ACTIVIDADES	Sem 1	Sem 2	Sem 3	Sem 4	Sem 5	Sem 6	Sem 7	Sem 8	Sem 9	Sem 10	Sem 11	Sem 12	Sem 13	Sem 14
Identificar los elementos básicos acerca de la importancia de la seguridad informática en las organizaciones en Colombia.														
Indagar la Importancia de la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en las organizaciones colombianas.														
Presentar el estado de la seguridad informática para las organizaciones en Colombia.														

Fuente: El Autor

8. CONCLUSIONES

1. Durante el desarrollo del presente proyecto se presenta un análisis del estado actual de la seguridad informática en las organizaciones en Colombia buscando brindar un diagnostico general sobre la importancia y medidas necesarias para proteger el activo de la información.

   De esta manera se identificó los antecedes de la seguridad informática, contextualizando para realizar un análisis de cómo se encuentra actualmente la seguridad informática en Colombia teniendo en cuenta los informes emitidos anualmente por las más grandes empresas de antivirus, Kaspersky, Symantec, McAfee, ESET y Norton, además teniendo en cuenta reportes realizados por la ONU, la ISO, la Asociación Colombiana de Ingenieros de Sistemas (ACIS), el Ministerio de Tecnologías de Información y las Comunicaciones de Colombia y la policía nacional de Colombia.

   Donde se logró identificar que las organizaciones en Colombia se ven enfrentadas cada día a nuevas tecnologías que por supuesto pueden mejorar el desarrollo de sus actividades y su rendimiento en general, pero también se ven cada vez más expuestas a riesgos, por tanto se ven obligadas a tomar medidas de seguridad que permitan reducir sus riesgos, es por ello que aunque el panorama en general de la seguridad informática en Colombia no sea muy desalentador ya que se encuentra en un nivel medio en general, si genera una cierta incertidumbre con respecto a la importancia que se le está dando en general a la seguridad informática en las organizaciones, sobre todo aquellas empresas pequeñas pymes que no gastan gran presupuesto en su seguridad, ya que se ha analizado las empresas grandes o las empresas públicas que en su mayoría han implementado políticas de seguridad, pero las pymes son un blanco atractivo para los delincuentes ya que saben que estas empresas no invierten mucho presupuesto en su seguridad ya que por lo general no el mas de un 8% de su presupuesto, esto es realmente preocupante ya que las pymes en Colombia mueven alrededor de un 96% de la economía del país, y están siendo atacas anualmente alrededor de un 73% de las pymes en Colombia, a través de extraer información de sus correos electrónicos o redes sociales, ataques de Phising, no dejando atrás el robo de información internamente en las empresas donde los mismos empleados pueden robar la información, además con la tendencia actual de que los empleados puedan llevar sus dispositivos portátiles personales, para realizar trabajos y conectarse a la red y recursos corporativos conocido como Bring Your Own Device, o también con el incremento del tele trabajo a puesto más en vilo el tema de la seguridad de la información, por esta y muchas más razones es necesario que las pequeñas y medianas empresas reconozcan la

importancia de la seguridad del información y generen más recursos para la implementación de políticas de seguridad en sus organizaciones, ya que los atacantes son inteligentes y sabrán donde atacar.

2. Se identificó que cualquier organización puede implementar su SGSI, lo que debe hacer o por donde debe empezar inicialmente es realizar una análisis del estado actual, identificar con qué recursos cuenta y que recursos necesita, luego de esto debe definir el alcance que depende de cada organización este debe ser muy claro y preciso, debe contar con un plan que por supuesto este plan lo da la misma norma que dice que se debe hacer, además debe haber un líder que se empodere del proceso y lo saque adelante, también se debe contar con una apoyo del personal operativo, ya que se debe contar con todas las áreas de la organización que apoyen en el proceso de identificación e implementación, además se iniciara con los riesgos donde se debe realizar una matriz de riesgos, el impacto de estos riesgos para su posterior gestión, algo que también se debe tener en cuenta para iniciar es buscar apoyo de los socios o empresas aliadas, para que compartan experiencias con respecto a la implementación del SGSI, allí se puede identificar cual es mejor forma de hacerlo y examinar las mejores alternativas.

3. Se presentaron algunas medidas para proteger el activo de la información teniendo en cuenta que los ataques informáticos no disminuyen por el contrario cada vez son las efectivos y organizados, se debe estar siempre a la vanguardia de la tecnología en cuanto a protección se trate, se debe tener en cuenta la importancia de la implementación del SGSI ya que este se puede adaptar a todas las organizaciones de Colombia, no olvidar que el recurso humano debe siempre estar capacitado y sensibilizado en cuanto la seguridad de la organización así como también no olvidar la seguridad física y del entorno y aplicar los controles necesarios.

   Otras alternativas de seguridad para tengan en cuenta las organizaciones es adquirir servicios de CSIRT o SOC, que son muy útiles en el momento de adquirir métodos de seguridad de la información además de recomendar a las organizaciones que se mantengan informados sobre los mecanismos con que cuenta el estado y la Policía Nacional para apoyar y proteger la seguridad informática del país además de dar apoyo ante posibles amenazas y en caso de presentarse un ataque poder denunciar, esto con el fin de que entre todos se puedan contrarrestar estos ataques y en conjunto poder combatir a los ciber delincuentes.

BIBLIOGRAFIA.

AGUILERA LOPEZ. Seguridad informática: Madrid: Editex, S.A, 2010. 240 p.

AREITIO, Javier. Seguridad De La Información: Redes Informática y Sistemas de Información. Madrid: Paraninfo S.A, 2008. 567 p.

CHIAVENATO, Idalberto. Introducción a la teoría general de la administración, Séptima Edición, de Chiavenato Idalberto, McGraw-Hill Interamericana, 2006, 562 p.

FERRELL O. C. y HIRT Geoffrey, Introducción a los Negocios en un Mundo Cambiante, cuarta Edición, McGraw-Hill Interamericana, 2004, 638.p.

CZINKOTA Michael R y KOTABE , Administración de Mercadotecnia, Segunda Edición, International Thomson Editores, 2001,600 p.

WEBGRAFIA

INFORME SOBRE LAS AMENAZAS PARA LA SEGURIDAD EN INTERNET DE 2017 DE SYMANTEC. {En línea}. {Consultado el 11 de septiembre de 2017} Disponible en: <https://www.symantec.com/es/mx/security-center/threat-report?inid=symc-home-page_ghp_to_security-center_threat-response.html

SGSI. {En línea}. {Consultado el 24 de Agosto de 2017} Disponible en: http://www.iso27000.es/sgsi.html

EL PORTAL DE ISO 27001 EN ESPAÑOL. {En línea}. {Consultado el 22 de Agosto de 2017} Disponible en: http://www.iso27000.es/faqs.html#seccion1

ISO 27000. {En línea}. {Consultado el 22 de Agosto de 2017} Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

RESOLUCIÓN 26930 DE 2000. {En línea}. {Citado el 16 de Septiembre de 2017} Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5793

INFORME DE MCAFEE LABS SOBRE AMENAZAS JUNIO DE 2017. {En línea}. {Consultado el 12 de Septiembre de 2017} Disponible en: https://www.mcafee.com/es/resources/reports/rp-quarterly-threats-jun-2017.pdf

INFORME SOBRE FRAUDE FINANCIERO KASPERSKY NOVIEMBRE DE 2015. {En línea}. {Consultado el 12 de Septiembre de 2017} Disponible en: https://latam.kaspersky.com/about/press-releases/2015_kaspersky-lab-publica-informe-sobre-el-fraude-financiero-la-amenaza-que-a-las-empresas-les-gustaria-prevenir-a-toda-costa.

INFORME SOBRE CIBERSEGURIDAD DE NORTON 2016. {En línea}. {Consultado el 11 de Septiembre de 2017} Disponible en: https://mx.norton.com/cyber-security-insights-2016

CENTRO DE PRENSA ESET {En línea}. {Consultado el 29 de Septiembre de 2017} Disponible en: http://www.eset-la.com/centro-prensa/articulo/2017/los-10-incidentes-seguridad-mas-importantes-del-ultimo-a%C3%B1o/4439

ALERTA DE SEGURIDAD INFORMÁTICA {En línea}. {Consultado el 02 de octubre de 2017} Disponible en: https://www.policia.gov.co/noticia/alerta-seguridad-informatica

ENCUESTA NACIONAL DE SEGURIDAD INFORMÁTICA 2017 {En línea}. {Consultado el 02 de octubre de 2017} Disponible en: http://acis.org.co/revista143/content/encuesta-nacional-de-seguridad-inform%C3%A1tica-2017

CARACOL RADIO {En línea}. {Consultado el 02 de octubre de 2017} Disponible en: http://caracol.com.co/radio/2017/06/09/nacional/1497042960_148590.html

RETOS DE SEGURIDAD PARA LAS PYMES {En línea}. {Consultado el 03 de octubre de 2017} Disponible en: http://www.enter.co/especiales/enterprise/los-retos-de-seguridad-para-las-pymes/

CIO AMERICA LATINA {En línea}. {Consultado el 15 de noviembre de 2017} Disponible en: http://www.cioal.com/2016/09/08/delitos-ciberneticos-en-colombia/

COLCERT {En línea}. {Consultado el 15 de noviembre de 2017} Disponible en: http://www.colcert.gov.co

CSIRT-PONAL {En línea}. {Consultado el 15 de noviembre de 2017} Disponible en: https://cc-csirt.policia.gov.co

CONPES CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL REPUBLICA DE COLOMBIA {En línea}. {Consultado el 12 de febrero de 2018} Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf