INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE COMERCIO Y ADMINISTRACIÓN
UNIDAD SANTO TOMÁS
Sección de Estudios de Posgrado e Investigación

"PROPUESTA PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN CON BASE EN LAS TI EN LA EMPRESA "CARE ENTERPRISE NETWORKS"

TESIS

Que para obtener el grado de

Maestría en Ciencias en Administración de Negocios

Presenta

MOISÉS DÍAZ DÍAZ

Directoras de Tesis

Dra. María del Rocío Soto Flores

Dra. Susana Asela Garduño Román

México D.F., Agosto 2016

SIP-14-BIS

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de **MÉXICO, D. F.** siendo las **17:00** horas del día **20** del mes de **JUNIO** del **2016** se reunieron los miembros de la Comisión Revisora de Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de **LA E. S. C. A.** para examinar la tesis titulada:

"PROPUESTA PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN CON BASE EN LAS TI EN LA EMPRESA "CARE ENTERPRISE NETWORKS""

Presentada por el alumno:

DÍAZ	**DÍAZ**	**MOISÉS**
Apellido paterno	Apellido materno	Nombre(s)

Con registro:

B	1	2	0	9	9	8

aspirante de:

MAESTRÍA EN CIENCIAS EN ADMINISTRACIÓN DE NEGOCIOS

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***APROBAR LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Directores de tesis

DRA. MARÍA DEL ROCÍO SOTO FLORES

DRA. SUSANA ASELA GARDUÑO ROMÁN

DR. LUIS ROCHA LONA

M. EN C. LETICIA REFUGIO CHAVARRÍA LÓPEZ

M. EN C. MARTÍN JESÚS MILLÁN MANJARREZ

PRESIDENTE DEL COLEGIO DE PROFESORES

DR. LUIS ROCHA LONA

INSTITUTO POLITÉCNICO NACIONAL
E.S.C.A. SANTO TOMÁS
SECCIÓN DE ESTUDIOS DE
POSGRADO E INVESTIGACIÓN

INSTITUTO POLITÉCNICO NACIONAL

COORDINACIÓN GENERAL DE POSGRADO E INVESTIGACIÓN

CARTA CESIÓN DE DERECHOS

En la Ciudad de México, D.F. el día 23 del mes de Junio del año 2016, el que suscribe Moisés Díaz Díaz alumno del Programa de Maestría en Ciencias en Administración de Negocios, con número de registro B120998, adscrito al Instituto Politécnico Nacional, Escuela Superior de Comercio y Administración Unidad Santo Tomás, Sección de estudios de Posgrado e Investigación, manifiesto que es autor intelectual del presente trabajo de Tesis bajo la dirección de la Dra. Maria del Rocio Soto Flores y de la Dra. Susana Asela Garduño Román y cede los derechos del trabajo titulado **"Propuesta para mejorar la seguridad de la información con base en las TI en la empresa Care enterprise networks"**, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o directoras del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección **ddmoises@gmail.com.** Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Moisés Díaz Díaz

Resumen

Las tecnologías de la información son la herramienta base para incrementar la seguridad de la información. En México, hace falta dar la importancia necesaria a la información que viaja a través del internet y que se aloja en los miles de equipos y servidores que tienen las empresas para almacenarla. Es por ello que se requieren tecnologías de la información de vanguardia y dar uso a los modelos de seguridad de la información para ofrecer mayor seguridad a los usuarios y que las empresas tengan mayor captación de clientes.

La presente investigación tiene como objetivo elaborar una propuesta de mejora para incrementar la seguridad de la información con base en las tecnologías de la información a través de la identificación de las amenazas y vulnerabilidades que atañen a la empresa Care Enterprise Networks. Dado el carácter de la información analizada, la estrategia metodológica se basa en una investigación documental, lo que permitió analizar las causas de pérdida de información y la incorrecta aplicación de las tecnologías de la información que tiene la empresa, así como las amenazas y vulnerabilidades que impactan a los objetivos del negocio.

Los resultados obtenidos, muestran que la empresa presenta trece amenazas que engloban a ochenta y dos vulnerabilidades con base en el análisis documental a cada departamento de la empresa, lo que refleja que las tecnologías de la información no han sido aplicadas adecuadamente y por ende los clientes se quejan constantemente por la pérdida de información y los ataques que han recibido a sus aplicativos corporativos.

La propuesta de mejora realizada, hace una recomendación para cada vulnerabilidad encontrada y a su vez, se proponen acciones para cada amenaza que se identificó con base en el modelo de seguridad de ISO/IEC 27001:2013 que ayudarán a incrementar la seguridad de la información dentro de la empresa estudiada.

Abstract

Information technologies are the basic tool to increase information security. In Mexico, it is necessary to give the necessary importance to the information traveling across the internet and staying in the thousands of computers and servers that companies have to store it. That is why information technology and cutting edge required using models of information security to provide greater security to users and businesses to have greater customer acquisition.

This research aims to make a proposal for actions to increase the security of information based on information technologies through the identification of threats and vulnerabilities regarding the company Care Enterprise Networks. Given the nature of the information analyzed, the methodological strategy is based on documentary research, which allowed analyzing the causes of data loss and incorrect application of information technology that the company, as well as threats and vulnerabilities impacting business objectives.

The results show that the company has thirteen threats encompass eighty two vulnerabilities, reflecting that information technologies have not been adequately implemented and therefore customers constantly complain about the loss of information and attacks they have received their corporate applications.

The proposed made, makes a recommendation for each vulnerability found and in turn, actions for each threat identified based on the security model ISO / IEC 27001:2013 are proposed to help increase the security of information within the company studied

ÍNDICE

Índice de tablas

Índice de figuras

Índice de graficas

Siglas y abreviaturas

BCP: Business Continuity Plan

CERT: Computer Emergency Response Team

DoS: Denial of Service

HTTP: Hypertext Transfer Protocol

IEC: International Electrotechnical Commission

IP: Internet Protocol

ISO: International Organization

ITIL: Information Technology Infrastructure Library

ITSCM: Information Technology Service Continuity Management

KPI: Key Performance Indicators

MAGERIT: Metodología de Análisis y Gestión de Riesgos

MAAGTICSI: Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información

NFS: Network File System

RFC: Request for Comments

SGSI: Sistema de Gestión de Seguridad de la Información

TI: Tecnologías de la información

Glosario

A

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. BS. (2013)

Ancho de banda: Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobites por segundo (kbps), o megabites por segundo (mps). CEPAL. (2010).

Ataque: Intento de destruir, exponer, alterar, inutilizar, robar u obtener acceso no autorizado de un activo. Patrick Engebretson, P. (2013)

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta. BS. (2013)

B

Backdoor: Es una forma alterna de acceso a una aplicación o sistema dejada por el programador o creada mediante algún programa para burlar los controles normales de acceso. Patrick Engebretson, P. (2013)

C

Código malicioso: Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Patrick Engebretson, P. (2013)

Confidencialidad: Información que no debe de estar disponible o no debe ser revelada individuos, organizaciones o personal no autorizado. BS. (2013)

Cracker: Es una persona que irrumpe en los sistemas de un tercero, normalmente a través de la red, evitando los controles de acceso o de alguna manera rompiendo la seguridad del sistema. Sterling, B. (1992)

E

Evento de seguridad de la información: Es cualquier situación o condición que indica una posible violación de seguridad de la información a la política o la falta de salvaguardas, o de una situación desconocida que puede ser relevante a la seguridad. BS. (2013)

F

Firewall: Un sistema o combinación de sistemas que refuerzan los límites entre dos o más redes. Un firewall regula el acceso entre las redes de acuerdo a una política de seguridad específica. Stallings, W. (2013)

G

Gestión de Seguridad de la Información: Es el proceso dentro de la Fase de Diseño del ciclo de vida del Servicio cuyo propósito es que los aspectos de seguridad respecto a los servicios y todas las actividades de Gestión de Servicios se manejen y controlen apropiadamente y en línea con las necesidades y riesgos del negocio. BS. (2013)

H

Hacker: Es un término que se empleaba para definir a un programador habilidoso, actualmente se utiliza para definir a la persona que intenta acceder a los sistemas de una manera inapropiada. Sterling, B. (1992)

P

Plan de Tratamiento del Riesgo: Conjunto de programas de Seguridad que permiten materializar las decisiones de gestión del riesgo. BS. (2013)

Port scanning: Es un ataque que consiste en identificar los puertos que están activos en un dispositivo conectado a una red TCP. Stallings, W. (2013)

Puerto: Son las puertas de entrada a los servicios de red de un sistema. Cada servicio está asociado a un puerto, por ejemplo, el puerto 21 pertenece a FTP, el 80 a HTTP, el 25 a SMTP, etc. Stallings, W. (2013)

R

Riesgo: Efecto o incertidumbre sobre objetivos; estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a los servicios de negocio. BS. (2013)

Riesgo Aceptable: Aquel nivel de riesgo donde la Alta Dirección decide que las afectaciones derivadas de la materialización de la amenaza no implican un daño importante a los activos de la empresa y por tanto se decide asumir el riesgo. BS. (2013)

Router: Dispositivo encargado de indicar el camino que deberá seguir la información que viaja por la red para llegar a su destino. Stallings, W. (2013)

S

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. BS. (2013)

Servidor de Seguridad: Tiene software especializado para detener intrusiones maliciosas, normalmente tienen antivirus, antispyware, antimalware, además de contar con cortafuegos redundantes de diversos niveles y/o capas para evitar ataques, los

servidores de seguridad varían dependiendo de su utilización e importancia. Stallings, W. (2013)

Sniffer.- Programa empleado para "escuchar" todo el tráfico que pasa por una red. Michael E. Whitman, Herbert J. Mattord. (2012)

Spoofing.- Es la imitación de la dirección IP del remitente o incluso hacerse pasar por un usuario autorizado en un intento por obtener la entrada ilegal a un sistema. Michael E. Whitman, Herbert J. Mattord. (2012)

Switch.- Es un dispositivo digital de lógica de interconexión de redes que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. Stallings, W. (2013)

V

Vulnerabilidad.- Debilidad de un activo o control que puede ser explotado por una o más amenazas. BS. (2013)

Z

Zone Transfer.- Ataque empleado por un hacker para desplegar toda la base de datos de un DNS. Stallings, W. (2013)

Introducción

Las tecnologías de la información son la vanguardia de la tecnología en todo el mundo, pero sin su adecuada aplicación a los diferentes campos que tiene, puede impactar a los millones de usuarios que las utilizan. Tal es el caso del robo de información que hoy en día es uno de los problemas más importantes a resolver en el mundo de las nuevas tecnologías expresadas en el uso intensivo del internet.

En México, aún no se ha dado la importancia adecuada a la información que está almacenada en los centros de datos, equipos y sistemas. Las TI son amenazadas y vulneradas en diferentes niveles de criticidad según sea la orientación y el ámbito de su utilización.

Es preocupante que las empresas grandes, medianas y pequeñas en México no cuentan con una aplicación adecuada de las tecnologías de la información con respecto a la seguridad de la información, es así como los espionajes, la ingeniería social, los hackers, crackers, virus y ataques, penetran la infraestructura de la empresa para obtener información y vulnerar los sistemas centrales, y en algunos casos llevar a un caos a la empresa.

Cada día se desarrollan nuevos métodos de ataque y penetración que afectan la seguridad de la información de las organizaciones; por ello, se requiere de una nueva estrategia de seguridad de la información que tome en cuenta tanto la adecuada aplicación de las tecnologías de la información como los métodos convenientes para salvaguardar la información y evitar factores de riesgo que conlleven a la poca confiabilidad por parte de los clientes y socios del negocio.

En la seguridad de la información no se pueden obviar los factores de riesgo que existen por desastres que no están previstos eficientemente y sin planes de contingencia y/o de recuperación que puedan provocar daños irreparables en tiempo y costos de recuperación. Esto de no ser tomado en cuenta puede llevar a que la empresa no tenga continuidad en sus servicios de negocio.

Conforme al objetivo general esbozado, esta investigación se plantea desarrollar una propuesta de seguridad de la información con base en las TI, que contenga los elementos necesarios para disminuir las amenazas y vulnerabilidades de la información en la empresa estudiada, por lo cual la tesis está organizada en cinco capítulos:

En el primer capítulo se presenta la estrategia de la investigación que permea todo el trabajo; aquí se revisan los antecedentes que originaron la problemática planteada, la pregunta de investigación, los objetivos, su justificación, el diseño metodológico y sus elementos. Se continúa, en el segundo capítulo, con el marco teórico el cual engloba la problemática del sector, las tecnologías de la información, el uso de las redes en el internet y seguridad de la información, su definición, los elementos que se deben de proteger de los espías corporativos, los delitos cibernéticos y su clasificación. Posteriormente se incluye el tema de identificación y evaluación de los riesgos informáticos, sus alcances y limitaciones, los diferentes tipos de riesgos, amenazas y vulnerabilidades, así como el panorama actual de la seguridad en la red. Para el tercer capítulo se menciona el marco de referencia de ISO 27001, cuya metodología es referenciada para las tecnologías de la información en cuanto a seguridad de la información, además se contemplan los beneficios, estructura y empresas en México que cuentan con este marco de referencia.

Posterior se tiene el capítulo cuarto en el que se define la estrategia metodológica que se llevo a cabo para identificar el tipo de estudio, diseño de la investigación, variables y el supuesto teórico. Enseguida se culmina con la propuesta para aumentar la seguridad de la información en Care Enterprise Networks, la cual comprende el objetivo de la propuesta, alcances y limitaciones, la forma de atacar las trece amenazas identificadas así como las ochenta y dos vulnerabilidades relacionadas a cada amenaza y por último se incluye un plan de acción para atacar cada una de la amenazas.

CAPÍTULO 1. Estrategia de la investigación

1.1 Problemática del sector

Esta investigación se originó en un problema concreto de inseguridad de la información que enfrentan diariamente los sectores: financiero, productivo, gobierno, servicios y usuarios particulares. La ausencia de sistemas de seguridad que permitan salvaguardar la información electrónica, con estrategias adecuadas, sobre todo para la seguridad cibernética, dio lugar a esta tesis. Por lo tanto, en este capítulo se incluyen los aspectos relevantes de la seguridad de la información que conlleva el uso de las tecnologías de la información.

El desarrollo tecnológico, en los últimos siglos, ha sido el más grande en la historia y en los últimos años la rápida evolución de la informática, las computadoras y su conexión en red han cambiado la forma en que el ser humano percibe el mundo. El sistema digital, debido a su crecimiento exponencial, ha cambiado fuertemente la cultura, ya que para casi todo el quehacer humano es necesario utilizar una computadora.

En el entorno de los negocios en el siglo XXI, la mayor ventaja que tiene una computadora conectada a internet es la enorme cantidad de información que alberga, equivalente a tener la mejor biblioteca disponible al alcance de la mano. Otras ventajas de las computadoras con conexión a red, es el acceso a la diferente variedad de información y manipulación que se puede hacer. Es decir, la utilidad que tiene la informática en todos los ámbitos del quehacer humano, obliga a contemplar la forma en que se debe almacenar la información y resguardarla de posibles eventualidades que la amenacen (Larsen, 2002).

Las tecnologías de la información están hoy presentes en casi todos los campos de la vida. Con mayor o menor rapidez, todas las ramas del saber humano se involucran en los progresos tecnológicos y utilizan los sistemas de información para ejecutar tareas

que en otros tiempos se realizaban manualmente. El progreso de los sistemas computacionales permite procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, tecnológico, profesional y personal se incorporan a sistemas informáticos que, en la práctica cotidiana, entregan con facilidad un conjunto de datos que hasta hace años sólo podría ubicarse en grandes cantidades de archivos y documentos.

El enorme caudal de conocimientos puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operación, confiables y capaces de responder a casi toda la gama de interrogantes que se planteen a los archivos informáticos. Este panorama lleva a considerar a la informática como una forma de poder social, ya que pone a disposición de gobiernos y particulares, con rapidez y ahorro de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícitos e ilícitos, donde es necesario el derecho para regular los múltiples efectos de una situación nueva y de tantas potencialidades en el medio social.

En la actualidad, los cambios tecnológicos y el enorme aumento de las tecnologías de la información, también han desarrollado un lado negativo e inseguro para las redes de información, por lo que las organizaciones se han visto obligadas a establecer mecanismos de seguridad informática en sus operaciones, tema que se aborda en esta tesis.

El problema esencial que enfrentan las empresas dedicadas al área de tecnologías de la información, y que en particular manejan información de empresas, es que hoy en día tienen un reto muy importante; salvaguardar la información mediante políticas, controles, equipos de seguridad y software especializado, basado en las TI.

Por ejemplo, en un hecho reciente apareció en el periódico, el hackeo a la red de datos de Liverpool; prácticamente hicieron una intrusión minuciosa a los correos electrónicos de la empresa, así como el robo de información de clientes.

Este pequeño ejemplo muestra la vigencia y relevancia que tiene la seguridad de la información sobre todo para quienes tienen la responsabilidad de resguardarla, tenerla disponible, utilizable y segura. Estas son tareas directamente relacionadas con la plataforma de Tics que posee una organización.

De acuerdo con el listado del *Registro Internacional de Certificados ISMS*, en 2013, se tuvieron 5,059 organizaciones certificadas en ISO/IEC 27001 alrededor del mundo en el sector de tecnologías de la información y la comunicación.

En ese mismo año en México, se tuvieron solo 5 empresas certificadas en el sector de las Tics; este dato refleja que la cultura de seguridad de la información en México, es muy limitada. Además, se puede inferir que los dueños de empresas (empresarios), y los ejecutivos de las mismas, no están debidamente sensibilizados sobre la importancia que ha venido tomando la seguridad de la información y por ende, la inversión en el sector de las Tics de las empresas, apenas creció un 9.6%, que representa el 5.6% de ocupación en el PIB (producto interno bruto) de México. Este porcentaje de inversión es similar a las economías de Sudáfrica y Perú.

1.2 Empresa bajo estudio

La empresa “Care Enterprise Networks”, es una unidad de negocio dedicada a la administración, gestión y monitoreo de enlaces de comunicaciones, mediante mejores prácticas y procedimientos para ayudar al logro de los objetivos de negocio de cada uno de los clientes, además de encargarse del desarrollo de nuevos proyectos de TI para cada uno de ellos.

Care Enterprise Networks, inició su construcción en enero 2010 y su operación de manera formal en agosto del mismo año, con la siguiente misión, visión y servicios de negocio.

Misión

Ser el centro de operaciones de redes de clientes líder en el sector de tecnología de información y comunicaciones, proporcionando a los clientes servicios administrados de clase mundial, a través del desarrollo humano, tecnología de punta y procesos basados en mejores prácticas bajo estándares de calidad.

Visión

Consolidar el liderazgo del “Care Enterprise Networks”, expandiendo la penetración y alcance de servicios administrados en todos los mercados posibles, generando confianza en los clientes para establecer sociedades de negocio a largo plazo.

Servicios de Negocio

La unidad de negocio “Care Enterprise Networks” ha definido en su estructura los siguientes servicios de negocio con los cuales se provee el alcance de administración, gestión y monitoreo de redes de voz, datos, video e internet.

1. **Servicio de atención de eventos**

   Existen dos funcionalidades para la detección e identificación de eventos:

   Monitoreo Proactivo.- Consiste en la detección temprana de eventos sobre los componentes monitoreables que integran la red del cliente, para la generación inmediata de registros de incidentes, su atención y notificación.

   Reactivo.- Consiste en la recepción eficiente de eventos sobre los componentes que integran la red del cliente, para la generación de registros de incidentes, cambios y peticiones de servicio, su atención y notificación.

2. **Servicio de consulta de información**

   Las funcionalidades de este servicio incluyen como línea base las siguientes vistas:

   Estado de la Red.- Muestra las alertas sobre up-down y umbrales de desempeño.
   Eventos.- Muestra información sobre los eventos de la red del cliente (peticiones de servicio, cambios e incidentes)
   Salud de la Red.- Muestra información en línea sobre el desempeño de los componentes que integran la red del cliente.

3. **Servicio de reportes de desempeño de red**

   Las funcionalidades de este servicio incluyen como línea base los siguientes reportes:

   Reporte de Desempeño.- Permite conocer el desempeño de los componentes de la red del cliente.
   Reporte de Comportamiento.- Permite conocer la estabilidad de la Red.

Reporte de Tendencia.- Permite conocer el histórico y tendencia en el comportamiento.

Cabe señalar que el servicio de atención de eventos es el Core del negocio de Care Enterprise Networks, por lo que es de alta prioridad dar continuidad a este servicio en caso de que se tenga una contingencia en el negocio.

Care Enterprise Networks, es una organización que se clasifica como grande empresa, ya que actualmente cuenta con 457 trabajadores, los cuales trabajan los 7x24x365 días al año, ofreciendo los tres servicios de negocio a todos sus clientes de forma continua. Esta organización tiene presencia a nivel nacional y es subsidiaria de una telefónica, la cual tiene presencia a nivel internacional.

Care Enterprise Networks, cuenta con tecnología de punta, la cual está instalada a nivel infraestructura y a nivel software. La tecnología a nivel hardware se consideró prioritaria, para que con el tiempo no se vuelva obsoleta rápidamente y su ciclo de vida se alargue. Algunos de los equipos instalados para soportar la operación son: Equipos PC Dell, equipos de comunicación Cisco, Juniper, Alcatel, Avaya, Blue coat, Fortinet, Motorola, Huawei, LG, Samsung y Polycom. La tecnología instalada a nivel de software se engloba en algunos propietarios de los equipos de comunicación, ya que la mayoría del hardware cuenta con software previamente instalado; sin embargo para algunos aplicativos se utiliza: HP, IBM, Ubuntu, Windows Server, Oracle, Java, Avira, Red Hat y VMware.

1.3 Análisis técnico de la empresa

Care Enterprise Networks cuenta con diversas herramientas dentro del departamento de TI, operaciones y niveles de servicio, las cuales son puntos vulnerables de ataque para las amenazas que hay en el entorno. A continuación se mencionan las herramientas de hardware y de software que se tienen en los diferentes departamentos de la empresa, ver Tabla 1.

Nombre	Descripción de la herramienta	Criticidad
RSA	SIEM (Analizador de eventos)	Baja
OSSEC	SIEM (Analizador de eventos)	Baja
SFTP (FTP)	Servidor de File transfer	Alta
NNM	Gestión de aplicativos y servidores	Alta
OM	Gestión de aplicativos y servidores	Alta
NMIS	Monitoreo de desempeño	Alta
LDAP	Autenticación de servicios	Alta
TACACS	Servicio de autenticación AAA	Alta
Jack-v	Integración con otras herramientas	Alta
FDR	Monitoreo de desempeño, incluyendo incidentes, niveles de servicio Interfaz interna para los de ABC, inventario, calendario de cambios	Alta
Dashboard	Interfaz web para los clientes	Alta
Nessus	SIEM (Scanner de vulnerabilidades)	Baja
Solarwinds	Monitoreo de desempeño, incluyendo netflow	Baja
Active Directory	Autenticación Windows Controlador de dominio CNOC	Alta
Service manager	Aplicación para la solución de mesas de servicio TI	Alta
NAS	Administrador de configuraiones y aprovisionamiento de los equipos de los clientes	Alta
Open VPN	Creación de túneles para conexiona las redes de los clientes	Alta
NTP	Sincronización de relojes para servidores	Baja
Avaya	Aplicacion de la suite de HP encargada de generar una conexión al servidor de Service Manager	Alta
Data protector	Respalda servidores información	Baja
Vmware	Virtualización	Alta
Syslog interno	Línea de configuración.	Baja
GIT	Gestor de versiones	Baja
Mail	Servico de correo electrónico	Alta
DNS	Resolución de nombres	Alta
SAN	Gestión de almacenamiento en la red	Alta
Firewall VPN	Creación, habilitación y pruebas vpn site to site gestión aplicativo	Alta

Cisco Works	Gestión de aplicativo y servidor	Baja
Connect IT	Gestión de aplicativo	Baja
DWH/DB SQL	Gestión de base de datos	Alta
Nagios	Monitoreo de servidores	Baja
Cassandra	Base de datos para alta escalabilidad y disponibilidad	Alta
Netcool	Fault management	Alta
ABC tasks	Interfaz para generar scripts	Alta
DAPPS	Aplicativo para el desarrollo de Apps	Alta
ESX	Plataforma de virtualización de VMware	Alta
Automatizaciones	Creación, diseño, pruebas, liberacion y documentación	Baja
Zscaler	Se refiere a una aplicación diseñada para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de Internet	Baja
Presto	Software para el análisis de bases de datos ligadas a SQL	Baja
SSH	Software de acceso a los equipos de red	Alta
Firewall Analizer	Equipo de comunicación para el análisis de trafico interesante	Alta

Tabla 1. Herramientas; funciones y criticidades
Fuente: (Cnvrep003\ Doc_Trabajo\Matriz de Herramientas productivas 2015)

Con base en la información de la Tabla 1, enseguida se muestra en la Tabla 2, algunos de los incidentes que se relacionan entre seguridad de la información y las herramientas de la empresa (ver Tabla 2).

Incidente	Activo	Descripción	Proceso
IM0254757	NMIS	MODIFICACION DE URL EN DASHBOARD PARA EL AREA FTP DE LOS CLIENTES	Seguridad
IM0270834	Desktop Operaciones	ESTADIO-PC-VIRUS	Seguridad
IM0234266	Data Protector	TRIARA - CI0000053455 - DATA PROTECTO SERVICIO PTO 5555/TCP	Seguridad
IM0228916	SERVIDOR	CUICUILCO DATOS INTENTOS FALLIDOS DE LOGUEO EN SERVIDORES	Seguridad
IM0229308	NMIS	REACTIVACION DE USUARIO HPBAC	Seguridad
IM0232946	NAS	ERROR EN LA CONFIGURACION	Seguridad
IM0228906	SO Linux	CONFIGURACION DE LOGROTATE EN SERVIDOR SYSLOG	Seguridad
IM0186542	INSTALACIONES CUICUILCO	CUICUILCO-SISMO	Seguridad
IM0177637	INSTALACIONES CUICUILCO	CUICUILCO-SISMO	Seguridad
IM0185484	INSTALACIONES CUICUILCO	CUICUILCO-SISMO	Seguridad
IM0173774	Service Manager	INCIDENTE DE SEGURIDAD POR EL EVENTO	Seguridad

		RELACIONADO A ACCESOS A BD SM	
IM0173774	Service Manager	INCIDENTE DE SEGURIDAD POR EL EVENTO RELACIONADO A ACCESOS A BD SM	Seguridad
IM0143534	NNM	MONITOREO Y GESTION-NNM DE FAHORRO SIN GESTIONAR NODOS	Seguridad
IM0112178	Desktop Operaciones	USO NO AUTORIZADO DE EQUIPO	Seguridad
IM0090899	REPOSITORIO CNOC	DATOS - ACCESO NO AUTORIZADO A REPOSITORIO	Seguridad
IM0092284	PERSONAL	DATOS - SE DETECTAN CONEXIONES DE EQUIPOS MOVILES EN RED WIRELESS (GUEST)	Seguridad
IM0082972	Dashboard	DASHBOARD-DATOS-FALTA CAPA 4 EN DASHBOARD DE KUO	Seguridad
IM0078873	Service Manager	CUICUILCO-SEGURIDAD CMDB	Seguridad

Tabla 2. Incidentes de seguridad; Herramientas
Fuente: (Cnvrep003\ Doc_Trabajo\Incidentes_Vs_Vulnerabilidades, 2015)

Se realizó una prueba a los servidores principales de monitoreo junto con la IP y el dominio al que pertenece cada servidor para tratar de vulnerar el sistema y poder proponer acciones a seguir (ver Tabla 3).

Host	Dirección IP	Sistema operativo	Rol	¿Vulnerado?	NR [1]
enduserexp.cnoc.telmexit.com	189.254.230.182	Linux 2.6	BMC End User Experience Management	No	Alto
proactivenet.cnoc.telmexit.com	189.254.230.183	Microsoft Windows Server 2008 R2	BMC ProactiveNet	Si (BMC ProactiveNet)	Alto
discovery.cnoc.telmexit.com	189.254.230.184	Linux 2.6	BMC Atrium Discovery Appliance	Si (BMC Atrium Discovery Appliance)	Alto
cmdb.cnoc.telmexit.com	189.254.230.185	Microsoft Windows Server 2008 R2	BMC Remedy Mid Tier	Si (BMC Remedy Mid Tier)	Alto
capacity.cnoc.telmexit.com	189.254.230.187	Linux 2.6	BMC Capacity Optimization	Si (BMC Capacity Optimization)	Alto
cnvtelmexit001.cnoc.telmexit.com	189.254.230.166	Linux 2.6	Power DNS	No	Alto
ftp.cnoc.telmexit.com	189.254.230.190	Linux 2.6	Secure FTP	No	Alto
customer-189-254-230-200-sta.uninet-ide.com.mx	189.254.230.200	Linux 2.6	NMIS	No	Alto
lan-d32-0912-0155.uninet-ide.com.mx	187.141.47.161	Linux 2.6	Dashboard	No	Alto
customer-187-141-47-162-sta.uninet-ide.com.mx	187.141.47.162	Linux 2.6	Dashboard	No	Alto
cnvmail001.cnoc.telmexit.com	189.254.230.186	Linux 2.6	Postfix Dovecot Mysql	No	Alto

Tabla 3. Penetración de servicios y/o servidores
Fuente: (Cnvrep003\ Doc_Trabajo\Penetración_Servidores, 2015)

En la Tabla 3, se puede apreciar en el campo “¿Vulnerado?”, los sistemas que no están cumpliendo el estándar y que son de alta criticidad para ser atendidos y que se les dé una solución inmediata, ya que de esto depende la seguridad de los clientes que tiene la empresa.

De las herramientas afectadas, se encuentran NMIS y iDashboard; cabe resaltar que estas son las únicas herramientas dentro del alcance del proveedor y que posiblemente ayuden a resolver sus respectivas vulnerabilidades.

Así mismo, de la Tabla de penetración de servicios y/o servidores, descritos en la Tabla 3, se destacan las siguientes tareas que se deben atender de inmediato, ya que implican un riesgo para Care Enterprise Networks:

- Revisión de la divulgación de información sensible en servicios WEB
- Revisión de puertos abiertos
- Revisión de tráfico en claro en servicios WEB
- Revisión de usuarios por default
- Revisión de trafico de http a https
- Revisión de puertos de uso y puertos de monitoreo
- Bloqueo de puertos que no son utilizados
- Bloque de ip’s o segmentos que no sean permitidos para su acceso
- Colocar listas de acceso in & out

1.4 Análisis de capacidad y madurez de la empresa

Con base en el plan de negocio de Care Enterprise Networks, desde su origen ha tenido como objetivo migrar a su operación las redes administradas que actualmente son gestionadas por proveedores externos, las cuales representan un universo de 36,000 dispositivos de red monitoreables; este objetivo se pretende lograr durante los primeros cinco años de operación (del 2011 al 2016).

Adicionalmente se prevé proporcionar servicios a clientes nuevos, lo que se estima represente 9000 dispositivos monitoreables a lo largo de los primeros 5 años de su operación. Sin embargo, debido al crecimiento de clientes se ha ido modificando la proyección, ya que se han incorporado distintos proyectos de migración de clientes al centro de operación, tal es el caso de clientes internacionales.

Con base en lo anterior, se pronostica un total aproximado de 60,135 dispositivos a monitorear a lo largo de los 5 primeros años de operación.

Por otro lado, se considerarán los cambios contractuales provenientes del área comercial, cambios organizacionales provenientes de Recursos Humanos, impactos financieros, impactos potenciales estatutarios y regulatorios provenientes de la dirección, y todo referente a capacidad.

Con base en los dispositivos que se tiene en monitoreo al cierre del año 2015, se logró estimar la penetración que ha tenido Care Enterprise Networks en el mercado de Redes y comunicación de TI (ver Tabla 4).

Tipo de Nodo	Nodos monitoreables	Total
MPLS	15,576	$ 37, 382, 400
IDE	9,987	$ 23, 968,800
ADSL	1,123	$ 2, 695, 200
PEX	225	$ 540, 000
Total	26,911	$ 64, 586, 400

Tabla 4. Dispositivos monitoreables vs Ventas netas 2015
Fuente: (Cnvrep003\ Finanzas\Dispositivos monitoreables Vs ventas, 2015)

De acuerdo al total de ventas del 2015, y de acuerdo al objetivo del plan de negocio, se tienen los siguientes puntos de fortalecimiento y madurez:

- Care Enterprise Networks tiene el 45% del mercado esperado hasta 2015.
- Care Enterprise Networks requiere reforzar la penetración en el mercado, implementando nuevos productos, nuevas tecnologías, procesos y fortalecimiento de la seguridad de la información.
- Care Enterprise Networks necesita recuperar los clientes perdidos que representan 3% del mercado, ya que estos clientes decidieron regresar con su antiguo proveedor debido a los ataques cibernéticos que sufrió la empresa el pasado mes de noviembre del 2015.
- Care Enterprise Networks requiere un plan de fortalecimiento en el área de TI con respecto a seguridad de la información, para recuperar el 3% del mercado perdido y penetrar con mayor fuerza en el mercado.
- Care Enterprise Networks requiere fortalecer los puntos críticos de cada área de la empresa y madurar el monitoreo y seguridad TI.
- Care Enterprise Networks necesita invertir en personal con skill especializado en el área de TI y operaciones. Inversión proyectada del 15% para personal con respecto a ventas netas de 2015.
- Care Enterprise Networks requiere de un proveedor que identifique los puntos medulares de ataque, así como amenazas y vulnerabilidades para proponer una nueva concepción del área de TI, así como la emisión de nuevas propuestas que ayuden a dar confianza al cliente. Inversión proyectada del 17%.
- Care Enterprise Networks requiere de nuevo software y hardware para aumentar su capacidad y aunado a ello, productos que ayuden a contrarrestas los ataques cibernéticos. Inversión proyectada 13%.

1.5 Descripción del problema

La empresa Care Enterprise Networks carece de medidas de protección para salvaguardar la información de los clientes, basadas en las TI. Es por ello que debe diseñarse una propuesta que ayude a evitar el robo de información, robo de identidad, ciberataques, phishing, backdoors, keyloggers, sniffers, gusanos, troyanos, spyware, spam, invasión a la privacidad, extracción de datos y llenar huecos muy importantes que se tienen, ya que desde su inicio sólo se visualizó el tener procesos basados en buenas prácticas.

Al paso del tiempo, la empresa, con el afán de captar más clientes, ha identificado que requiere de una robusta seguridad de la información, para evitar que se realicen robos de información por varios métodos que no mitigan las políticas y controles establecidos hoy en día.

No basta tener equipos de comunicación que eviten ataques o software dedicados a detectarlos, sino que es necesario establecer políticas y controles adecuados mediante un análisis de riesgos, amenazas y vulnerabilidad del hardware y software.

El subgerente de operación y el gerente de la empresa han recibido quejas de los clientes relacionadas con la seguridad de la información, ya que su inconformidad es acerca de la baja seguridad de la información, pues la empresa no cuenta con las políticas y controles adecuados, así como el software y hardware especializado para poner alto a las amenazas y vulnerabilidades que hoy atañen a la empresa. Las quejas han ido en aumento a través de los 5 años que tiene la empresa en el mercado, (ver Gráfica 1).

Grafica 1. Quejas por año
Fuente: (Repositorio de Care Enterprise Networks: Cnvrep003\CEN\Quejas)

Algunos de los problemas que hoy día enfrenta Care Enterprise Networks, es que las TI tanto en hardware como en software no están siendo aplicadas de forma adecuada; la forma de constatar esto, es que los ataques cibernéticos han sido constantes y afectan de manera directa y contundente la información de sus clientes.

Uno de los más recientes problemas fue la falta de políticas en un firewall de la infraestructura de Care Enterprise Networks, lo que ocasionó que un cliente tuviera una pérdida monetaria por más de 1 millón de pesos, debido a que al momento del ataque, el hacker se infiltró y pudo obtener números de cuenta e información confidencial del cliente. Esta situación generó enojo, frustración y descontento en el cliente, al verse vulnerado por el ataque que sufrió y por la pérdida monetaria que causó impacto en su negocio.

Care Enterprise Networks, en su concepción, se centró en las mejores prácticas basadas en el marco de referencia de ITIL (Information Tecnology Infraestructure

Library); sin embargo, dejó de lado el robustecimiento de la buena aplicación de las TI tanto en software como en hardware.

Las políticas y controles que se tienen actualmente son deficientes y cuentan con limitaciones, como son:

- Debilidades en la infraestructura tanto a nivel hardware y software
- Falta de recursos
- Expertise de los especialistas tanto en hardware como en software
- Llevar el control de cambios implementados bajo supervisión
- Tener una revisión de los cambios efectuados en los equipos, tanto a nivel software como hardware.
- Políticas débiles aplicadas en software
- Controles insuficientes para la seguridad
- Falta de análisis de amenazas y vulnerabilidades
- Ineficiencia de políticas que controlan la red de la empresa
- Inconsistencias en la CMDB que puede provocar cambios mal aplicados
- Falta de procesos y procedimientos que ayuden a mejorar la seguridad de la información en las TI.

Esta lista de limitaciones, políticas y controles ineficientes, ha provocado la continua queja de los clientes ante la subgerencia de operaciones y la gerencia general. Por tal motivo se requiere una propuesta que aumente la seguridad de la información y conlleve a la satisfacción y confianza del cliente, y el aumento de la cartera de cliente para Care Enterprise Networks.

1.6 Enunciado del problema

La inadecuada aplicación de las TI en Care Enterprise Networks, tiene como consecuencia una baja seguridad de la información que conlleva a mayores amenazas y vulnerabilidades en el robo de la información de la empresa.

1.7 Objetivo general

Elaborar una propuesta de seguridad de la información con base en las TI, que minimice las amenazas y vulnerabilidades que atañen al robo de información en la empresa Care Enterprise Networks.

1.8 Objetivos específicos

1. Analizar las políticas y controles implementados en la empresa que llevan a la baja seguridad de la información.

2. Identificar las tecnologías de la información que utiliza la empresa y que benefician y/o afectan la seguridad de la información. Así como las TI que ayuden a garantizar la seguridad de la información

3. Identificar las amenazas y vulnerabilidades de seguridad de la información en la empresa con el fin de contar con elementos que apoyen la propuesta de seguridad de la información.

4. Diseñar una propuesta de seguridad de la información con base en las TI que ayude a reducir las amenazas y riesgos de la información de la empresa.

1.9 Preguntas de investigación

¿Cómo afectan las políticas y controles implementados en la empresa que llevan a una baja seguridad de la información?

¿Qué tecnologías de la información están implementadas y vinculadas con la seguridad de la información en la empresa?

¿Cuáles son las amenazas y vulnerabilidades de seguridad de la información que atañen a la empresa?

¿Qué elementos debe contener la propuesta de seguridad de la información con base en las TI que ayude a reducir las amenazas y riesgos de la información de la empresa?

1.10 Justificación

Cuando se maneja información mediante las TI, la seguridad de la información se convierte en una necesidad, la cual debe de cubrir los principios de la seguridad, tales como: confidencialidad, disponibilidad e integridad; de esta manera se puede asegurar que la información no tenga alteración en los sistemas, ataques y accesos no autorizados. Por lo anterior, una propuesta de seguridad de la información puede ser la base para que cada usuario tenga una protección en la red de la empresa.

Con la aplicación de la identificación de riesgos, amenazas y una propuesta para aumentar la seguridad en la información, se evalúan las prácticas de seguridad informática en una organización para que obtenga el control total de la información y se genere la responsabilidad en cada persona por la información que maneje. Lo anterior propiciará que exista un sentido de conciencia del funcionamiento adecuado de la red y el resultado será el control de los datos de la organización.

Las empresas actualmente manejan su información y la administran por medio de software y hardware, por lo que es necesaria la evaluación de riesgos de la información para proteger su integridad y cumplir con los controles de políticas de seguridad. Así, la

propuesta de seguridad que se derive de esta investigación, pretende evitar pérdidas de información, fundamentada en el establecimiento de controles e implantación de procedimientos y métodos, que minimicen los riesgos, amenazas y vulnerabilidades en la seguridad de la información de cualquier organización. El propósito es administrar y proteger el activo de la información y evitar que las amenazas se materialicen en la empresa. Así, el desarrollo de normas de seguridad en la empresa es posible, ya que se tienen marcos de referencia para implementar los controles específicos de seguridad con la incorporación de las nuevas Tics para salvaguardar la información confidencial de los usuarios de la organización y de los clientes. De no implementar normas de seguridad, se pueden presentar robos de información y con esto existe la posibilidad de que la empresa tenga pérdidas en sus proyectos de desarrollo, en sus bancos de datos y, por ende, incumpla sus objetivos, afectando sus resultados.

Si se adoptan medidas adecuadas para asegurar la información de las Tics, será posible tener una defensa idónea que proteja los activos de información. Por otra parte, esto repercutirá en el uso íntegro de las Tics y se favorecerá que otras empresas tomen como referencia el caso de la empresa estudiada para así implementar controles que minimicen los riesgos del negocio.

CAPÍTULO 2. Las TI y la seguridad de la información

2.1 Tecnologías de la información

A través de nuestra historia la tecnología ha sido parte de nuestras vidas, pues desde los orígenes de la humanidad se ha manipulado la naturaleza a través de técnicas y métodos que permitieron mejorar los niveles de vida de las personas. En el presente capítulo, el interés se centra en ubicar algunas etapas del desarrollo de la tecnología, con el fin de llegar a definir la etapa actual en la que se encuentra el desarrollo de ésta.

En la evolución de la sociedad, el desarrollo de la tecnología ha tenido un papel preponderante, por ello se cita a Cabero (2001) que a la letra dice “la historia de las civilizaciones es en cierta medida la historia de sus tecnologías, y nunca hasta la fecha había existido una relación tan estrecha entre las tecnologías y la sociedad, y nunca la sociedad se ha visto tan influenciada por las diferentes tecnologías que están apareciendo; siendo éstas, las TIC, las que más destacan sobre todas las tecnologías”. Aludiendo a esta cita, se cree que en el tiempo pasado la influencia de las tecnologías en nuestras vidas pasaba desapercibida porque en la mayoría de los casos el beneficio de éstas era de manera indirecta, sin embargo, hoy en día palpamos la tecnología en todo momento de la vida cotidiana.

Retomando la revisión de distintas concepciones sobre el desarrollo de la tecnología, en el siglo X y el Siglo XIII, Mumford (2000) señala que “durante los últimos mil años la base material y las formas culturales de la civilización occidental han sido profundamente modificadas por el desarrollo de la máquina”. En esta época hubo un desarrollo importante de lo que se concebía como “la máquina”, así como de la técnica misma para usarla. Pero señala que es durante la revolución industrial cuando los cambios son más radicales sobre el uso de la máquina y la técnica misma. Aludiendo a la revolución industrial, es en ésta época en la que se modificaron los sistemas de producción, se manifestó fuertemente una revolución demográfica, se modificó la estructura social, se gestaron nuevas clases sociales como consecuencia implícita del desarrollo tecnológico. Los obreros de esta época protestaron por lo que consideraron

una amenaza para su trabajo. En la actualidad, las tecnologías también están provocando cambios significativos en el empleo, en la educación, en las comunicaciones y en general en la forma de vida de la sociedad.

Ahora bien, veamos otra postura sobre las etapas clave en el desarrollo de la tecnología. Lévy (2005), señala que la revolución tecnológica alcanzó su pleno desarrollo a principios del siglo XVIII, con el descubrimiento de la máquina de vapor, y con ello su utilización inmediata en los trasportes fluviales, marítimos y terrestres. Todo esto transformó en poco tiempo todo el tejido social. Para Levy, la revolución industrial del siglo XIX es considerada como la segunda revolución. La tercera revolución, en plena expansión, se basa en el uso de las tecnologías informáticas en el mundo de los intercambios globales. Por consiguiente, menciona también que la Revolución Industrial como la postindustrial ha influido no sólo en la vida cotidiana, sino también en las capacidades intelectuales del ser humano. Se observa aquí que aparece el concepto de “las tecnologías informáticas”.

Otra postura interesante sobre las etapas de desarrollo de las tecnologías es la de Kerckhove (1999a, en Solano, 2003). Este autor identifica dos grandes bloques. El primero, lo referencia como la escritura, la aparición del alfabeto griego a partir del 1000 a. J.C y la imprenta hacia el año 1440. En el segundo bloque, hace referencia a los avances tecnológicos (radio, televisor, computadora, interactividad y multimedia online), inventados en un margen de más de cien años (desde 1887, fecha del descubrimiento por Hertz de la radiación electromagnética), los más recientes pertenecen al ámbito de las telecomunicaciones y la telemática.

Solano (2003) manifiesta que Kerckhove considera que existen una serie de sesgos que reflejan la evolución de la tecnología. Considera que los cambios más significativos se han dado en el tercer sesgo con la llegada de la imprenta que da paso a la mecanización; en el cuarto sesgo la radio y televisión, dan paso a la cobertura mundial de la comunicación. La computadora, quinto sesgo, que desde esta postura es el punto de partida hacia las nuevas tecnologías, en el marco de referencia de esta clasificación.

Desde esta perspectiva, en el sexto sesgo se deja ver las tecnologías actuales, concretamente Internet (ver Figura 1).

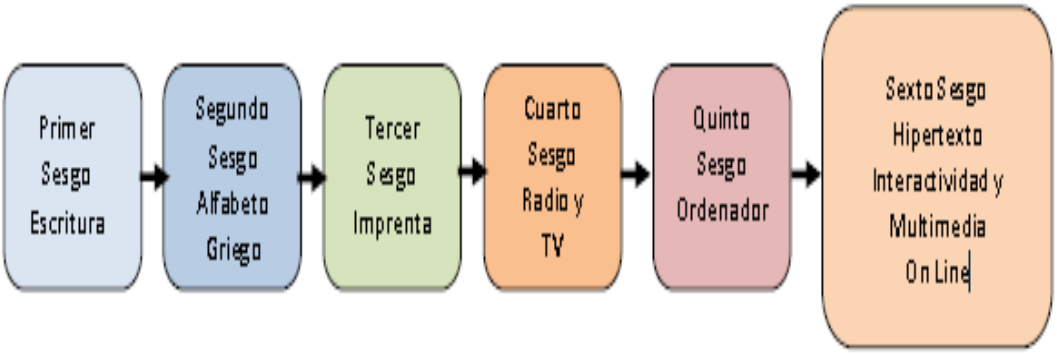

Figura 1. Sesgos de la evolución de la tecnología
(Fuente: Los sesgos de la evolución tecnológica, Solano, 2003)

Estas concepciones, en lo general, permiten ver aquellas etapas clave en la historia del desarrollo de las tecnologías. De esto se identifica que la máquina, la escritura, la imprenta, y las TIC han sido las etapas determinantes en la evolución de la sociedad, y que la Revolución Industrial es el punto de partida para un desarrollo acelerado de las tecnologías que por sí mismas no son determinantes de la evolución de la sociedad, sino que más bien hay una relación de interdependencia entre la tecnología y el factor humano, de tal forma que las primeras, para que nazcan, necesitan de un contexto social específico y, al mismo tiempo con su presencia, configuran nuevos modelos y escenarios sociales, culturales y económicos. Por tanto, bien cabe lo que menciona Cabrero (2007) que: “las tecnologías no son ni autónomas ni independientes respecto a las fuerzas sociales que las han creado, y al mismo tiempo configuran nuevas formas de relación”.

En el siglo XX, se desarrolla fuertemente el campo de la electrónica, las comunicaciones, el desarrollo de la informática, las redes telemáticas y de la comunicación. El siglo XX permite hablar de nuevas tecnologías. Pero es tan acelerado el cambio de la tecnología que el sustantivo nuevo es un concepto efímero, es decir, lo que hoy es nuevo, también, hoy deja de serlo. El tiempo de vida de una “nueva”

tecnología es casi perecedero por la acelerada evolución de la misma, cuando una nueva tecnología se integra, apenas ésta se posiciona, ya se desarrolló otra que bien puede sustituirla.

La intención en este orden de ideas, es llegar a comprender la concepción de la tecnología en la sociedad actual y principalmente cuál es su verdadero papel en el ámbito de las organizaciones. De todas las tecnologías que han surgido en los últimos tiempos, Internet se ha convertido en una tecnología fundamental para la innovación y desarrollo de los procesos productivos y educativos; así que en el devenir histórico de las etapas trascendentes del desarrollo de la tecnología, bien vale la pena revisar de forma muy general el desarrollo de la red de redes. Ésta es otra tecnología que caracteriza a la hoy llamada Sociedad de la Información y del Conocimiento y, también es una tecnología que ha generado innovaciones en la educación. Desde un punto de vista, esta sociedad será considerada como una etapa significativa que será señalada en la historia de la evolución social. Puesto que como ya se mencionó, la historia de la tecnología es la historia de la humanidad misma.

Para concluir con las etapas clave en el desarrollo de la tecnología, se denota que en la sociedad actual las últimas etapas significativas que pudieran señalarse son: el surgimiento de las computadoras y el Internet y a partir de ello el desarrollo de la Informática, por lo cual se presenta un resumen muy general del desarrollo de éstas.

La seguridad informática consiste en el resguardo de la información que se maneja por medios magnéticos, incluida en archivos personales, privados, organizacionales, financieros, políticos, ambientales, estadísticos, institucionales, entre otros. En este sentido diversas organizaciones han dedicado esfuerzos a desarrollar planes de acción para resguardar y proteger su información.

En Estados Unidos, el Instituto de Seguridad de Computadoras (CSI) publicó la Encuesta Mundial del Crimen y la Seguridad en las Computadoras, con participación de la Escuadra de Intrusión en Computadoras de la Oficina Federal de Investigaciones (FBI) en San Francisco. Esa encuesta, aplicada en 2005, reportó pérdidas por

aproximadamente 378 millones de dólares, que fueron resultado de graves violaciones de seguridad, principalmente, a las computadoras de grandes corporaciones, agencias de gobierno y universidades. Las violaciones de seguridad detectadas por los encuestados incluyen una gama diversa de ataques tales como: acceso no autorizado por parte de personal de la misma entidad, negativa de servicio, penetración de sistemas de elementos ajenos a la entidad, robo de información protegida por derechos de propiedad intelectual, fraude financiero y sabotaje de datos y redes.

Para hacer frente a posibles violaciones de seguridad, se diseñaron los sistemas de Control Supervisor y Adquisición de Datos (SCADA) que son particularmente vulnerables cuando se usa el internet para vigilar y controlar procesos en sitios distantes. Esta práctica es empleada por industrias como la química, petroquímica, petróleo y gas, de alimentos, pulpa y papel, productos farmacéuticos, agua y aguas servidas, transporte, administración de energía y otras aplicaciones manufactureras.

En la última década, la seguridad cibernética ha comenzado a tomar relevancia en todo el mundo; en México los ataques cibernéticos pasaron del cuarto, al tercer lugar según SYMANTEC (empresa dedicada a la seguridad en internet). De acuerdo con Trend Micro México (empresa dedicada a la seguridad de contenidos en internet), en 2014, los ataques cibernéticos aumentaron un 40%.

Un estudio de Joint Future Systems en 2011, realizado en las principales ciudades de la República Mexicana (Distrito Federal, Guadalajara, Monterrey), arrojó que casi “58.6% de los informáticos no conocen normas o regulaciones que mejoren la seguridad en informática”. Por tal motivo el país se encuentra en desventaja en relación con otras naciones, ya que la difusión y la cultura de seguridad informática es deficiente.

De los ataques registrados, uno de los más importantes tuvo lugar en abril de 2004 a Banamex, donde, a través de internet, unos delincuentes hicieron transferencias bancarias ilegales por más de 516 millones de pesos y uno de los empleados era

cómplice del fraude. Otro fue en mayo 2003 en el IFE, donde un colaborador en informática, de la empresa Vanguardia, sustrajo ilegalmente el padrón electoral y lucró con éste con la empresa estadounidense Choice Point. Aunque en la actualidad 98% de las empresas del mundo utilizan programas antivirus, durante 2004, más del 90% tuvo problemas relacionados con el spyware y phishing, por lo que los expertos señalan que un minuto de tiempo de ataques es igual a una hora de esfuerzo de limpieza.

Para la propuesta de identificación de riesgos en internet y el robo de información personal y bancaria, la US-CERT (*United States Computer Emergency Readiness Team*), publicó que es importante identificar las tendencias de los ataques y la vulnerabilidad que ocasionan, aquí también señala que los ataques se han sofisticado para el robo de información en sitios web apócrifos, por lo que se deben adoptar los cuidados pertinentes para no caer en estos sitios.

De acuerdo con UNISYS, organización que ayuda a empresas y organismos públicos en la aplicación de las tecnologías de información para conseguir los más elevados niveles de competitividad y éxito, señaló que en 2007, en México, las pequeñas y medianas empresas aún distaban de alcanzar niveles óptimos de infraestructura informática y que estaba lejano establecer estrategias en cuanto a la seguridad, ya que esto dependía del entorno económico y de las políticas de incentivos financieros y fiscales que les permitieran crecer en las TICs (tecnologías de la información). Sin embargo, México podría ser el segundo país del bloque latinoamericano que obtuviera un alto crecimiento en inversión en tecnologías de seguridad, al llegar al 10% en relación con el 13% que tenía Brasil.

Entre las empresas importantes en este rubro, se encuentra *Systematics* de México S. A., organización dedicada a los servicios y soluciones de tecnología de información. El equipo de desarrollo de la empresa combina la experiencia en integración de sistemas con un enfoque preciso y ejecución impecable para ayudar a sus clientes a alcanzar ventajas en su control administrativo y recursos de comunicación en forma rápida y eficaz. Sin embargo esta agrupación se muestra reacia a admitir que sus sistemas han

sido saboteados o violados por miedo a dañar su reputación y admite que nunca ha emprendido acciones legales.

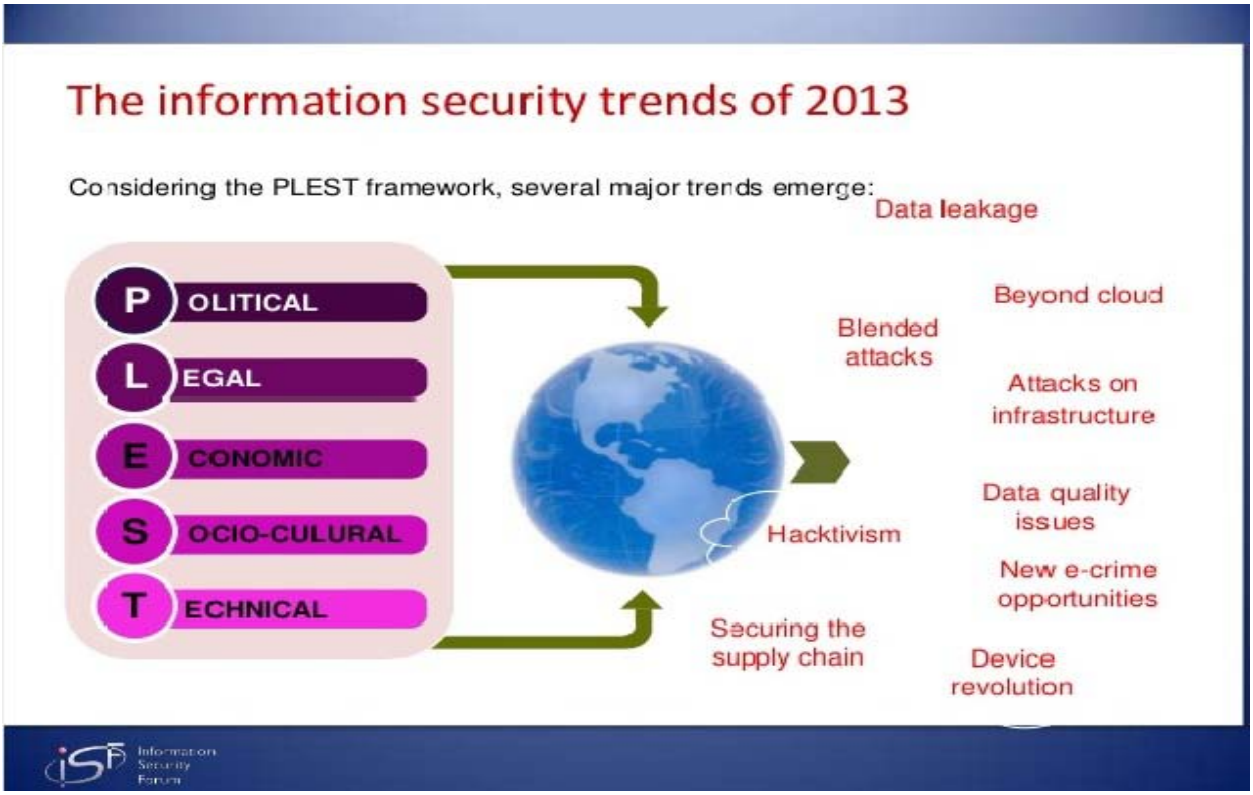

Figura 2. The information security trends of 2013
Fuente: (https://www.securityforum.org)

2.1.2 Origen y desarrollo de la red de redes (Internet)

Como señala Castells (2001), los orígenes de Internet hay que situarlos en ARPANET, una red de ordenadores establecida por ARPA (Advanced Research Projects Agency) en septiembre de 1969, agencia de proyectos de investigación avanzada fundada por el Departamento de Defensa de Estados Unidos en 1958. Todo ello con el fin de alcanzar la superioridad tecnológica militar, sobre la Unión Soviética.

ARPANET, fue un programa menor surgido en uno de los departamentos de ARPA, llamado: Información Processing Techniques Office (IPTO), el objetivo de este Departamento era estimular la investigación en el campo de la informática interactiva.

Para establecer una red de informática interactiva IPTO, se basó en una revolucionaria tecnología de trasmisión de telecomunicaciones y la conmutación de paquetes (packet switching).

En 1969 los primeros nodos de la red se encontraban en la Universidad de California en los Ángeles, en el SRI (Stanford Research Institute), en la Universidad de California de Santa Bárbara y en la Universidad de Utah. En 1971 había un total de 15 nodos de los cuales la mayor parte eran centros de investigación universitarios.

El diseño de ARPANET lo llevó a cabo BBN (Bolt, Beranek y Newmann), una empresa de ingeniería acústica de Boston, que se había pasado a la informática aplicada.

En 1972 tuvo lugar la primera demostración con éxito de ARPANET durante un congreso internacional en Washington D.C. El siguiente paso fue posibilitar la comunicación de ARPANET con otras redes de ordenadores como PRNET Y SATNET que ARPA estaba gestionando. A partir de entonces se introdujo un nuevo concepto la red de redes. En 1973 Robert Kahn y Vint Cerf esbozaron la arquitectura básica de Internet basándose en el diseño de Network Working Group, un grupo técnico corporativo formado en los años sesenta y que se conectaban mediante ARPANET.

Para lograr que las redes de ordenadores pudieran comunicarse entre ellas, fue necesario un protocolo de comunicación estandarizado. Así que en 1973 se consiguió alcanzar parcialmente este objetivo, gracias al diseño del Protocolo de Control de Transmisión (TCP: Transmission Control Protocol). En 1978 se crea el protocolo TCP/IP estándar sobre el que aún opera Internet.

El Departamento de Defensa de Estados Unidos había decidido comercializar la tecnología Internet financiando la inclusión del TCP/IP en los protocolos de los ordenadores fabricados por empresas norteamericanas en los años ochenta.

En febrero de 1990 ARPANET, tecnológicamente obsoleto, fue desmontado. Para entonces la mayor parte de los ordenadores de Estados Unidos estaban capacitados para funcionar en red, sentando así las bases para su interconexión.

Para el año 1995, se da paso al uso privado de Internet. Ahora bien, señala Castells (2001), ARPANET no fue la única fuente para la constitución de Internet tal y como se conoce hoy. Internet es también el resultado de una tradición de interconexión informática autónoma y alternativa. Por ello se explica brevemente aquellos eventos que también fueron contundentes para llegar a lo que hoy conocemos como Internet.

Los Tablones de Anuncios Electrónicos (BBS: Bulletin Board Systems) forman parte de esta tradición, pues fueron producto de la conexión en red de los PC a finales de los años setenta. En 1997, dos estudiantes Ward Chritem y Randy Suess, diseñan un programa al que denominaron MODEM, este programa permitía la transferencia de archivos entre sus PC y decidieron hacerlo público. En 1983, Tom Jennings creó su propio programa BBS, FIDO, y puso en marcha una red de BBS, FIDONET.FIDONET. Castells (2001), considera que sigue siendo la red de comunicación informática más barata y accesible del mundo, basada en la utilización de PC y que en el 2000 contaba con 40,000 nodos.

El uso de la red BBS y la cultura simbolizada por FIDONET, fueron de gran influencia para la configuración de Internet. En 1981, Ira Fuchs y Greydon Freeman iniciaron una red experimental basada en el protocolo IBM RJE, construyendo así una red para usuarios de IBM, que se le llama BITNET (Because It’s There o Because it’s time), esta red estaba ubicada principalmente en las universidades. No obstante a todo este desarrollo y a la participación de los distintos expertos ya mencionados, la comunidad de usuarios de UNIX fue representativa y decisiva en la conexión informática en red.

En 1978, los laboratorios Bell distribuyeron un programa UUCP, copia de UNIX a UNIX (UNIX-to-UNIX copy) que permitía copiar archivos de un ordenador a otro. En 1979 cuatro estudiantes de Carolina del norte (Truscott, Ellis, Bellavin y Rockwell) diseñaron un programa para la comunicación entre ordenadores UNIX, y para el año 1980 lo

difundieron gratuitamente. Esto permitió la formación de redes de comunicación de ordenadores, dando paso a Usenet News, fuera del eje troncal de ARPANET, extendiéndose con ello la práctica de la comunicación informática. Usenet News llegó en 1980 al departamento de Informática de la Universidad de Carolina, en la que existía un nodo ARPANET, por lo que un grupo de estudiantes doctorandos (Mark Horton y Bill Joy y otros) que trabajaban en adaptaciones y aplicaciones de UNIX, desarrollaron un programa para tender un puente entre las dos redes, a partir de ese momento USENET quedó ligada a ARPANET y estas dos tradiciones fueron unificándose gradualmente, permitiendo que varias redes informáticas pudieran comunicarse entre ellas, compartiendo con frecuencia el mismo eje troncal (cortesía de alguna universidad), fue así que estas redes terminaron uniéndose dando así el paso a lo que hoy es Internet. Y en 1990 la world wide web, hizo posible que Internet abarcara a todo el planeta. La world wide web es una aplicación para acceder a la información y fue desarrollada por Tim Berners-Lee.

Respecto al desarrollo de otras tecnologías, en las décadas de los 50 y 60 los ordenadores permitían acumular y procesar grandes cantidades de datos, estos eran principalmente cifras, palabras y sonidos. La capacidad de transformarlos en información era un gran desafío y lo que se podía hacer con estos datos determinaba el valor de los mismos.

La década de los 70’s da la pauta a la revolución electrónica y constituye el punto de partida para el desarrollo de la era digital. Las investigaciones desarrolladas en los años 80 ocasionaron la convergencia de la electrónica, la informática y las telecomunicaciones, posibilitando así la interconexión entre redes y por tanto la comunicación. Como dato trascendente la empresa IBM en 1981 puso el primer ordenador PC en el mercado. Hoy las TIC pueden permitir desde servicios básicos como la telefonía, el correo electrónico, hasta aplicaciones más complejas, como por ejemplo, la telemetría que permite supervisar a distancia las condiciones de agua como parte de un sistema de pronóstico de inundaciones.

En la década de los 80 los microprocesadores permitieron un avance importante y, los datos pudieron ser procesados y utilizados de forma más fácil. El rápido acceso al significado de estos datos se convirtió en algo relevante e importante. Desde entonces los datos siguen siendo la base de cualquier situación, pero no tienen significado si estos se convierten en conocimiento. Hoy, el reto continúa y, es cuando se puede seleccionar y convertir la información en conocimiento.

A partir de esta década ha sido desenfrenado el desarrollo de la tecnología y su implementación en los distintos procesos que constituyen el desarrollo de la sociedad. Para concluir, es importante mencionar que hoy las tecnologías permiten un acceso abierto a la información, se democratiza la información, se superan las barreras del espacio y el tiempo, se digitaliza la información, y por tanto se facilita la distribución de la misma y de esta forma se contribuye a la difusión del conocimiento y, a su vez, todo esto ha permitido flexibilizar los procesos formativos, que es uno de los puntos de interés.

No obstante, de todos estos beneficios es necesario reflexionar sobre el hecho de quiénes son estas tecnologías y cuáles son sus efectos (positivos y negativos también) y beneficios que aportan a la sociedad. Es frecuente que cuando se habla de tecnologías, aparezca la idea de beneficios, prejuicios o también, como dice Martínez (2007) “de bondad o maldad de las mismas, tratando de evaluar las consecuencias de su aplicación en la sociedad de la información”. Lo importante es ser conscientes y responsables del desarrollo de las tecnologías y del uso que se les da. Por ello, se debe conocerlas y saber cuál es su utilidad en beneficio de la sociedad y de acuerdo con el contexto para el que fueron inventadas aquellas tecnologías que por su especificidad propia, benefician y mejoran el desarrollo de las organizaciones y los sistemas educativos. Por ello se revisa y se plantean algunas concepciones y características de las TIC en la sociedad actual.

2.1.3 Características y posibilidades de las TI

El concepto de TIC surge como convergencia tecnológica de la electrónica, el software y las infraestructuras de telecomunicaciones. La asociación de estas tres tecnologías da lugar a una concepción del proceso de la información, en el que las comunicaciones abren nuevos horizontes y paradigmas, sobre todo para el contexto educativo.

Las TIC es una expresión que engloba una concepción muy amplia y a su vez muy variable, respecto a una gama de servicios, aplicaciones y tecnologías, que utilizan diversos tipos de equipos electrónicos (hardware) y de programas informáticos (software), y que principalmente se usan para la comunicación a través de las redes. De forma breve, se describe cada uno de estos elementos.

- **Los servicios** de telecomunicación como la telefonía e Internet, que se utilizan combinados con soporte físico y lógico para constituir la base de muchos otros servicios, como el correo electrónico, la transferencia de archivos, la videoconferencia, el Chat, los foros de discusión, news o newsgroups, IRC (Internet Relay Chat), entre muchos.

- **La tecnología** se puede señalar de las precursoras, la que se usa en el teléfono, radio y televisión. Las actuales se refieren a comunicaciones móviles. Por ejemplo el mismo tipo de tecnologías que se utilizan para trasmitir la voz pueden también trasmitir el fax, datos y el vídeo de compresión digital.

- **Las redes** son aquellas que usan cable de cobre, cable de fibra óptica, cable coaxial, conexiones inalámbricas, telefonía celular y los enlaces por satélite.

- **Por equipos** se entiende el hardware y hay una gama muy amplia. Por ejemplo los ordenadores y todos los equipos que se utilizan para la conectividad de la red y para la comunicación.

- **Los programas informáticos** (software) que son el fluido de todos estos elementos.

Pero más allá de esta percepción sobre las TIC, a continuación se referencian algunas de las distintas definiciones que se han dado en el tiempo y no por ello las no expuestas aquí dejan de ser trascendentes. Ahora bien, no hay un consenso entre los profesionales de la educación sobre una definición absoluta de las TIC. Hoy también se habla de nuevas tecnologías para referirse a las TIC como medios que giran en torno a la informática, la microelectrónica, los multimedia y las telecomunicaciones.

Es interesante el análisis que hace Cabero (2001) sobre las concepciones de diferentes autores (ver Tabla 5).

Concepciones de las tecnologías	
Ortega, (1997)	Discrimina entre tecnologías convencionales (diaporamas, audiovisuales y prensa) y tecnologías avanzadas (diseño y animación informática, acceso a bibliotecas virtuales y navegación a través de redes,)
Tirado (1997)	Distingue entre nuevas tecnologías y tecnologías avanzadas, indicando que las últimas son aquellas que poseen respeto a las anteriores los atributos de interactividad multimedia frente a la interactividad mono media de las denominadas "nuevas", y susceptibilidad de flexibilidad espacio-temporal frente a la flexibilidad espacial y temporal.
Cabero y Martínez (1995)	hablan de nuevos canales de la comunicación en vez de nuevas tecnologías, ya que estas suelen implicar la utilización de tecnologías tradicionales, pero con usos diferentes y novedosos, es decir, se refiere a la integración de las tecnologías anteriores, pero de una forma tanto cuantitativa como cualitativa
Adell (1997)	Las nuevas tecnologías son: El conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizados de la información.
Duarte y Gonzalez(1998)	Las nuevas tecnologías son aquellos medios electrónicos que crean, almacenan, recuperan y trasmiten la información cuantitativamente veloz y en gran cantidad, y lo hacen cambiando diferentes tipos de códigos en una realidad hipermedia
Pérez (1997)	Al hablar de nuevas tecnologías deberíamos contemplar, por una parte, una dimensión técnica, y por otra, una expresiva, repercutiendo ambas en la creación de nuevos entornos comunicativos.
Sáez Vacas (1999)	Las tecnologías de la información comprenden el conjunto formado por las telecomunicaciones y la informática y todos sus antecedentes y consecuentes (microelectrónica, redes de ordenadores, ofimática, groupware, red Internet, tecnologías del multimedia, etc.), conjunto que, como infraestructura creciente en tamaño y capilaridad tendiente a la ubicuidad
Cebreiro (2007)	Se refiere a que estas éstas giran en torno a cuatro medios básicos: la informática, la microelectrónica, los multimedia y las telecomunicaciones. Y lo que más importante, giran de manera interactiva e interconexionada, lo que permite conseguir nuevas realidades comunicativas, y potenciar las que pueden tener de forma aislada.
Comisión de Comunidades Europeas	Las tecnologías de la información y de las comunicaciones (TIC) son un término que se utiliza actualmente para hacer referencia a una gama amplia de servicios, aplicaciones, y tecnologías, que utilizan diversos tipos de equipos y de programas informáticos, y que a menudo se transmiten a través de las redes de telecomunicaciones.

Tabla 5. Concepciones de las tecnologías

Fuente: (Tecnología Educativa: diseño, producción y evaluación de medios, Cabero, J. 2001)

No teniendo la intención de validar o analizar estas distintas definiciones, de alguna forma hay cierta coincidencia en considerar a las tecnologías como instrumentos técnicos que giran en torno a la información o trasmisión de ésta; es decir, de alguna manera implícitamente son los medios que sirven para que se lleve a cabo el proceso de comunicación.

Las características identificadas más significativas de las TIC en las últimas décadas, son las que señala Cabero (2001), ver Tabla 6.

Características de las TI	
Inmaterialidad	Hace referencia a que la materia prima en torno a la cual desarrollan su actividad es la información, e información en múltiples códigos y formas, es decir: visuales, auditivas, audiovisuales, textuales de datos estacionarios y en movimiento.
Interconexión	Se refiere a diferentes formas de conexiones, vía hardware y que se permitirá el acto de la comunicación en el que se han desarrollado nuevas realidades expresivas y comunicativas.
Interactividad	Hace referencia a que el control de la comunicación se centra más en el receptor, desempeñando un papel importante en la construcción del mensaje, el rol del trasmisor evoluciona
Instantaneidad	Rompe las barreras de espacio y tiempo
Creación de nuevos lenguajes expresivos	Se refiere a que permiten nuevas realidades expresivas, como es el caso de los multimedia e hipermedia, estos a su vez ocasionan nuevos dominios alfabéticos, potenciando la alfabetización en el lenguaje informático y multimedia
Ruptura de la linealidad expresiva	Se refiere a que los mensajes tienden a organizarse no de forma lineal, sino de manera hipertextual, lo que traerá una serie de consecuencias significativas, como son la desestructuración del discurso, la transferencia del peso de la comunicación del autor al texto, el desafío de pasar de la distribución de la información a su gestión, y la construcción del significado de forma diferente en función de la navegación hipertextual realizada por el receptor.
Diversidad	Se refiere a que no existe una única tecnología disponible, sino que por el contrario, se tiene una variedad de ellas.
Innovación	Se refiere a señalar que es tan acelerado el proceso de innovación de la tecnología que rebasa al contexto educativo en ocasiones por su poca capacidad para absorber la tecnología, en muchas ocasiones cuando se incorpora una tecnología a la institución educativa, ésta tecnología ya está siendo remodelada y trasformada.
Elevados parámetros de calidad, imagen y sonido	Se refiere la calidad con que pueden transferir la información, y sin lugar a duda se ha logrado por la digitalización de las señales visuales, auditivas y de datos y por los avances significativos en el hardware usado para las comunicaciones.
Potenciación, audiencia segmentaria y diferenciada	Se refiere a que comprendemos como la especialización de los programas y medios en función de las características y demandas de los receptores, es decir en el caso de los medios televisivos, pueden provocar una segmentación de audiencias, según la conveniencia. También el caso de las redes sociales o comunidades virtuales rompen el concepto de cultura de masas y se superpone la cultura de la fragmentación de las audiencias en función de los intereses y actitudes de los que participen.

Tabla 6. Características de la TI
Fuente: (Tecnología Educativa: diseño, producción y evaluación de medios, Cabero, J. 2001)

En líneas generales (Cabero, 1998), se puede afirmar que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres grandes innovaciones: la

informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo, lo hacen de manera interactiva e interconexionadas, lo que permite conseguir nuevas realidades comunicativas.

2.2 Seguridad de la información

Las tecnologías de la información y comunicación han revolucionado la creación de nuevas herramientas informáticas que han impactado en todas las ramas del conocimiento y a su vez, han generado nuevas oportunidades, vínculos, negocios y hasta relaciones personales, facilitando la realización de actividades negativas como la existencia de conductas antisociales y de nuevos delitos asociados al uso de la información.

Las telecomunicaciones conectadas con el internet han penetrado en todo el mundo de una forma global, hecho que ha traído consigo una serie de beneficios como lo son: envío de correos electrónicos, envío de información, redes sociales, minería de datos en la nube, almacenamiento en la nube, telepresencia, comunicación VoIP, smartphones, virtualización, centros de datos, etc. Sin embargo estos beneficios tan ricos para las organizaciones y para los países emergentes, han traído también un hoyo negro que muchos desconocen: la seguridad en la información.

La seguridad de la información de acuerdo al marco de referencia ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

En todo el mundo existen organizaciones sin fines de lucro que juntas han creado alianzas en el campo de la seguridad de la información; esto con el fin de preservar la disponibilidad, integridad y confidencialidad de la información. Algunas de esas alianzas las podemos visualizar en la Tabla 7.

Alianza	Objetivo de la alianza
Unión internacional de telecomunicaciones (ITU)	Cooperación sobre la Ciberseguridad, para la creación de confianza y seguridad en la utilización de TIC. La ITU debe ayudar a los países miembros sobre técnicas para reducir las vulnerabilidades, especialmente a los países en desarrollo. Su objeto es analizar las amenazas y vulnerabilidades existentes y futuras.
ICSPA y Europol	Para analizar el futuro de la ciberdelincuencia especialmente en los países emergentes, ha creado el Proyecto 2020. Su objetivo es identificar patrones de desarrollo de los futuros ataques.
Facebook anti-virus Marketplace	Además de las seguridades implementadas, Facebook ha realizado una alianza con Microsoft, McAffe, TendMicro, Sophos y Symantec para aumentar la seguridad de los usuarios, quienes pueden gozar de seis meses de una versión full de antivirus
ASI – Alianza por la seguridad en internet	Asociación civil sin fines de lucro en México para la orientación social para el uso seguro de las tecnologías de la información y comunicación

Tabla 7. Alianzas en seguridad de la información
Fuente: (Elaboración propia)

2.2.1 Informes anuales de seguridad de la información

Para fortalecer el marco teórico de la Seguridad de la información es importante conocer los informes anuales que presentan diversas entidades relacionadas con la Seguridad de la Información y de entidades relacionadas con la auditoría. A continuación se resumen algunas de ellas en la Tabla 8.

Entidad	Informe	Dirección WEB
Price Waterhouse Coopers (PWC)	Encuesta global de la seguridad de la información 2012 elaborada por pwc	http://www.pwc.es/es/sala-prensa/notas-prensa/2011/encuesta-seguridad-informacion-2012-pwc.html
Ernest & Young	Encuesta global sobre seguridad de la información EY de 2015	http://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015/$FILE/ey-encuesta-global-seguridad-informacion-2015.pdf
Deloitte	Panorama de Ciber Seguridad en México para 2016-2017	http://www2.deloitte.com/mx/es/pages/risk/articles/ciber-seguridad-ciso-mty.html
Verizon	Verizon 2011 Payment Card Industry Compliance Report	http://www.verizonenterprise.com/resources/reports/rp_2011-payment-card-industry-compliance-report_en_xg.pdf
CISCO	Informe anual de seguridad de cisco 2016	http://globalnewsroom.cisco.com/es/la/press-releases/informe-anual-de-seguridad-de-cisco-revela-una-dis-1239705
Sophos	Informes de amenazas de seguridad 2013	https://www.sophos.com/es-es/security-news-trends/reports/security-threat-report.aspx
Eset	Informe de seguridad 2016 de Latinoamérica	http://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf
Symantec	Internet Security Threat Report 2013	http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v18_2012_221284438.en-us.pdf

Tabla 8. Informes anuales de seguridad
Fuente: (Elaboración propia)

2.2.2 Equipo de respuesta ante emergencias informáticas (CERT)

La gestión de la Seguridad de la Información recomienda la creación de entidades especializadas de Seguridad de la Información como es la creación de equipos de respuesta ante emergencias de Seguridad (CERT, del inglés *Computer Emergency Response Team*), para la centralización de las actividades relativas a la Seguridad de la Información. Existen CERT de contexto nacional y de contexto local, los primeros tienen una visión macro cuyo objetivo es coordinar y regular los CERT locales.

Se considera que debe existir un CERT Nacional, un CERT Gubernamental, un CERT de la Educación, CERT Financieros, CERT de infraestructuras críticas, etc. Entre los servicios que puede ofrecer un CERT tenemos: Soporte para la prevención, detección,

análisis de vulnerabilidades, respuestas ante incidentes, recuperación de desastres, análisis forense, capacitación. La razón de ser de un CERT es la Gestión de Incidentes.

Para cumplir su objetivo debe abarcar marcos técnicos, normativos y legales; el establecer alianzas con otros CERT nacionales e internacionales también son de gran aporte.

También se puede hablar de un Equipo de Respuestas ante Incidencias de Seguridad CSIRT de sus siglas en inglés (Computer Security Incident Response Team) que tiene un ámbito similar.

¿Qué es el CERT México?

El Centro Nacional de Respuesta a Incidentes Cibernéticos es el organismo acreditado para atender amenazas de ciberseguridad en México, creado por la división científica de la policía federal. Se encarga de atender denuncias de ataques a los activos tecnológicos de la infraestructura crítica de México, monitorea la seguridad de la red y los sistemas, y coordina la respuesta a incidentes a víctimas de ataques cibernéticos.

Este CERT, esta creado bajo un manual administrativo de aplicación general en materia de tecnologías de la información y comunicación y de seguridad de la información; mejor conocido como MAAGTICSI.

2.2.3 Tendencias de la seguridad de la información

El uso de las nuevas tecnologías lleva a la aparición de nuevas amenazas de Seguridad de la Información. Las nuevas tendencias de la Seguridad de la Información a las que están expuestos los usuarios finales tienen un nuevo enfoque, en el que están inmersos el ciudadano y el gobierno.

La inversión en nuevas tecnologías de Seguridad Informática en los países emergentes como (Brasil, Rusia, India, China y países de Latinoamérica), están en auge con un crecimiento del 9% al 11% en Infraestructura de Seguridad entre el 2011 y 2013. Según Relasec Inc. habrá un crecimiento importante en EEUU y Latinoamérica, esto debido a la crisis de Europa, en especial en los países emergentes donde hay más fraude por la falencia de leyes y normativas.

Se está en una etapa de transición, donde los niveles de defensa estáticos están siendo reemplazados por niveles de defensa dinámicos, ocasionados por el rápido ritmo de cambios de las TIC. Se han generado nuevas amenazas, nuevas variantes de malware (software malicioso), amenazas persistentes, ataques dirigidos, nuevos vectores de ataque; motivo por el cual es necesario realizar un análisis de estas amenazas. Considerando un contexto general, las principales causas que pueden relacionarse en incidentes de seguridad se resumen en la Tabla 9.

EQUIPO	Hardware vulnerable o mal configurado
SOFTWARE	Sistemas operativos o aplicativos inseguros
PERSONAS	Diseños y configuraciones de seguridad estáticos, falta de procesos y aplicación de controles
NORMATIVA	Falta de normativas y leyes aplicadas a la seguridad de la información

Tabla 9. Causantes de incidentes de seguridad
Fuente: (Elaboración propia)

Las principales y nuevas amenazas de la Seguridad de la Información, de las que actualmente nos vemos afectados podemos considerar:

El hacktivismo (fusión de actividades entre hacker y el activismo), protestan y dan a conocer su ideología haciendo uso no adecuado de herramientas informáticas para conseguir objetivos políticos, sociales, etc. Los Hacktivistas promulgan la libertad de acceso a la información, están en oposición a nuevas leyes que restringen el acceso a la información. Entre los hacktivistas más conocidos en las redes sociales se tiene a “Anonymous”.

Los retos y amenazas de la Ciberseguridad son considerados como principales riesgos de TI, de aquí aparecen otros términos como la Ciberguerra y la Ciberdefensa. La Ciberguerra con su quinto elemento el Ciberespacio (así se tienen: aire, mar, tierra, espacio, ciberespacio).

La Ciberseguridad debe promover la seguridad y la confianza de la nación, para ello considera la protección de al menos ocho sectores estratégicos: energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, telecomunicaciones, bancos y finanzas, suministro de agua, transporte, servicios de emergencia y operaciones gubernamentales.

Dentro del contexto de la Ciberseguridad tenemos el Ciberespionaje, lo más conocido en los últimos días es el caso del Proyecto PRISM (de sus siglas en ingles), que permitía a la Agencia Nacional de Seguridad (SNA de sus siglas en ingles) de los EEUU, realizar un seguimiento de los registros telefónicos y digitales de los ciudadanos sin permiso, desde los servidores de las redes sociales de las empresas (Google, Facebook, Apple, Microsoft, Hotmail, Yahoo, Skype, Youtube, entre otras); este proyecto se vino desarrollando desde el año 2007, se conoce que el gobierno del Reino Unido también mantenía proyectos similares.

El Crimen Organizado y las Nuevas Tecnologías, generalmente relacionado con el narcotráfico y la inseguridad. El crimen organizado en la Región Andina (Bolivia, Perú, Ecuador, Venezuela y Colombia), su principal debilidad es la no existencia de leyes de gobernanza, de monitoreo y control en este campo.

Ataques Persistentes Avanzados (APT), son ataques especializados de red dirigidos a organizaciones, se caracteriza por borrar pistas, utiliza métodos de ataque, ocultamiento y propagación.

La Consumerización y el BYONG, que no es otra cosa que la incursión de nuevas plataformas móviles de comunicación en el ámbito laboral, tipo tablets o teléfonos

inteligentes. La Consumerización ha aumentado el trabajo desde los dispositivos móviles aportando comodidad y productividad, por otro lado ha aumentado el número de amenazas, como la fuga de información; no se disponen de controles adecuados de acceso y de seguridad de los datos.

Digiware, consultora de seguridad, en junio de 2012 resume que las principales tendencias para la Seguridad de la Información a las que nos veremos expuestos en estos años serán principalmente: el Hacktivismo, la Ciberseguridad, las amenazas persistentes avanzadas (APT) y la Consumerización. Para garantizar seguridad de las transacciones en línea, proteger las infraestructuras críticas de información y salvaguardar los sistemas de información y de los datos de las organizaciones, el gobierno y el ciudadano deben fortalecerse con alianzas locales e internacionales.

El uso de internet ha revolucionado nuestro tiempo, es un espacio virtual donde hay una enorme fuente de información, ya que permite acumular el conocimiento humano de múltiples ámbitos en un solo lugar. Ha cambiado la forma de aprender, de estudiar y de hacer investigaciones.

Un signo distintivo ha sido la potenciación de su capacidad como medio de comunicación, ya que se pasó de las páginas web a los sitios interactivos, a la web 2.0, donde existe una interacción en doble vía, entre usuarios con medios como el correo electrónico, los chats, los servicios de mensajería instantánea y las redes sociales.

Esto obliga a transformar también el marco jurídico, ya que a través de estos medios se realizan conductas humanas, que tienen efectos en el mundo real y afectan la esfera jurídica de las personas.

Actividades como el comercio electrónico, el periodismo digital, la publicidad y las opiniones, mensajes o elementos vertidos en redes sociales pueden derivar en menoscabos del patrimonio, la reputación, el honor o la actividad profesional de alguien.

Acciones como el acoso y el contacto en redes sociales con fines de trata de personas, los fraudes, la suplantación de identidad, entre otros son conductas nocivas que están presentes cada vez más.

El incremento de los incidentes va en estricta relación con el incremento del número de usuarios de internet, redes sociales y medios informáticos.

De acuerdo con las cifras de la Unión Internacional de Telecomunicaciones (UIT), en el mundo existen alrededor de 3,000 millones de cibernautas (40% de la población mundial)1, con una tasa de crecimiento anual aproximada de 14%. Un estudio realizado por la firma de software Symantec, señala que la cifra de víctimas es de aproximadamente 12 víctimas por segundo: 1 millón diarias y 378 millones al año. El reporte indica que las pérdidas económicas anuales oscilan entre los 375 y 575 mil millones de dólares (MDD).

Un dato relevante del panorama mundial, es que el Foro Económico Mundial considera las fallas de la infraestructura crítica y los ciberataques como parte de los principales riesgos globales, incluso entre los primeros diez lugares.

El uso y abuso de las tecnologías de la información, la incorporación del Internet al mundo real fue avasallador. De tal manera, que los sistemas jurídicos de las naciones no se encontraban preparadas con los mecanismos legales necesarios para afrontar dicha problemática. México, no fue la excepción.

En Latinoamérica, y conforme al estudio realizado por la Organización de Estados Americanos (OEA) en colaboración con la firma de software Trend Micro 4, se presentó un incremento entre el 8% y el 40% en ataques durante 2012, siendo México el mercado más problemático. Dicho aumento se generó en ciberataques y acciones “hacktivistas”, lavado de dinero y ataques a infraestructuras críticas.

El robo de la banca en línea ha sido ampliamente reportado en América Latina. Esta actividad presentó características distintivas entre los países, dependiendo del banco o país de destino y la naturaleza de las medidas de seguridad que protegen los datos financieros.

De acuerdo al decreto publicado en el Diario Oficial de la Federación el 11 de junio de 2013, el Estado Mexicano garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet.

El escenario en México, de acuerdo con datos de la Asociación Mexicana de Internet (AMIPCI), es el notable incremento en la cifra de cibernautas, pasando de 34.9 millones en 2010 a 53.9 millones en 2014, 43% de la población nacional. Es uno de los países con más actividad en la red según el reporte de la OEA y se espera una cobertura de hasta un 98% con la implementación del proyecto México conectado, a cargo de la Secretaría de Comunicaciones y Transportes.

La actividad de programas de cómputo maliciosos (malware) también fue una de las principales afecciones, registrándose un incremento del 40% en incidentes cibernéticos en 2012. Se estima que en 2013 la pérdida económica anual en México fue alrededor de los 3 mil MDD según los datos del Reporte Norton de 2013. En países como Alemania, la afectación del cibercrimen representa una afectación del 1.6% del PIB; en Estados Unidos del 0.64% y en Brasil del 0.36%, según el estudio publicado por la Unión Internacional en Telecomunicaciones denominado “Comprensión del Ciberdelito, Fenómenos, Dificultades y Respuesta Jurídica”.

El Estudio sobre los hábitos del Internet en México realizado por la AMIPCI (2014), indica que 18.4 millones (36%) de cibernautas son personas menores de edad, un gran número de posibles víctimas de delitos contra menores. El estudio arrojó que el promedio en el tiempo de conexión a Internet de los cibernautas en México es de más

de cinco horas al día y que el uso es principalmente para el correo electrónico, redes sociales (9 de cada 10 lo utilizan) y búsqueda de información, en ese orden.

La AMIPCI identificó que en México se incrementó el comercio electrónico en 2014, llegando a movilizar más de 10 mil MDD, lo que representa un 34% más que en el año anterior.

Otro dato relevante de México es la importancia que tienen las micro, pequeñas y medianas empresas (MIPYMES) en el desarrollo económico y social de la nación, ya que datos de Promexico refieren que existen cerca de 4.2 millones de MIPYMES que generan el 52% del Producto Interno Bruto (PIB) y el 72% de los empleos formales. El 95% de ellas son particularmente Pequeñas y Medianas e impulsan de manera relevante el crecimiento económico digital del país con el fortalecimiento de sus infraestructuras tecnológicas.

Otro ejemplo, según datos del último Reporte Global de Cibercrimen Norton (2013), en 12 meses, al menos 556 millones de usuarios web en todo el mundo, fueron víctimas de acciones como la recepción de virus o malware, robo de identidad, ciberbullying, hackeo de cuentas, fraude financiero difamación a través de fotografías y filtración de videos íntimos. Esto significó un incremento de 118% respecto de los 255 millones de personas en 2011.

Por obvias razones, el estudio señala que el mercado virtual al que se accede mediante teléfonos móviles es el medio donde más crece el cibercrimen. El 48% de usuarios de Smartphone no utiliza medidas de protección básicas como contraseñas de acceso y un 57% desconoce la existencia de software de protección para dispositivos móviles.

De igual manera, existe el uso de conexiones WiFi inseguras para acceder a cuentas personales (bancarias, correo electrónico o redes sociales), un escenario extremadamente fácil para que quienes cometen cibercrímenes ganen acceso a la información de las personas.

2.3 Introducción al delito informático

El uso de las tecnologías de la información en México ha avanzado rápidamente conforme a los desarrollos tecnológicos que ha habido en el mundo, sin embargo el uso particular de internet que es una red mundial, ha causado un gran número de actividades antijurídicas que se realizan a través de este medio. La legislación actual en materia federal y las de los estados de la República sobre delitos informáticos, se ha visto superada por la rápida evolución de los medios electrónicos. Uno de los principales problemas es la incorporación de las nuevas figuras delictivas que han surgido a la largo de los últimos años y de la adecuación de los distintos tipos penales ya existentes, por lo que resulta de vital importancia reformar las leyes federales y locales que logren sancionar adecuadamente los delitos informáticos.

En los últimos años el uso de dispositivos electrónicos, tales como: PC, lap top, tablets, smart phones, etc., se ha incrementado por parte de la población ya que los costos son más accesibles y los proveedores de internet dan mayor cobertura y facilidad a los planes que ellos ofrecen. La mayoría de estos dispositivos electrónicos están conectados a Internet, por lo tanto los usuarios pueden realizar diversas operaciones a través de ellos, como: operaciones bancarias, publicación de información a través de redes sociales (facebook y twitter), envío de correos electrónicos, revisan información del trabajo, etc. Sin embargo, al estar conectados a Internet, las personas están expuestas a un sinfín de riesgos y amenazas que atañen a la seguridad de la información como son: Pérdida de información, robo de identidad, robo de números bancarios, pie a ingeniería social, etc.

Algunas de estas actividades ya se encuentran tipificadas en los distintos ordenamientos penales, ya sea en el ámbito federal o local. Sin embargo, debido a que la tecnología avanza a pasos agigantados, comienzan a aparecer nuevas formas y figuras que no están contempladas y que no pueden ser clasificadas como delitos. La razón es que se estipulan de manera específica ciertos requisitos para que dichas figuras sean tipificadas como tales.

Las contravenciones legales en el ámbito informático, han sido definidas tanto por organizaciones internacionales como por estudiosos de la materia. La Organización para la Cooperación y el Desarrollo Económicos (OCDE), estableció en 1983, que el Computer Crime es “cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos”.

Antonio-Enrique Pérez Luño, ha sostenido que es “aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan el funcionamiento de los sistemas informáticos”.

Sabemos que un delito es el acto u omisión que sancionan las leyes penales. Ahora bien, el delito informático “son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).

El mismo autor establece como característica de dichos antijurídicos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos.

Se puede dar cuenta que entre dichas conductas criminales de cuello blanco, auspiciadas bajo la denominación de Delito Informático, destacan: hacking, cracking, phishing, evil twins, pharming y spamming, robo de identidad; cyberterrorismo; propagación de Malware a través de las redes de datos; el empleo de tecnologías Pop-Up Ads y Adware, la instalación de sniffers, spyware, o programas espía en las computadoras personales para conocer los hábitos y actividades de familiares o empleados; así como la vigilancia internacional de las comunicaciones electrónicas a través de programas gubernamentales como ECHELON o los de control fronterizo como el US-VISIT, son tan sólo algunas de las tantas expresiones de tan variada fenomenología que han hecho que la seguridad jurídica de las personas y de las

transacciones comerciales electrónicas, dependan de las medidas de seguridad de los sistemas informáticos de información y comunicación.

La concepción de los delitos informáticos en México tendrá escasos diez años; sin embargo, en los Estados Unidos de Norteamérica, la primera propuesta de legislar sobre delitos informáticos, se presentó en 1977 por el senador Ribicoff en el Congreso Federal.

Años después, en 1983 en París, la OECD designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los códigos penales. El dictamen de esta organización, recomendó a los países miembros la modificación de su legislación penal, de forma que se integraran los nuevos delitos informáticos.

En 1989, el Consejo de Europa convocó a otro comité de expertos, que en la Recomendación emitida el 13 de septiembre de ese año, presentaron una lista mínima de los delitos que debían necesariamente agregarse a las legislaciones de cada país miembro, junto con una lista opcional.

También se llegó a discutir sobre estos temas en el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal en 1990, en el Octavo Congreso Criminal de las Naciones Unidas celebrado en el mismo año, y en la Conferencia de Wurzburgo, en Alemania, en 1992. En 1996, se estableció por el Comité Europeo para los Problemas de la Delincuencia, un nuevo comité de expertos para que abordaran el tema de los delitos informáticos.

Con el fin de combatir los delitos informáticos, sobre todo los cometidos a través de las redes de telecomunicaciones, en Internet, como pueden ser las transacciones de fondos ilegales, la oferta de servicios ilegales, la violación de los derechos de autor, así como también los delitos que violan la dignidad humana y la protección de los menores, se encargó la tarea de elaborar un borrador del instrumento legal obligatorio al recién

formado “Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras”.

El 23 de noviembre de 2001, el Consejo de Ministros de Europa, compuesto por los Ministros del Interior de los estados que conforman la Unión Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón, firmó en Budapest, la convención sobre delitos informáticos, cuyos objetivos fundamentales son los siguientes:

1. Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático.
2. Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes, las facultades necesarias para la investigación y persecución de tales conductas delictivas.
3. Establecer un régimen dinámico y efectivo de cooperación internacional.

En el sistema jurídico mexicano se incluyó a los delitos informáticos justamente con las reformas que se publicaron en el Diario Oficial de la Federación el diecisiete de mayo de mil novecientos noventa y nueve.

Los novedosos ilícitos se ubicaron dentro del Título Noveno del código punitivo federal, al que se denominó “Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática”.

Resulta de interés al desarrollo de estas líneas las causas medulares que dieron origen a la exposición de motivos de la reforma, al considerarse que la iniciativa propone adicionar un capítulo al código penal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la pérdida de información que contenga, por lo que se pretende tutelar la privacidad y la integridad de la información.

2.3.1 Legislación informática en México

La regulación del Internet es un enorme reto en razón de su carácter internacional y de la enorme cantidad de sitios que existen de tan variada índole e interés, a manera de ejemplo, las personas pueden jugar en casinos virtuales sin ninguna regulación; a la fecha actual se puede decir que el único contenido de Internet prohibido y sancionado en el país, es el de la pornografía infantil.

Lo anterior, da una idea de lo grave que resulta carecer de reglas de comportamiento en el Internet; por ello, se considera que los valores fundamentales de la sociedad, con independencia de la raza, credo, cultura y educación, son necesarios para la interacción en ese mundo virtual, por lo que al darse de alta una persona en el Internet debe ser consciente y actuar de buena fe, expresando los datos que corresponden a su identidad, de igual manera los prestadores de servicio deben exigir mayores requisitos para la autorización de direcciones electrónicas.

Bajo el anterior marco de referencia, es posible adentrarnos al conocimiento de los Delitos Informáticos previstos y sancionados en el ordenamiento jurídico mexicano.

Algunos artículos importantes tipificados por la ley son los siguientes:

Código penal para el D.F. Art. 231:

Se impondrán las penas previstas en el artículo anterior, a quien: V. Para obtener algún beneficio para sí o para un tercero, por cualquier medio acecé, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución.

CONDUCTA	PENA
Destruir información sin autorización	6 meses a 2 años de prisión, 100 a 300 días multa
Si se trata de sistemas o equipos del Estado	1 a 4 años y 200 a 600 días de multa
Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero	6 meses a 4 años de prisión, 100 a 600 días de multa
Conocer o copiar información sin autorización	3 meses a 1 años de prisión, 50 a 150 días de multa
Si se trata de sistemas o equipos del Estado	6 meses a 2 años y 100 a 300 días de multa
Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero	3 meses a 2 años de prisión, 50 a 300 días de multa
"Destruir información cuando se tenga autorización para el acceso"	
Si se trata de sistemas o equipos del Estado	2 a 8 años y 300 a 900 días de multa
Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero	6 meses a 4 años de prisión, 100 a 600 días de multa
"Conocer o copiar información cuando se tenga autorización para el acceso"	
Si se trata de sistemas o equipos del Estado	1 a 4 años de prisión y 150 a 450 días de multa
Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero	3 meses a 2 años de prisión, 50 a 300 días de multa

Tabla 10. Conducta y penas para el Art. 211 bis 1 al 211 bis 7
Fuente: (Código penal federal. Art. 211 bis 1 a 211 bis 7)

Ley Federal del derecho de autor. Art. 11:

Establece el reconocimiento del Estado al creador de obras literarias o artísticas, entre las que están los programas de cómputo. La reproducción queda protegida a favor del autor y se prohíbe la fabricación o uso de sistemas o productos destinados a eliminar la protección de los programas.

“El Código Penal Federal tipifica y sanciona esta conducta con 2 a 10 años de prisión y de 2000 a 20000 días de multa”.

Ley Federal del derecho de autor. Art. 107 al 110:

Protege como compilaciones a las bases de datos legibles por medio de máquinas que por razones de disposición de su contenido constituyan obras intelectuales, otorgándole a su organizador el uso exclusivo por cinco años; asimismo, exceptuando las investigaciones de autoridades, la información privada de las personas contenida en bases de datos no podrá ser divulgada, transmitida ni reproducida salvo con el consentimiento de la persona de que se trate.

Ley de Protección de Datos Personales del Estado de Colima

Los principios bajo los cuales deberán manejarse los datos personales, entre los que destacan:

1. Sólo podrán obtenerse y ser sujetos de tratamiento cuando sean adecuados, pertinentes y no excesivos.
2. Deben ser correctos y actualizados.
3. Deberán obtenerse por medios lícitos y será necesario el consentimiento del interesado.

Código Penal Federal. Art. 167 Fr. VI:

Sanciona con uno a cinco años de prisión y 100 a 10000 días de multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alambricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos. Aquí tipificaría el interceptar un correo antes de que llegue a su destinatario, pero no el abrir el buzón o los correos una vez recibidos.

2.3.2 Falta de leyes limita el combate del cibercrimen en México

Ahora bien, la falta de un marco legal y fiscalías especiales limitan la persecución del cibercrimen; en México el ciberdelito de mayor incidencia es la pornografía infantil.

La carencia de correspondencia con la Procuraduría General de la República, además de un marco legal poco claro, limita el nivel de acción de la Policía Cibernética para perseguir y dar seguimiento al cibercrimen en México.

El director general para la Prevención de Delitos Electrónicos de la Policía Federal, el Comisario Jefe Maestro Marcos Arturo Rosales, dijo que mientras no se logre llenar los huecos legales, poco se podrá hacer, para perseguir este tipo de delitos. Afirmó el Comisario en conferencia, “no hay una fiscalía especializada en la Procuraduría para darle seguimiento penal a este tipo de delitos, eso lo complica mucho. Pero estoy seguro que ya no falta mucho tiempo para que exista una contraparte de ese lado”.

Rosales hizo hincapié en la necesidad de ministerios públicos especiales para dar seguimiento penal a las denuncias por estos ilícitos, los cuales en su mayoría están ligados a redes de pornografía infantil; sin embargo, dijo que existen otras vías para atacar otros delitos, como la pérdida de información en empresas. Aquí si hay un contrato, es posible investigar y detener a responsables.

El hecho de que actualmente en México no exista un marco jurídico en este tema, no significa que no suceda; por el contrario, datos detectados del departamento jurídico de Microsoft, revelan que tanto empresas, como personas y gobierno mexicanos, están más vulnerables a los ataques, por no contar con la protección necesaria o por malos hábitos como el uso de software pirata.

En México, una de cada 3 personas cuenta con una computadora infectada de *malware*; la razón principal es porque usan software pirata. Un mapa realizado por Microsoft, mostró que la colonia Roma es una de las más atacadas por hackers.

“Hace tan sólo 15 días, se registraron 181,000 direcciones IP’s infectadas por *malware*”, dijo la directora para Asuntos de Propiedad Intelectual y Seguridad Digital de Microsoft México, Jimena Mora.

Al cierre de 2014, existieron 45 millones de víctimas de ciberataques en el mundo, lo que provocó 4,000 millones de dólares en pérdidas económicas.

Rosales dijo que al momento se encuentran en cabildeo en el Congreso para empujar una iniciativa de ley que dé un mejor marco legal para combatir las amenazas cibernéticas. Por otro lado, comentó que es necesario que México se adhiera al Convenio de Budapest para homologarse con otras prácticas internacionales para el tratamiento de estos delitos; dicha adhesión ya está en curso pero aún no hay logros en concreto.

Otros países como Estados Unidos, Reino Unido e Israel, forman parte de estos estatutos mundiales para el mejor combate al cibercrimen, el cual dijo el presidente de la Comisión de Inteligencia Corporativa y Gestión de Riesgo de ICC México, Brian Weihs, es una tendencia que no tendrá freno en años futuros y es preciso prepararse para hacerles frente.

2.3.3 El convenio de Budapest

Es imprescindible la celebración de tratados internacionales que fortalezcan la colaboración con Policías Cibernéticas de otros países, y el Convenio de Budapest resulta conveniente para México en virtud de lo siguiente:

- Es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. También contiene una serie de competencias y

procedimientos, tales como la búsqueda de las redes informáticas y la interceptación legal.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Los principales objetivos de este tratado son los siguientes:

1) La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.

2) La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.

3) Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

Los siguientes delitos están definidos por el Convenio: acceso ilícito, interceptación ilegal, la interferencia de datos, la interferencia del sistema, mal uso de los dispositivos, la falsificación informática, el fraude relacionado con la informática, los delitos relacionados con la pornografía infantil y los delitos relacionados con los derechos de autor y derechos conexos (Comisión de Comunidades Europeas, 2001)

Asimismo, se exponen cuestiones de derecho procesal como la preservación expeditiva de los datos almacenados, la preservación expeditiva y divulgación parcial de los datos de tráfico, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido. Además, el Convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren

asistencia mutua (con consentimiento o disponibles al público) y prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las Partes Colaboradoras.

El Convenio es el resultado de cuatro años de trabajo de expertos europeos e internacionales. Se complementa con un Protocolo Adicional que realiza cualquier publicación de la propaganda racista y xenófoba a través de redes informáticas como una ofensa criminal. En la actualidad, el terrorismo cibernético también se estudia en el marco del Convenio. México sería el tercer país en Latinoamérica en adherirse al Convenio después de República Dominicana y Panamá.

2.4 Amenazas en la seguridad de la información

Las amenazas son eventos que desencadenan un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información. El Sistema de Gestión de Seguridad de la Información basado en la ISO 27001 ayuda a controlar las amenazas que pueden desencadenar los incidentes.

2.4.1 Características de las amenazas

La definición anterior recoge la esencia de las amenazas, es decir, es un potencial evento. La consecuencia de las amenazas es un incidente que modifica el estado de seguridad de los activos amenazados, por lo que se hace pasar de un estado anterior al evento a otro posterior, de cualquier forma que se trate la amenaza o las agresiones materializadas.

La distancia que hay entre la amenaza potencial y su materialización como agresión real, se mide por la frecuencia o la potencialidad de esta materialización, por lo que se cuenta una agresión materializada, las amenazas se verán si son agresiones potenciales o materializadas.

2.4.2 Tipos de amenazas

Todas las causas de las amenazas permiten ser clasificadas por su naturaleza. Podemos emplear cuatro causas amenazadoras: no humanas, humanas involuntarias, humanas intencionales que necesitan presencia física y humana intencional que proceden de un origen remoto. (BS, 2013)

No humanas

- Accidente físico de origen industrial, incendios, explosiones, inundaciones, contaminación.
- Averías que pueden ser de origen físico o lógico, se debe al el efecto de origen.
- Accidente físico de origen natural, riada, fenómeno sísmico o volcánico.
- Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros.
- Accidentes mecánicos o electromagnéticos.

Humanas

- Errores de utilización ocurridos durante la recogida y transmisión de datos.
- Errores de diseño existentes desde los procesos de desarrollo del software.
- Errores de ruta, secuencia o entrega de la información durante el tránsito.
- Errores de monitorización, trazabilidad o registros del tráfico de información.

Humanas intencionales que necesitan presencia física

- Acceso físico con inutilización.
- Acceso lógico con intercepción pasiva simple de la información.
- Acceso lógico con alteración o sustentación de la información en tránsito, o reducir la confidencialidad para aprovechar los bienes o servicios.

- Acceso lógico con corrupción o destrucción de información de configuración, o con reducción de la integridad y la disponibilidad del sistema sin provecho directo.

Humana intencional que proceden de un origen remoto

- Acceso lógico con intercepción pasiva.
- Acceso lógico con corrupción de información en tránsito o de configuración.
- Acceso lógico con modificación de información en tránsito.
- Suplantación de origen o de identidad.
- Repudio del origen o de la recepción de información en tránsito.

2.5 Vulnerabilidades

Las vulnerabilidades son una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, y disponibilidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen.

Las vulnerabilidades pueden encontrase asociadas al aspecto físico, organizacional, procedimental, personal, de gestión, de administración, equipos, software o información.

Si existe una vulnerabilidad no implica que se cause un daño, pero la amenaza se puede explotar generando un daño a los activos de información del sistema TI. (BS, 2013)

2.5.1 Características de la vulnerabilidad

La vulnerabilidad es una propiedad de la relación entre un activo y una amenaza, aunque se suele vincular más al activo como una no calidad de éste. La vulnerabilidad es un concepto que tiene dos aspectos básicos:

- Forma parte del estado de seguridad del activo en su función-propiedad de mediación entre el activo y la amenaza como acción.
- En su aspecto dinámico, es el mecanismo obligado de conversión de la amenaza en una agresión que se ha materializado sobre el activo de información.

2.5.2 Tipos de vulnerabilidad

Se pueden considerar dos acepciones principales:

- La vulnerabilidad intrínseca del activo, respecto del tipo de amenaza sólo depende de ambas cantidades.
- La vulnerabilidad efectiva del activo tiene en cuenta las salvaguardas aplicadas en cada momento a dicho activo, como un factor en el que se estima la eficacia global de dichas salvaguardas.

2.5.3 Atributos de las vulnerabilidades

La vulnerabilidad intrínseca puede descomponerse en análisis detallados, que se encuentran en varios bloques de atributos:

- Potencialidad autónoma respecto al activo de seguridad que se encuentre amenazado.

- Potencialidad derivada de la relación entre activo y amenaza.
- Factores subjetivos generadores de más o menos fuerza.
- Oportunidad de acceso al dominio si se tiene la suficiente capacidad y los recursos necesarios, que son cuatro: Accesibilidad física presencial, accesibilidad física cualificada, accesibilidad lógica competencial y accesibilidad lógica instrumental.

2.6 Riesgos

EL riesgo es la estimación del grado de exposición de que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la empresa. (BS, 2013)

2.6.1 Tipos de riesgos

Riesgo aceptable: Aquel nivel de riesgo donde la Alta Dirección decide que las afectaciones derivadas de la materialización de la amenaza no implican un daño importante a los activos de la empresa y por tanto decide asumir el riesgo.

Riesgo residual: Riesgo remanente en el sistema tras la implantación de los controles determinados en el Plan de Tratamiento del Riesgo de la información.

2.6.2 Nivel de riesgo aceptable

La dirección de cada organización deberá asignar un nivel de riesgo aceptable, que servirá como línea base para establecer las actividades para mitigar los riesgos de negocio identificados para los objetivos de negocio.

El criterio para generar el valor de riesgo aceptable es el siguiente: “cualquier valor de nivel riesgo que se encuentre en los rangos de mínimo y bajo. (BS, 2013)

2.6.3 Mejores prácticas en la gestión del riesgo

La gestión del riesgo en las organizaciones consiste en dos elementos principales:

- Análisis de Riesgo: Se ocupa de la recopilación de información sobre la exposición al riesgo, y con el cual el CNOC puede tomar decisiones adecuadas y controlar los riesgos.

- Gestión de Riesgo: Es el proceso de seguimiento de los riesgos que incluye la información adecuada sobre los riesgos y el proceso adoptado para el apoyo del análisis de riesgos, la identificación y su evaluación. Una vez identificados los riesgos y el grado de exposición de estos, se deberá establecer la estrategia para la gestión del riesgo y las responsabilidades asociadas a la misma.

Dependiendo del tipo de riesgo y la significancia para el negocio, se deberá seleccionar una de las siguientes acciones:

- Mitigar: Implementando controles.
- Transferir: Compartir o transferir el riesgo.
- Aceptar: Mediante un método formal se hace del conocimiento de la existencia del riesgo y su monitoreo

Las acciones a realizar como estrategias van ligadas hacia los activos que están por arriba de un nivel de riesgo aceptable. (BS, 2013)

CAPÍTULO 3. Metodología para la seguridad de la información

3.1 Metodología en seguridad de la información para instituciones gubernamentales (MAAGTICSI).

MAAGTICSI contiene tres grupos y nueve procesos necesarios para propiciar la operación ágil y oportuna de las actividades de TIC de las instituciones gubernamentales del Estado.

El objetivo principal de MAAGTICSI es definir los procesos con los que, en las materias de TIC y de seguridad de la información, las instituciones deberán regular su operación, independientemente de su estructura organizacional y las metodologías de operación con las que cuenten.

El 8 de Mayo del 2014, se publicó en el Diario Oficial de la Federación (DOF) el acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional en materia de Tecnologías de la Información y Comunicaciones, y la de seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias, donde se establecen los mecanismos para el almacenamiento y gestión de información sensible y de seguridad nacional que manejan las instituciones de Gobierno.

MAAGTICSI es el principal Manual en materia de Tecnologías de la Información y Comunicación (TIC) de la Administración Pública Federal (APF) en México, ya que establece nuevas obligaciones derivadas del Plan Nacional de Desarrollo 2013-2018 (PND), decreto de disciplina presupuestaria y sus respectivos lineamientos en materia de TIC.

Para el CERT de México que está creado bajo el MAACTIGSI, los principales procesos que se llevan a cabo son los siguientes:

- Implantar y operar los controles de seguridad de la información.
- Definir y aplicar la planeación para la mitigación de riesgos por incidentes.
- Implantar las mejoras recibidas del proceso ASI (Administración de la seguridad de la información), para el fortalecimiento del SGSI, tanto de sus guías técnicas como de los controles de seguridad de la Información en operación.
- Elaborar la guía técnica de atención a incidentes, de acuerdo a la criticidad de los activos de TI afectados.

3.2 Metodología basada en ISO/IEC 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2

La normas más conocidas en la familia de la Norma ISO/IEC 27000, que tiene su origen en la norma ISO 17799 y para efectos de nuestro tema la última norma es ISO/IEC 27001-2013 (ver Tabla 11).

Familia de la norma ISO/IEC 27000	
NORMA	DESCRIPCIÓN
ISO/IEC 27000	Términos y Definiciones de la familia de norma 27000. Proporciona una visión general de la norma 27000.
ISO/IEC 27001	Requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). Es auditable y certificable. Permite la ejecución del Ciclo de Deming PDCA (Planear, Hacer, Verificar y Actuar) para la mejora continua. Adopta un enfoque por procesos.
ISO/IEC 27002	Guía de Buenas Prácticas de la Seguridad de la Información. Contiene 39 objetivos de control, 133 controles de Seguridad en 11 dominios, abarca el contexto de la Seguridad de TI y de la Seguridad de la Información, considera riesgos Organizacionales, Operacionales, Físicos, etc. No es certificable.
ISO/IEC 27003	Guía que cubre aspectos críticos necesarios para el diseño e implementación del SGSI.
ISO/IEC 27004	Métricas y Mediciones para la Gestión de la Seguridad para determinar la eficacia de un SGSI.
ISO/IEC 27005	Gestión del Riesgo de la Seguridad de la Información. Basada en un enfoque de Gestión del Riesgo.
ISO/IEC 27006	Especifica los requisitos para la acreditación de entidades de auditoría y certificación de SGSI
ISO/IEC 27007	Guía de auditoría de un SGSI
ISO/IEC 27014	Guía de Gobierno Corporativo de Seguridad de la Información
ISO/IEC 27015	Guía de SGSI orientada a organizaciones del sector financiero y de seguros
ISO/IEC 27017	Guía de seguridad para el Cloud Computing
ISO/IEC 27018	Código de Buenas Prácticas en controles de protección de datos para Servicios Cloud

Tabla 11. Normas de seguridad ISO 27000
Fuente: (http://www.iso.org/iso/home.html)

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

Con base en ISO/IEC 27001, existen tres pilares para la correcta administración de la seguridad de la información, estos son:

1. Confidencialidad: Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad

puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización

2. Integridad: Busca asegurar:

- Que no se realicen modificaciones por personas no autorizadas a los datos o procesos
- Que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos.
- Que los datos sean consistentes tanto interna como externamente

3. Disponibilidad: Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para

asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Este sistema de gestión de seguridad de la información debe de ser conocido por toda la organización con el objetivo de que la información sea correcta y completa, que además esté siempre a disposición del negocio y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

3.3 Estructura de ISO/IEC 27001:2013

La estructura de ISO/IEC 27001:2013 ha sido desarrollado con base en el anexo SL de ISO/IEC del “Suplemento Consolidado de las Directivas ISO/IEC” (anteriormente publicado como “Guía ISO:83”), en el cual se proporciona un formato y un conjunto de lineamientos a seguir para el desarrollo documental de un sistema de gestión sin importar su enfoque empresarial, alineando bajo una misma estructura todos los documentos relacionados con los sistemas de gestión y evitando así problemas de integración con otros marcos de referencia (ver figura 3).

Figura 3. Estructura de ISO/IEC 27001
Fuente: (Information security management systems. Requirements, ISO/IEC 27001:2013)

Descripción de las principales secciones

1. Alcance

En esta sección se establece la obligatoriedad de cumplir con los requisitos especificados en los capítulos 4 a 10 del documento, para poder obtener la conformidad de cumplimiento y certificarse.

2. Referencias normativas

El estándar ISO-27002 ya no es una referencia normativa para ISO-27001:2013, aunque continúa considerándose necesario en el desarrollo de la declaración de aplicabilidad (SOA, por sus siglas en inglés).

El estándar ISO 27000:2013 se convierte en una referencia normativa obligatoria y única, ya que contiene todos los nuevos términos y definiciones.

3. Términos y definiciones

Los términos y definiciones que se manejaban en 27001:2005 los trasladaron y agruparon en la sección 3 de ISO 27000:2013 *"Fundamentos y vocabulario"* (lo cual se llevará a cabo en todos los documentos que forman parte de esta familia), con el objetivo de contar con una sola guía de términos y definiciones que sea consistente.

4. Contexto de la organización

Esta cláusula hace hincapié en identificar los problemas externos e internos que rodean a la organización.

- Instituye los requerimientos para definir el contexto del SGSI sin importar el tipo de organización y su alcance.
- Introduce una nueva figura (*las partes interesadas)* como un elemento primordial para la definición del alcance del SGSI.

- Establece la prioridad de identificar y definir formalmente las necesidades de l*as partes interesadas* con relación a la seguridad de la información y sus expectativas con relación al SGSI, pues esto determinará las políticas de seguridad de la información y los objetivos a seguir para el proceso de gestión de riesgos.

5. Liderazgo

Ajusta la relación y responsabilidades de la Alta Dirección respecto al SGSI, destacando de manera puntual cómo debe demostrar su compromiso, por ejemplo:

- Garantizando que los objetivos del SGSI y *"La política de seguridad de la información",* anteriormente definida como *"Política del SGSI",* estén alineados con los objetivos del negocio.
- Garantizando la disponibilidad de los recursos para la implementación del SGSI (económicos, tecnológicos, etcétera).
- Garantizando que los roles y responsabilidades claves para la seguridad de la información se asignen y se comuniquen adecuadamente.

6. Planeación

Esta es una nueva sección enfocada en la definición de los objetivos de seguridad como un todo, los cuales deben ser claros y se debe contar con planes específicos para alcanzarlos.

Se presentan grandes cambios en el proceso de evaluación de riesgos:

- El proceso para la evaluación de riesgos ya no está enfocado en los activos, las vulnerabilidades y las amenazas.
- Esta metodología se enfoca en el objetivo de identificar los riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad de la información.

- El nivel de riesgo se determina con base en la probabilidad de ocurrencia del riesgo y las consecuencias generadas (impacto), si el riesgo se materializa.
- Se ha eliminado el término “Propietario del activo” y se adopta el término “Propietario del riesgo”.
- Los requerimientos del SOA no sufrieron transformaciones significativas.

7. Soporte

Marca los requerimientos de soporte para el establecimiento, implementación y mejora del SGSI, que incluye:

- Recursos
- Personal competente
- Conciencia y comunicación de las partes interesadas

8. Operación

Establece los requerimientos para medir el funcionamiento del SGSI, las expectativas de la Alta Dirección y su realimentación sobre estas, así como el cumplimiento con el del estándar.

Además, plantea que la organización debe planear y controlar las operaciones y requerimientos de seguridad, erigiendo como el pilar de este proceso la ejecución de evaluaciones de riesgos de seguridad de la información de manera periódica por medio de un programa previamente elegido.

Los activos, vulnerabilidades y amenazas ya no son la base de la evaluación de riesgos. Solo se requiere para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad. (BS, 2013)

9. Evaluación del desempeño

La base para identificar y medir la efectividad y desempeño del SGSI continúan siendo las auditorías internas y las revisiones del SGSI.

Se debe considerar para estas revisiones el estado de los planes de acción para atender no conformidades anteriores y se establece la necesidad de definir quién y cuándo se deben realizar estas evaluaciones así como quién debe analizar la información recolectada.

10. Mejora

El principal elemento del proceso de mejora son las no-conformidades identificadas, las cuales tienen que contabilizarse y compararse con las acciones correctivas para asegurar que no se repitan y que las acciones correctivas sean efectivas.

Aquí se observa uno de los cambios más importantes porque las medidas preventivas se fusionarán con la evaluación y tratamiento del riesgo, algo más natural e intuitivo que permite enfrentar los riesgos y las oportunidades con base en cuándo estos se identifican y cómo se tratan. Además, se distingue entre las correcciones que se ejecutan como una respuesta directa a una "no conformidad", en oposición a las acciones correctoras que se realizan para eliminar la causa de la no conformidad. (BS, 2013)

Anexos

El "Anexo *A – Referencia de objetivos y controles"* continúa formando parte de este estándar (ver figura 4).

- El número de dominios del anexo aumenta de 11 a 14, de esta manera, donde algunos controles se incluían de forma "artificial" en ciertas áreas donde no encajaban perfectamente, ahora se organizan mejor.

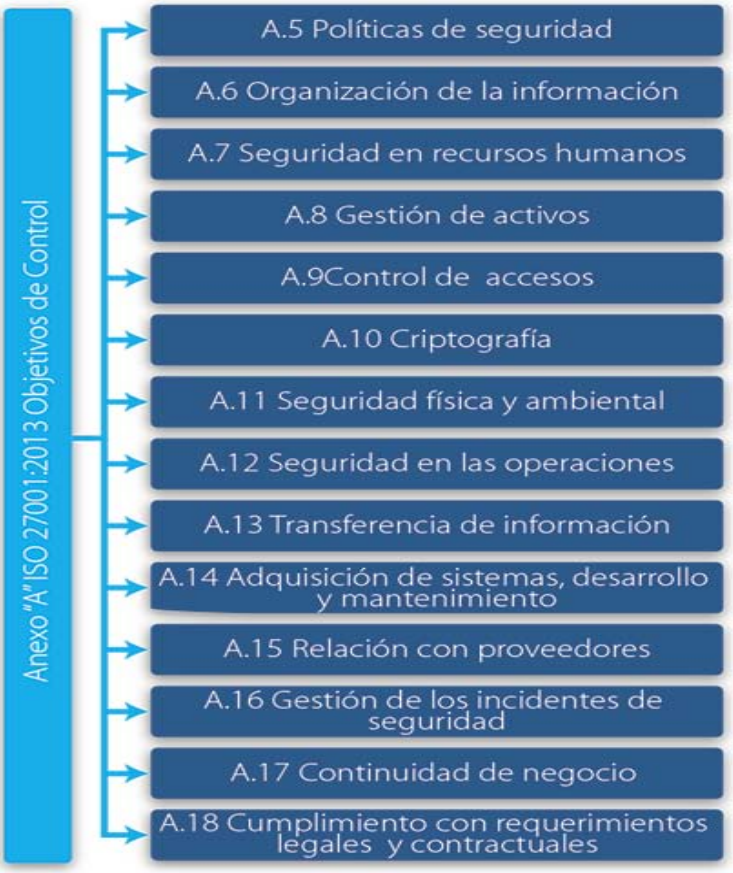

Figura 4. Objetivos de control
Fuente: (Information security management systems. Requirements, ISO/IEC 27001:2013)

3.4 ISO/IEC 27001:2013 bajo la metodología del círculo de Deming

El establecimiento de un sistema de gestión de la seguridad de la información con base en ISO 27001-2013, utiliza el ciclo de Deming (Edwards Deming 1900 – 1993), o más conocido como PDCA (plan, do, check and act), es una serie de pasos sistemáticos para adquirir conocimientos valiosos y conocimientos para la mejora continua de un producto o proceso. El concepto y la aplicación fue introducido por primera vez al Dr. Deming por su mentor, Walter Shewhart de los famosos Laboratorios Bell, en Nueva York.

El ciclo comienza con la etapa de Plan. Esto implica identificar un objetivo o propósito, la formulación de una teoría, la definición de métricas de éxito y poner un plan en acción. Estas actividades son seguidas por el paso Do, en el que los componentes del plan son las tragaperras en línea realizadas como la fabricación de un producto. Luego viene la etapa de Check, donde los resultados son monitoreados para probar la validez del plan para detectar signos de progreso y éxito, o problemas y áreas de mejora. El paso Act cierra el ciclo, integrando el aprendizaje generado por todo el proceso, que puede ser utilizado para ajustar el objetivo, cambiar los métodos o incluso formular una teoría del todo. Estos cuatro pasos se repiten una y otra vez como parte de un ciclo interminable de mejora continua (ver figura 5).

Este modelo de gestión del cambio beneficia a las empresas, proporcionando un enfoque sistemático para lograr la mejora continua.

Figura 5. Plan, Do, Check and Act
Fuente: (https://www.deming.org/theman/theories/pdsacycle)

Los pasos del ciclo de Deming implementados en el SGSI ISO 27001-2013, tienen el siguiente objetivo:

Plan (planificación)

Define el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Es importante que defina los límites del SGSI ya que no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado). Es importante disponer de un mapa de procesos de negocio, definir claramente los interfaces con el exterior del alcance, determinar las terceras partes (proveedores, clientes...) que tienen influencia sobre la seguridad de la información del alcance, crear mapas de alto nivel de redes y sistemas, definir las ubicaciones físicas, disponer de organigramas organizativos, definir claramente los requisitos legales y contractuales relacionados con seguridad de la información, etc.

La política del SGSI es normalmente un documento muy general, una especie de "declaración de intenciones" de la Dirección pero que: incluya el marco general y los objetivos de seguridad de la información de la organización; tenga en cuenta los requisitos de negocio además de considerar los requerimientos legales o contractuales relativos a la seguridad de la información; esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI; establezca los criterios con los que se va a evaluar el riesgo; esté aprobada por la dirección.

Definir el enfoque de evaluación de riesgos mediante una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio. El riesgo nunca es totalmente eliminable “ni sería rentable hacerlo”, por lo que es necesario definir una estrategia de aceptación de riesgo estableciendo criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de la metodología es que los resultados obtenidos sean comparables y repetibles para evitar grados de subjetividad

que falseen la valoración de los riesgos. Existen numerosas metodologías estandarizadas para la evaluación de riesgos y la organización puede optar por una de ellas, aplicar una combinación de varias o crear la suya propia. ISO 27001:2005 no impone ninguna para que cada organización pueda aplicar la que estime más oportuno y funcional según el esfuerzo de análisis y recursos que pueda aplicar. Como documento de apoyo ISO 27005 sí profundiza en directrices sobre la materia.

Identificar los riesgos:

- Identificar todos aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
- Identificar las amenazas relevantes asociadas a los activos identificados;
- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

Analizar y evaluar los riesgos:

- Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
- Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
- Estimar los niveles de riesgo;
- Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

- Aplicar controles adecuados (mitigación)
- Aceptar el riesgo (de forma consciente), siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos
- Evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan
- Transferir el riesgo total o parcialmente a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.

Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001:2013 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI. Hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación final en cada revisión y/o acciones de tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

Definir una declaración de aplicabilidad también llamada SOA (Statement of Applicability) que incluya:

- Los objetivos de control y controles seleccionados y los motivos para su elección;
- Los objetivos de control y controles que actualmente ya están implantados;
- Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

DO (implementar y utilizar el SGSI)

Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

Gestionar las operaciones del SGSI.

Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

CHECK (monitorear y revisar)

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
- Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
- Identificar brechas e incidentes de seguridad;
- Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.

Realizar periódicamente auditorías internas del SGSI en intervalos planificados para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001:2005, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.

Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido siga siendo el adecuado y las posibles mejoras en el proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

ACT (mantener y mejorar)

La organización deberá regularmente:

Implantar en el SGSI las mejoras identificadas.

Realizar las acciones preventivas y correctivas adecuadas para prevenir potenciales no conformidades antes de que se produzcan y solucionar no conformidades detectadas y materializadas. En relación a la cláusula 8 de ISO 27001:2005 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.

Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

Asegurarse que las mejoras introducidas alcanzan los objetivos previstos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases.

3.5 Beneficios de contar con una certificación y un SGSI

Las organizaciones que obtienen una certificación ISO 27001 tienen beneficios que van más allá del cumplimiento de la norma, además trae necesariamente cierto rigor y formalidad al proceso de aplicación, lo que implica mejoras en la seguridad de la información y todos los beneficios que aporta a través de la reducción del riesgo.

El certificado tiene el potencial de comercialización y demuestra que la organización toma en serio la gestión de seguridad de la información; sin embargo, el valor del certificado depende del alcance del SGSI. Por otra parte el tener un certificado no significa que se garantice la seguridad en todos los aspectos de TI.

Otros beneficios son los siguientes:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.

- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.
- Evaluación integral de los riesgos
- Reduce la probabilidad y el impacto de los incidentes de seguridad

3.6 Certificaciones ISO/IEC 27001 en México y el mundo

Las certificaciones son un punto estratégico para la organización ya que detona el ingreso de más clientes, prestigio a la organización, más confianza por parte del cliente y credibilidad a la organización, sin embargo en México las organizaciones que cuentan con un certificado en que avale el funcionamiento adecuado de un SGSI son muy pocas en el sector de TI.

De acuerdo a la última encuesta de certificaciones por parte de la ISO (ISO survey 2014 certifications), solamente hay 96 organizaciones certificadas en esta norma; esto quiere decir que solo el 25.8% de las empresas del sector de TI en México están certificadas.

De acuerdo a estas cifras podemos apreciar que la seguridad de la información en México aun no tiene la importancia que debe.

En otros países la seguridad de la información es vital para sus organizaciones, por lo que mostramos de acuerdo a la encuesta de ISO la siguiente tabla con el top 10 de países certificados (ver tabla 12).

Top 10 countries for ISO/IEC 27001 certificates - 2014		
1	Japan	7181
2	United Kingdom	2261
3	India	2170
4	China	2002
5	Italy	970
6	Romania	893
7	Taipei, Chinese	781
8	Spain	701
9	United States of America	664
10	Germany	640

Tabla 12. Top 10 de países certificados en ISO/IEC 27001
Fuente: (http://www.iso.org/iso/iso-survey)

CAPÍTULO 4. Estrategia metodológica

4.1 Tipo de estudio

Desde el punto de vista metodológico, esta investigación es exploratoria y descriptiva, ya que los alcances exploratorios investigan problemas poco estudiados, indagan desde una perspectiva innovadora, ayudan a identificar conceptos promisorios y preparan el terreno para nuevos estudios. Por otra parte los alcances descriptivos son aquellos que consideran al fenómeno estudiado y sus componentes, miden conceptos y defines variables (Hernández, Fernández y Baptista, 2010).

La investigación es del tipo exploratoria**,** pues el tema de la seguridad de la información, sus amenazas y riesgos para las empresas, ha sido poco estudiado en México. Analizar y valorar la situación que existe en el área de TI, con respecto a la seguridad de la información con base en información obtenida por medio de normas aplicadas a la seguridad de la información así como de diferentes fuentes bibliográficas, uso de la internet, revistas, libros y documentos oficiales, además fue necesario acudir a fuentes de experiencias internacionales donde la seguridad de la información es un elemento importante de las políticas de la empresa.

Es de alcance descriptivo, pues la investigación se realizó partiendo del conocimiento y experiencia de la situación que tiene una empresa mexicana basada en las TI y que la seguridad de la información es crucial para la organización; es por ello que se debe conocer la situación actual y su problemática en relación con la seguridad de la información. Esta investigación descriptiva permitió conocer las propiedades y características más importantes del sujeto de estudio así como los diferentes aspectos a analizar.

Así mismo, el eje temporal es de orden transversal; los diseños de investigación transeccional o transversal recolectan datos en un momento o tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado (Hernández, Fernández y Baptista, 2010). El criterio de clasificación de la

investigación en cuanto a su dimensión temporal es transversal o transeccional por el análisis y recopilación de la información de la empresa, el cual se llevó a cabo de enero de 2014 a abril de 2016.

4.2 Diseño de la investigación

Una vez que se tiene el carácter del fenómeno de estudio, el alcance inicial y el eje temporal de la investigación, se seleccionó el contexto particular de estudio. En este caso es un diseño no experimental, ya que no se manipularon las variables. Es decir, se trata de un estudio donde se observaron los fenómenos tal como se dan en su contexto natural, los cuales fueron analizados posteriormente (Hernández, Fernández y Baptista, 2010).

Para esta investigación no experimental, las variables de seguridad de la información, tecnologías de la información, amenazas y vulnerabilidades, se observaron tal como funcionan en la empresa de donde se obtuvieron resultados que permitieron diseñar la propuesta que ayude a disminuir la dimensión de los riesgos de la seguridad de la información.

4.3 Variables

Una variable es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse (Hernández, Fernández y Baptista, 2010). La definición de variable determinada en esta investigación, se realizó con base en el análisis del sujeto y objeto de estudio, tomando en cuenta las causas que provocan el problema antes expuesto.

Las variables que se tienen para esta investigación son:

1. *Tecnologías de la información*
2. *Seguridad de la información*
3. *Amenazas*
4. *Vulnerabilidades*

4.4 Establecer guía y análisis.

Para este trabajo también se hizo una investigación documental, la cual comprende los siguientes puntos:

- Revisión de los registros de las quejas de los clientes, con respecto a la baja seguridad de la información que se tiene en la empresa
- Revisión de los documentos que contengan las tecnologías de la información que están aplicadas
- Revisión de las políticas y controles que existen en la empresa

El carácter documental de esta investigación es de acuerdo con Barboza (2006), quien identifica las características siguientes:

1. Es un método de análisis de imágenes y de otros fenómenos culturales, donde se analizan los aspectos formales, de contenido característico del objeto de estudio, sin limitarse a un análisis inminente que, cuando se analiza la concepción del mundo se expresa a través de esos aspectos formales.
2. Cuando se amplía el análisis de varios fenómenos culturales no se acota a un campo sino a diferentes esferas culturales de una época, de una generación o grupo social que expresa en un estilo común a todas ellas. Es por esto que el método documental supera el análisis formal para llegar a un análisis autónomo y especializado para ubicarse en un análisis interdisciplinar.

Para Dulzaides y Molina (2004), el análisis documental es una forma de investigación técnica, un conjunto de operaciones intelectuales que buscan describir y representar los documentos de forma sistemática y unificada para facilitar su recuperación. Comprende el procesamiento analítico – sintético que incluye la descripción bibliográfica y general de la fuente, la clasificación, indización, anotación, extracción, traducción y confección de reseñas. El tratamiento documental significa también una extracción científico – informativa que propone ser un reflejo objetivo de la fuente original. Asimismo, busca identificar, describir y representar el contenido de los documentos en forma distinta a la original, con el propósito de garantizar su recuperación selectiva y oportuna, además, de posibilitar su intercambio difusión y uso, ver Tabla11.

Investigación documental	Pasos
Formulación del problema	• Definición del problema • Definición de los alcances • Definición de los problemas a responder
Ejecución del problema	• Recolección de información o de fuentes de información • Organización de los datos • Análisis de datos y organización del informe
Formulación y representación de la información	• Redacción de la investigación documental

Tabla 13. Investigación documental
(Fuente: Tema 3: Investigación documental; 2009)

Para fundamentar la investigación documental se construyó un supuesto teórico que sirvió de guía para identificar los alcances de los contenidos de análisis en relación con las variables.

4.5 Supuesto teórico

En la empresa hay una deficiencia en la aplicación de las TI en materia de seguridad de la información, por lo que la aplicación de la propuesta de seguridad de la información, con base en las TI, ayudará a minimizar las vulnerabilidades y amenazas de seguridad de la información en la empresa.

De acuerdo a este enunciado se seleccionan las variables que se indican a continuación:

1. *Tecnologías de la información*
2. *Seguridad de la información*
3. *Amenazas*
4. *Vulnerabilidades*

Definidas las variables de esta investigación, se establecieron los patrones para la obtención de información que por tratarse de una investigación documental, se dividen en información primaria, secundaria y terciaria, y cada una de ellas tiene elementos especiales que la componen (ver Tabla 14). La búsqueda de información se realizó en diferentes fuentes de investigación tales como libros, revistas y artículos, analizados en el marco teórico. La búsqueda en internet ofreció el mayor aporte para la investigación de estudios documentales de las variables de tecnologías de la información, seguridad de la información, amenazas y vulnerabilidades.

INVESTIGACION DOCUMENTAL. TIPO DE INFORMACION	ELEMENTOS DE INFORMACION
Información primaria	Información proveniente directamente de la investigación: • Artículos de revistas • Trabajos de grado • Tesis doctorales • Libros
Información secundaria	Información procesada por otras personas: • Manuales • Tratados • Diccionarios • Enciclopedias

Información terciaria	Ayudan a obtener información:
	• Revistas de información bibliográfica
	  ◦ Indicativas
	  ◦ Analíticas
	  ◦ Sintéticas
	• Bases de datos
	• Internet
	  ◦ Buscadores

Tabla 14. Tipos de investigación documental
(Fuente: Tema 3: investigación documental; 2009)

En la Tabla 15 se muestran los puntos principales de investigación documental de esta tesis, tales como, sector en el cual se hace la investigación documental, objetivo de la búsqueda, búsqueda o rastreo de la información, reportes documentales donde se extrajo información, y la publicación de los estudios, y qué es lo que se busca hacer con los resultados.

INVESTIGACIÓN DOCUMENTAL	SEGURIDAD DE LA INFORMACIÓN
Individuo, institución o sector de la investigación documental	Sector redes y comunicaciones
Objetivo de la búsqueda documental	Identificar y analizar las quejas recibidas por los clientes en el ámbito de seguridad de la información, así como revisar los documentos que contengan las tecnologías de la información que se tienen aplicadas en la empresa, para poder diseñar un propuesta que aumente la seguridad de la información
Rastreo y búsqueda de información para la investigación	• Libros (información primaria) • Artículos (información primaria) • Tesis (información primaria) • Internet: Páginas web de empresas especializadas, universidades, asociaciones (información terciaria) • Revistas (información primaria) • Buscadores digitales (información terciaria)
Reportes documentales que se presentan en este trabajo de investigación	1. "Quejas presentadas por clientes Care Enterprise Networks, 2014" Realizado por el área de TI. Autor: Care Enterprise Networks 2. "Tecnologías de la información aplicadas en Care Enterprise Networks, 2014" Realizado por el área de TI. Autor: Care Enterprise Networks 3. "Análisis de amenazas y vulnerabilidades, 2015" Realizado por el área de TI y redes y comunicaciones. Autor: Care Enterprise Networks
Variables empleadas en esta investigación documental	1. Tecnologías de la información 2. Seguridad de la información 3. Amenazas 4. Vulnerabilidades
Presentación de resultados	• Cada caso documental tendrá su propio análisis • Se darán como parte de esta tesis, recomendaciones y conclusiones sobre la seguridad de la información en Care Enterprise Networks

Tabla 15. Desglose de la investigación documental
(Fuente: Elaboración propia)

En la construcción de esta investigación se empleó principalmente información obtenida de páginas WEB, seguida por libros especializados en temas específicos de la seguridad de la información. Para la obtención de información relevante se emplearon buscadores como: Google académico, ERIC, y World Wide Science, así mismo se

investigó en páginas web del gobierno como la Secretaría de Comunicaciones y Transportes, el CISEN (Centro de Investigación y Seguridad Nacional), la CIDGE (Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico), US – CERT (United States Computer Emergency Readiness Team), FBI (Federal Bureau of Investigation). Se extrajo información relevante de organismos mundiales de cooperación como la UNESCO. Se investigó información de organismos nacionales y mundiales como el INEGI (Instituto Nacional de Estadística y Geografía), la ASI (Alianza por la Seguridad en Internet), ISO (International Organization for Standardization), ISF (Information Security Forum), ITU (International Telecommunication Union) y del World Economic Forum. Instituciones educativas tales como la UNAM, IPN y Tecnológico de Monterrey. Organismos de inversión como Deloitte, Ernst & Young y PWC (Price Waterhouse Coopers). Así mismo se extrajo información de páginas web relacionadas a las TI con respecto a seguridad de la información como Cisco Systems, Kaspersky, McAfee, Fortinet, Juniper Networks, Sonicwall, Sophos, ESET, Symantec, Check Point, HP (Hewlett Packard), Microsoft, Schlage, Netapp y Arbor Networks.

Una vez localizadas las fuentes, se extrajo información que podría ser relevante para esta tesis, se analizó el contenido que se consideró importante, se llevó a cabo un filtro de información apegada al tema investigado y se redactó la información más relevante.

Al definirse la estrategia metodológica, objetivo general y objetivos específicos, preguntas de investigación y supuesto teórico, se da paso a la propuesta de la investigación, apoyada en el análisis documental y análisis de la información y datos de la problemática de la empresa estudiada, la cual se presenta en el siguiente capítulo.

CAPÍTULO 5. Propuesta para aumentar la seguridad de la información en la empresa Care Enterprise Networks.

5.1 Objetivo de la propuesta

El objetivo de esta propuesta es incrementar la seguridad de la información para aminorar las amenazas, vulnerabilidades y riesgos dentro de la empresa Care Enterprise Networks.

Esta propuesta se lleva a cabo con base en el análisis de los documentos obtenidos de la empresa y que fundamentan la investigación que se realizó de manera lógica y física en los activos de la empresa.

5.2 Alcances y limitaciones de la propuesta

- Está orientada a disminuir las vulnerabilidades en los servicios que presta el negocio, para aumentar la confiabilidad de la empresa.

- Esta propuesta se limita a proponer controles para las vulnerabilidades conocidas hasta el momento, mediante software, hardware, políticas y recomendaciones.

- No se contempla una solución integral de seguridad, como podría ser la herramienta de seguridad perimetral.

- Esta propuesta es para la protección física y lógica de la información, tomando en cuenta sus propiedades de confidencialidad, integridad y disponibilidad.

5.3 Propuesta económica para mejorar la seguridad de la información en la empresa Care Enterprise Networks.

La siguiente propuesta económica se basa en la investigación que se realizó en los departamentos de TI, operaciones y niveles de servicio que corresponden a la empresa Care Enterprise Networks. Esta investigación se basa en los documentos de la empresa, las quejas hechas por los clientes, las TI que tiene la empresa (hardware, software, servidores, equipos de comunicación), y los elementos principales que conforman la infraestructura de la misma.

Las actividades que conforman la propuesta económica son:

- Revisión de las quejas hechas por los clientes
- Revisión de las TI aplicadas en la empresa hechas por el especialista en seguridad de la información
- Informe de análisis de amenazas
- Informe de análisis de vulnerabilidades
- Plan para mejorar la seguridad con base en las amenazas y vulnerabilidades encontradas
- Basar el plan de mejora en un sistema de gestión de seguridad de la información: ISO/IEC 27001:2013
- Conclusiones y recomendaciones
- En caso de aceptar la propuesta económica se entrega un nuevo plan de actividades junto con los entregables posibles.

Con base en las actividades mencionadas anteriormente e incluyendo las visitas de especialistas así como los honorarios correspondientes, el costo de la propuesta está estimada en $ 20,000 USD, más I.V.A.

De acuerdo a las necesidades del mercado de seguridad de la información, es necesario implementar un sistema de gestión basado en procesos y buenas prácticas que conlleven la mejora continua dentro de toda la empresa; por tal motivo se recomienda la implementación del sistema de gestión ISO/IEC 27001:2013.

Si la empresa se interesa por la implementación de la propuesta, el siguiente costo cubre los puntos anteriores, más entregables y las auditorias pertinentes por BSM para obtener la certificación. El costo es de $50,000 UDS, más I.V.A.

5.4 Revisión y aceptación de propuesta

Con base en el análisis realizado por la empresa y con base en las ventas netas reflejadas en la Tabla 4, se tiene que la propuesta para implementar un sistema de gestión para la obtención de la certificación de ISO/IEC 27001:2013, no es costeable para la empresa ya que de acuerdo a la inversión proyectada que es del 17% con respecto a las venta netas no se logra cubrir el costo, sin embargo con el 17% si se logra cubrir la propuesta para mejorar la seguridad de la información con base en el sistema ISO/IEC 27001:2013

Tipo de Nodo	Nodos monitoreables	Total
MPLS	15,576	$ 37, 382, 400
IDE	9,987	$ 23, 968,800
ADSL	1,123	$ 2, 695, 200
PEX	225	$ 540, 000
Total	26,911	$ 64, 586, 400

Tabla 4. Dispositivos monitoreables vs Ventas netas 2015
Fuente: (Cnvrep003\ Finanzas\Dispositivos monitoreables Vs ventas, 2015)

5.5 Amenazas, Vulnerabilidades y Riesgos. Forma de atacarlas y/o controlarlas con base en la norma ISO/IEC 27001:2013.

De acuerdo a la investigación realizada en cada departamento de la empresa y a la investigación documental, se encontraron ochenta y dos vulnerabilidades, las cuales fueron mapeadas con las trece amenazas que se clasificaron con base en ISO/IEC 27001:2013.

Amenazas:

1. Acceso no autorizado
2. Robo o fuga de información
3. Cambios no autorizados
4. Ataques lógicos internos y externos
5. Indisponibilidad o degradación de los servicios o aplicaciones
6. Código malicioso o hackeo
7. Daños a equipos o instalaciones
8. Inundación
9. Incendio
10. Falla de suministro de energía eléctrica
11. Sismo
12. Ingeniería social
13. Retraso en la entrega de servicios

A continuación se realiza la propuesta con base en la diferentes TI y con base en la norma de ISO/IEC 27001:2013.

Para cada amenaza se proponen acciones y recomendaciones

1. Acceso no autorizado

Se deben de difundir las políticas establecidas en la empresa, así como la mejora de ellas para fortalecer las medidas preventivas de vulneración para el acceso a los equipos.

Las políticas de la empresa deben de ser entregadas físicamente a cada integrante de la organización para que sean firmadas de recibido y se cuente con la seguridad de que se han revisado.

Se requiere endurecer las reglas de autenticación, encriptación y autorización mediante las diferentes tecnologías de la información que sean necesarias. Estas tecnologías de la información deben de ser evaluadas mediante un ambiente de pruebas, antes de pasar a producción. Las encriptaciones que se lleguen a realizar en los diferentes equipos, se tienen que documentar en un cambio que esté ligado a cada equipo que está siendo afectado (ver tabla 16).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Acceso no autorizado	Contraseñas compartidas por administradores	MEDIO	Realizar auditoria y revisión continua de los horarios y fechas de ingreso al sistema, contra las fechas y horarios en que esta el usuario registrado.
	Errores en la identificación y autenticación	MEDIO	Implementar nuevo software que no tenga alguna falla al autenticar o identificar usuarios y/o contraseñas
	Puertos abiertos	MEDIO	Realizar un escaneo de los puertos en los equipos con mayor vulnerabilidad cada determinado tiempo
	Configuración inadecuada por falta de validaciones	MEDIO	Tener un script que valide los puntos principales aunque no se tenga una validación
	Mala asignación de privilegios	BAJO	Revisión programada de los privilegios de cada usuario para evitar privilegios no autorizados
	Uso de configuraciones predeterminadas	BAJO	Revisión de los parámetros más importantes antes de aplicar la configuración a los equipos de comunicación
	Acceso de personal a áreas restringidas/no autorizadas	ALTO	Acompañar en todo momento al persona no autorizado a áreas restringidas para ser supervisados
	Ingeniería social a guardias de seguridad de la entrada principal	MEDIO	Validar identificaciones y nombres de cada persona para evitar un acceso mal intencionado a la empresa
	Eliminar información propietaria de la empresa	ALTO	Correlacionar la información que se intenta eliminar mediante una alarma al sistema central
	Falta de actualizaciones o cambios a los sistemas y aplicaciones sin ejecución de pruebas previas en ambientes no productivos	MEDIO	Llevar a cabo un plan previo para la ejecución de pruebas antes de la implementación del sistema para posterior llevarlo a producción

Tabla 16. Acceso no autorizado
Fuente: (Elaboración propia)

2. Robo o fuga de información

Dar a conocer las políticas de la empresa así como los actos jurídicos a que se pueden hacer acreedores las personas que intenten sustraer información importante de la empresa.

Se debe entregar por escrito las políticas y reglamento de la empresa, así como la firma del trabajador de que recibió dicha información para que se asegure la empresa que se tiene el conocimiento en caso de violación a dichas políticas y/o reglamento.

Además se requiere implementar software que no sea penetrado tan fácilmente por usuarios no autorizados. El software debe de ser previamente certificado y avalado por el comité de seguridad de la empresa de acuerdo a la metodología de ISO 27001.

El proveedor de software o hardware debe contar con una certificación que avale que los elementos adquiridos cuenten con las especificaciones estándar en el mercado (ver tabla 17).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Robo o fuga de información	Acceso a información del Disco Duro (DD) / No cifrado (información no cifrada)	MEDIO	Encriptar los documentos o archivos más importantes para tenerlos protegidos
	Falta o falla de controles de acceso físico o lógico	MEDIO	Realizar auditorías periódicas para verificar alguna nueva vulnerabilidad o falta de controles de acceso
	Falta de monitoreo a dispositivos	MEDIO	Escanear la red LAN de la empresa cada determinado tiempo para verificar si los dispositivos actuales están monitoreados correctamente
	Falta de procedimientos para notificación de incidentes	BAJO	Automatizar la herramienta de documentación para que las notificaciones sean en automático
	Copiar información en CD o USB	MEDIO	Quitar unidad de CD en todas las PC y lap top de la empresa, así como denegar el acceso al copiado de información a través de la USB
	Falta de concienciación en temas de seguridad, negligencia o impericia	ALTO	Programar cursos o platicas cada determinado tiempo para la concienciación de los temas, al personal de la empresa
	No se realiza un Backup	ALTO	Programar a los software específicos para que los backup se respalden en determinados periodos de tiempo
	Uso inadecuado de los servicios de mensajería instantánea (Whatsapp, Skype)	MEDIO	Bloquear los puertos de software mal intencionado dentro de la empresa y dar uso a los software de la empresa

Tabla 17. Robo o fuga de información
Fuente: (Elaboración propia)

3. Cambios no autorizados

Concienciación al personal de la empresa que juega un rol en el proceso de cambios, para que lleve a cabo el procedimiento adecuado en todo el clico del proceso, además de apegarse a las mejores prácticas que establece la metodología de ISO 27001.

Se debe de controlar los accesos tanto a equipos como para los diferentes niveles privilegiados de acceso a la información para evitar algún cambio no previsto o no analizado adecuadamente.

Además se debe de contar con un manual que especifique el procedimiento de cambios, así como los niveles de impacto que se tendrían en caso de llegar a aplicar un cambio que no tenga análisis o que haya pasado por un esquema de prueba en donde se refleje que de llevarse a cabo no impactaría a la operación del cliente (ver tabla 18).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Cambios no autorizados	Inadecuada asignación de privilegios	BAJO	Revisión programada de los privilegios de cada usuario para evitar privilegios no autorizados
	Falta o falla en la supervisión e implementación de cambios	ALTA	Dejar como responsable a otro usuario cuando no se tenga disponibilidad por parte de supervisión, y en el caso de falla se agrega nuevo procedimiento para que un especialista revise el cambio implementado
	Falta de expertis del personal	MEDIO	Capacitación constante en las diferentes plataformas tecnológicas, así como la revisión de los entregables por parte de un supervisor
	Mal diseño de la solución	MEDIO	Revisión por parte del área de especialistas para estudiar los puntos medulares del diseño y de esta manera contribuir a un mejor diseño
	Falta de detección de nuevas vulnerabilidades que provoquen afectaciones a los aplicativos	ALTO	Auditorias periódicas para la revisión de puertos y software vulnerable
	Falta de actualizaciones o cambios a los sistemas y aplicaciones sin ejecución de pruebas previas en ambientes no productivos	MEDIO	Programar cada software para que indique que cuenta con una nueva actualización para posterior hacer las pruebas necesarias de testing y corroborar que las nuevas actualizaciones no afecten el sistema en producción
	Acceso no autorizado (Debilidad en la gestión de accesos)	ALTO	Verificar que los usuarios y contraseñas sean los apropiados
	Uso de contraseñas predeterminadas	ALTO	Programar el software de los servidores y equipos para que el usuario y contraseña cumplan con determinados parámetros

Tabla 18. Cambios no autorizados
Fuente: (Elaboración propia)

4. Ataques lógicos externos e internos

Mediante el uso de las tecnologías de la información se debe realizar una ingeniería robusta que endurezca los hoyos que se detecten en los diferentes equipos y software instalados en la empresa, y así evitar accesos no autorizados a los diferentes equipos de comunicación, servidores, PC, mainframe, bases de datos, etc.

Se deben de controlar accesos físicos y lógicos a toda la infraestructura de la organización mediante usuarios y passwords robustos de tal forma que no sean cifrados rápidamente por algún atacante. Estos passwords deben de cambiarse cada tres meses por seguridad de casa usuario y de la empresa.

Se deben de realizar periódicamente auditorias que revisen cada una de las amenazas en el entorno que conlleven al descubrimiento de nuevas vulnerabilidades tanto a nivel lógico como físico (ver tabla 19).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Ataques lógicos externos e Internos	Falta o falla de seguridad perimetral	ALTO	Realizar pruebas de vulneración en la red para verificar en qué puntos se requiere la seguridad perimetral. Se debe de agregar un procedimiento en caso de falla de la seguridad perimetral
	Falta de concienciación en temas de seguridad	MEDIO	Realizar cursos o platicas periódicamente para que los usuarios tengan concienciación de los temas de seguridad informática
	Falta o falla de parches o actualizaciones	ALTO	Programar el software con el que cuenta cada servidor para que se descarguen en automático los parches o actualizaciones
	Uso incorrecto de activos por parte del personal	MEDIO	Hacerle saber al personal de las políticas internas de la empresa así como de las acciones legales a las que se pueden hacer acreedores
	Falta o falla en la supervisión e implementación de cambios	MEDIO	Dejar como responsable a otro usuario cuando no se tenga disponibilidad por parte de supervisión, y en el caso de falla se agrega nuevo procedimiento para que un especialista revise el cambio implementado
	Negligencia de personal	MEDIO	Hacerle saber al personal de las políticas internas de la empresa así como de las acciones legales a las que se pueden hacer acreedores
	Características de base de datos innecesariamente habilitadas	MEDIO	Auditar periódicamente las bases de datos con el objetivo de evitar ataques o penetraciones mal intencionadas
	Exposición de cookies de sesión a terceros mal intencionados	MEDIO	Borrar las cookies cada determinado periodo

Tabla 19. Ataques lógicos externos e internos
Fuente: (Elaboración propia)

5. Indisponibilidad o degradación de los servicios o aplicaciones

Contar con un plan de mantenimiento a toda la infraestructura y servicios que presenta la empresa así como mantener actualizados los diferentes tipos de software y hardware que soportan los servicios críticos del negocio.

Este plan debe ser apegado a las recomendaciones de la ISO 27001, donde menciona que los servicios de negocio deben de contar con una revisión constante para ofrecer servicios que sean satisfactorios para el cliente (ver tabla 20).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Indisponibilidad o degradación de los servicios o aplicaciones	Configuración inadecuada (falta de procedimientos formalmente establecidos, configuraciones por defecto, falta de restricciones, privilegios inadecuados).	ALTO	Revisión y análisis de las nuevas configuraciones así como la supervisión post configuración
	Errores en la programación de scripts	MEDIO	Supervisión y revisión en cada script elaborado
	Falta de expertis del personal	MEDIO	Capacitación constante en las diferentes plataformas tecnológicas, así como la revisión de los entregables por parte de un supervisor
	Mala gestión de capacidades (licenciamiento, almacenamiento, memoria física, procesamiento, configuraciones, balanceo)	MEDIO	Revisión por parte de especialistas para el correcto estudio de factibilidad de software y hardware necesario requerido
	Expiración de licencias	ALTO	Agregar un procedimiento que contemple la revisión de las fechas en que el software está próximo a vencer
	Mantenimiento inadecuado	MEDIO	Supervisión y revisión post mantenimiento
	Falta de instalación de parches y/o actualizaciones	MEDIO	Programar el software con el que cuenta cada servidor para que se descarguen en automático los parches o actualizaciones
	Término de contrato para el soporte con proveedores	BAJO	Revisión periódica de los OLA con cada proveedor, para definir nuevos contratos
	Software libre (sin contratación de soporte)	MEDIO	Revisión constantes por parte de especialistas en software para determinar mejoras o riesgos en la operación
	Personal interno, externo o terceros mal capacitados	MEDIO	Supervisar las actividades y tareas asignada que realiza el personal.

	Falta de equipos para poder garantizar la reposición de dispositivos	MEDIO	Contar con un stock de al menos cinco dispositivos para garantizar la continuidad de la operación
	Daño en el cableado por incumplimiento de medidas de seguridad necesarias para las instalaciones de la empresa	MEDIO	Revisión y supervisión del cableado para corroborar que se cuentan con las medidas de seguridad y el cumplimiento de las normas establecidas
	Instalación de parches o actualizaciones sin pruebas previas	MEDIO	Revisión y seguimiento adecuado del procedimiento que se tiene que seguir en estos casos
	Falta de redundancia y/o dependencia del proveedor	ALTO	Contratar un enlace redundante y con diferente proveedor para asegurar alta disponibilidad en el trafico de información
	Fallo de funcionamiento del software o hardware del fabricante por falta de mantenimiento	ALTO	Contar con un plan de revisión en periodos de tiempo determinados para asegurar el correcto funcionamiento y prever fallas
	Pérdida de paquetes durante la transmisión de datos	MEDIO	Asegurar la correcta configuración de los diferentes perfiles de QoS tanto en equipos de transmisión como de comunicación
	Saturación de memoria física y/o virtual por sobrecarga de procesos en el S.O.	MEDIO	Contar con equipo y enlace redundante en caso de tener un crash en el equipo por exceso de procesamiento
	Curva de aprendizaje por alineación de personal a procesos	MEDIO	Capacitar al nuevo personal conforme a los planes de inducción en tiempo y forma
	Personal interno o externo mal intencionado, descontento o negligente (Ej. personal de otros NOC en etapas de migración de nuevos clientes)	ALTO	Aplicar medidas de seguridad y ejecutar el código penal conforme a los actos de negligencia

Tabla 20. Indisponibilidad o degradación de los servicios o aplicaciones
Fuente: (Elaboración propia)

6. Código malicioso o hackeo

Con la ayuda de las tecnologías de la información se debe realizar una reingeniería para endurecer la seguridad de la información y garantizar que los datos alojados en los diferentes equipos de la estructura no sean vulnerados o hackeados por personas ajenas a la empresa.

También se debe de realizar una auditoría de seguridad de acuerdo a la ISO 27001, en donde especifica que se deben evaluar todos los equipos que conforman los servicios críticos que ofrece la empresa.

Las auditorias de seguridad deben de ser internas por parte de la empresa y las externas deben de ser aplicadas por un ente externo que especifique los puntos potenciales a vulnerar e indique las medidas a implementar o a corregir en la infraestructura de la empresa (ver tabla 21).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Código malicioso o hackeo	Puertos abiertos	ALTO	Hacer un escaneo de la red, servidores y equipos de comunicación cada determinado periodo de tiempo para detectar y llevar a cabo las medidas correspondientes
	DNS Spoofing	ALTO	Revisar que todas las conexiones hacia paginas externas sean a través de “https” y validar que la página no sea un clon
	Falta de actualización de parches	MEDIO	Programar periódicamente los software que requieren los parches o actualizaciones necesarias
	Servicios WEB débiles	MEDIO	Cerrar configuraciones por default para evitar disclosure de información así como endurecer algoritmos de cifrado
	Instalación de software sin autorización (software mal intencionado)	MEDIO	Ejecutar medidas de seguridad en cada Pc, lap top o servidores en donde impida la instalación de cualquier tipo de software. La instalación de nuevo software será llevada a cabo bajo supervisión

	Equipos de seguridad con configuración faltante	ALTO	Supervisar la configuración aplicada en cada equipo de acceso para asegurar que no se tengan puertos abiertos o que la información no sea encriptada
	No se realiza la actualización del Antivirus	MEDIO	Programar cada determinado periodo de tiempo que el software de antivirus se actualice constantemente y evitar software mal intencionado
	Segregación de redes	MEDIO	Por cada área de la empresa se tiene que hacer una VLAN con la finalidad de que los servidores y equipos dentro de la red tengan mayor seguridad
	DoS (Denial of service)	ALTO	Tener un plan de acción en el cual se tenga contemplado un ataque de esta magnitud, para lo cual se debe contar con un algoritmo riguroso en donde se validen que las solicitudes son reales
	Bug en IOS en los equipos de comunicación (router, switch y firewall)	ALTO	Tener un plan de revisión de los diferentes IOS que están instalados en los equipos de comunicación con la finalidad de que se busquen Bug en los software y encontrar una actualización que contrarreste esa amenaza
	Virus informáticos o algún tipo de malware (código de malicioso)	ALTO	Concienciación al personal que labora en la empresa de contar con antivirus actualizado, de no introducir memorias, de no bajar archivos sospechosos, etc.

Tabla 21. Código malicioso o hackeo
Fuente: (Elaboración propia)

7. Daño a equipos e instalaciones (Equipo Insuficiente)

Todas las instalaciones, infraestructura y servicios del negocio deben de contar con un respaldo de acuerdo a lo recomendado por la ISO 27001. De esta manera se puede garantizar la continuidad del negocio en caso de tener un incidente que afecte la entrega de servicios al cliente.

Además de que se debe contar con un respaldo, se debe de tener un plan de mantenimiento para toda la infraestructura, igualmente de la supervisión cuando se hagan instalaciones o mantenimientos a la infraestructura de la empresa.

De acuerdo a las recomendaciones de la ISO 27001, se deben de tener OLA´s (Operational level agreement), especificados con los diferentes proveedores de servicio para que se garantice tanto el mantenimiento como la calidad de los servicio tangibles e intangibles (ver tabla 22).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Daño a equipos e instalaciones (Equipo Insuficiente)	Falta de mantenimiento (Fuerza y Clima)	BAJO	Contar con una revisión periódica de todos los equipos de fuerza y clima para contrarrestar algún evento en los equipos
	Deficiente instalación del cableado que soporta a los equipos	MEDIO	Supervisar la instalación y mantenimiento de los cableados de la red así como verificar que los cableados cumplan con las normas adecuadas
	Personal mal intencionado o negligente	ALTO	Hacerle saber al personal de las medidas legales de las que pueden ser acreedores en caso de levar alguna acción que afecte los servicio o información de la empresa
	Falla en los componentes por falta de mantenimiento o agua, humedad, polvo, suciedad, corrosión, exposición solar o tiempo de vida	MEDIO	Contar con un plan de mantenimiento preventivo y correctivo para asegurar que los dispositivos y componentes que conforman la infraestructura de la empresa tengan buena funcionalidad
	Desgaste por obsolescencia o daño por defecto de fábrica (componente defectuoso)	MEDIO	Verificar que los componentes o dispositivos cuenten con las normas de calidad establecidas, así como asegurar los niveles de OLA establecidos entre el proveedor y la empresa
	Acceso físico no autorizado	ALTO	Contar con seguridad perimetral dentro y fuera de las instalaciones, así como bloquear el acceso a personal no autorizado, a menos que sea acompañado por personal de la empresa dentro de las instalaciones
	Montaje incorrecto de equipos	BAJO	Supervisión y revisión del correcto acoplamiento de los equipos en los rack correspondientes

Tabla 22. Daño a equipos e instalaciones (Equipo Insuficiente)
Fuente: (Elaboración propia)

8. Inundación

En la metodología de ISO 27001 recomienda que se tengan los equipos de comunicación en instalaciones seguras, es decir, que cuenten con una certificación en seguridad, la cual respalda la infraestructura arquitectónica del lugar donde se ubiquen los equipos.

Cabe mencionar que el lugar debe de contar con controles rigurosos para catástrofes o eventos climatológicos que afecten la continuidad de los servicios (ver tabla 23).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Inundación	Ubicación inadecuada del centro de datos	MEDIO	Análisis exhaustivo de la ubicación para evitar perdida de equipo e información vital de la empresa. Contar con un sitio alterno
	Inadecuado mantenimiento de tuberías	MEDIO	Supervisión periódica de las tuberías de agua dentro y fuera de las instalaciones

Tabla 23. Inundación

Fuente: (Elaboración propia)

9. Incendio

De acuerdo a la metodología ISO 27001, recomienda que se tengan los equipos en instalaciones seguras, que cuenten con una certificación en seguridad, la cual debe contar con instalaciones eléctricas y tomas de agua que hayan sido avaladas por dicha certificación.

Es necesario mencionar que el lugar debe de contar con controles rigurosos para catástrofes o eventos climatológicos que afecten la continuidad de los servicios (tabla 24).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Incendio	Ubicación inadecuada del centro de datos	MEDIO	Análisis exhaustivo de la ubicación para evitar perdida de equipo e información vital de la empresa. Contar con un sitio alterno
	Inadecuado mantenimiento a la instalación eléctrica	MEDIO	Supervisión periódica del cableado, centros de carga, tubería, baterías y centros de respaldo.

Tabla 24. Incendio
Fuente: (Elaboración propia)

10. Falla de suministro de energía eléctrica

En ISO 27001 se recomienda que las instalaciones cuenten con una certificación en seguridad, la cual respalda la infraestructura eléctrica del lugar tanto de instalación como la calidad de cableado.

El lugar debe de contar con controles rigurosos para catástrofes o eventos climatológicos que afecten la continuidad de los servicios (tabla 25).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Falla de suministro de energía eléctrica	Dependencia del proveedor	MEDIO	Tener centros de respaldo de energía eléctrica para los equipos de alta disponibilidad para la empresa
	Falta de suministro de energía alterna	MEDIO	Tener planta de emergencia en caso de que el centro de carga se termine
	Mantenimiento inadecuado	MEDIO	Supervisión de los centros de carga y de plantas de energía periódicamente

Tabla 25. Falla de suministro de energía eléctrica
Fuente: (Elaboración propia)

11. Sismos

Para la ISO 27001, es imperioso que los equipos de comunicación e infraestructura de la empresa estén en instalaciones seguras, que cuenten con una certificación en seguridad, la cual respalda la infraestructura arquitectónica del lugar donde se ubiquen los equipos tecnológicos.

El site debe de contar con controles rigurosos para catástrofes o eventos climatológicos que afecten la continuidad de los servicios. Además se debe de contar con los planes de acción correspondientes en caso de un sismo (tabla 26).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Sismo	Ubicación geográfica	MEDIO	Análisis exhaustivo de la ubicación y de las instalaciones. Contar con un sitio alterno.

Tabla 26. Sismos
Fuente: (Elaboración propia)

12. Ingeniería social

Con base en la metodología de ISO 27001, se deben promover pláticas y concienciaciones sobre las políticas establecidas en la empresa, así como los puntos medulares que se deben de tomar en cuanto se tenga sospecha de tecnologías fraudulentas que puedan ocasionar robo de información.

Las pláticas y/o concienciaciones se deben de impartir a todo el personal que labora en la empresa para que se tenga el mayor cuidado con personal no autorizado o ajeno a la empresa (tabla 27).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Ingeniería social	Falta de concienciación del personal	MEDIO	Concienciación periódica y difusión de información sobre cómo cuidarnos de ser víctimas de esta amenaza
	Desconocimiento de Políticas y/o Procesos	MEDIO	Elaborar trípticos con las políticas y procesos más importantes así como la programación constante de los procesos y políticas que tiene la empresa

Tabla 27. Ingeniería social
Fuente: (Elaboración propia)

13. Retraso en la entrega de servicios

De acuerdo a ISO 27001, se debe de contar con un proceso de continuidad de los servicios que entrega la empresa en caso de tener algún desastre o eventos que afecten la entrega de los servicios de TI.

Además se debe efectuar un simulacro de manera programada, en el que esté notificado el cliente. Este simulacro ayudará a evaluar los puntos más relevantes del plan de continuidad para garantizar a los clientes la entrega de servicios TI (tabla 28).

Amenaza	Vulnerabilidad	Riesgo	Recomendación
Retraso en la entrega de servicios	Curva de aprendizaje por incremento de la plantilla de personal interno	BAJO	Capacitación y supervisión constante tanto en las tecnologías de la información como en los procesos con los que cuenta la empresa

Tabla 28. Retraso en la entrega de servicios
Fuente: (Elaboración propia)

Conclusiones

Las conclusiones que se extraen de la investigación, son:

Las TI han evolucionado rápidamente en el mundo y el uso del internet conlleva el uso de redes y comunicaciones, lo que hace necesario que se busquen mejores soluciones para contrarrestar la problemática de seguridad de la información que se tiene actualmente en la empresa Care Enterprise Networks.

A partir de la información analizada, se concluye que la seguridad de la información y la aplicación de las TI en la empresa, no son bien aplicadas en la áreas principales de la organización y que hace falta utilizar software y hardware especializado que contrarreste los ataques que ha tenido la empresa, así como el robo y pérdida de información a lo largo del tiempo.

También se concluye que no existe un proceso claro y conciso que la empresa comunique a todas las áreas de la organización, es por ello que también se requiere un modelo que conjunte tanto los procesos de seguridad como el uso y aplicación adecuada de las TI.

La organización cuenta con insuficientes recursos económicos y humanos para tener una infraestructura de vanguardia y contar con personal que tenga los conocimientos necesarios para que sean aplicados en el manejo de los equipos y aplicativos que tienen mayor amenaza y riesgo de ser penetrados.

En los 5 años que lleva la empresa en el mercado, ha tenido constantes ataques, robos y pérdida de información que se han traducido en un sinnúmero de quejas de los clientes que se han visto vulnerados en su información. Las quejas de los clientes han provocado que las encuestas de satisfacción denoten desconfianza por un servicio que no cuenta con la suficiente seguridad para proteger los datos.

Existen modelos de seguridad de la información en las TI como el ISO/IEC 27001:2013; esta metodología hace énfasis en los procesos básicos de seguridad de la información con la que deben contar las organizaciones para contrarrestar las amenazas y vulnerabilidades en el manejo de su información, sin embargo para la empresa no le es costeable implementar una certificación debido a que la empresa solo cuenta con el 17% de inversión para este tipo de proyectos.

De acuerdo a la última encuesta de certificaciones por parte de la ISO (ISO survey 2014 certifications), solamente hay 96 organizaciones en México certificadas en la norma ISO 27001; esto denota que las empresas de TI no han dado importancia a la seguridad de la información y tampoco han reforzado su infraestructura.

Care Enterprise Networks no tiene la suficiente liquidez financiera para invertir en tecnología de punta, en personal lo suficientemente capacitado para solventar algún ataque cibernético, ni en poder contar con alguna certificación que de seguridad a los clientes.

Recomendaciones

Se recomienda el uso y aplicación adecuada de las TI en las organizaciones, además de utilizar una metodología de seguridad de la información que indique los procesos y procedimientos adecuados que se tienen que llevar en la organización para salvaguardar la información; es decir, contar con una certificación en ISO/IEC 27001:2013 para tener apertura en el mercado y dar confiabilidad en el negocio y al activo más importante que son los clientes.

También se sugiere que las políticas que se implementen en las organizaciones sean claras, concisas y horizontales, para que cada integrante de la empresa pueda integrarse a los modelos de seguridad en TI y lograr que los procesos sean llevados a cabo adecuadamente.

Es recomendable que las organizaciones inviertan en infraestructura ya sea de software y de hardware para contrarrestar los ataques y penetraciones que se tienen constantemente, además se sugiere invertir en recursos humanos que tengan la capacidad para tener la visión de las amenazas y vulnerabilidades que se pueden tener en la empresa.

Se recomienda que las organizaciones realicen periódicamente auditorías internas para detectar los puntos vulnerables, y así aplicar una re-ingeniería tanto a los procesos como a la infraestructura que conforma la empresa. Auditoría externa para realizar pruebas de penetración desde puntos remotos y detectar puntos vulnerables de la infraestructura de la empresa.

Referencias

1. Abbate, J. (2000). Inventing the Internet (Inside Technology). EUA: MIT University Press.

2. Adell, J. (1997). Tendencias en educación en la sociedad de las tecnologías de la información, EDUTEC. Revista Electrónica de Tecnología Educativa, nº 7. Universitat de les Illes Balears.

3. Álvarez G., Pérez P. (2004). Seguridad Informática para la Empresa y Particulares. España: McGraw-Hill.

4. Andrews M., Whittaker J. (2006). How to Break Web Software: Functional and Security Testing of Web Applications and Web Services. EUA: Addison-Wesley

5. Barboza, A. (2006). Sobre el Método de la interpretación Documental y el uso de las imágenes en la Sociología. El Método Documental del Sociólogo: Karla Mannheim. Artículo. Brasil

6. Basin D., Schaller P., Schläpfer M. (2011). Applied Information Security. EUA: Springer

7. Cabero, J. A. (2007). Tecnología Educativa. España: McGraw-Hill.

8. Cabero, J. A. (2003). Mitos de la sociedad de la información: sus impactos en la educación. En Aguiar, M. V. y otros (coords): Cultura y Educación en la sociedad de la información, La Coruña: Netbiblo.

9. Cabero, J. A. (2001). Tecnología educativa: diseño, producción y evaluación de medios. Barcelona: Paidós.

10. Cabero, J. (2004). Reflexiones sobre la brecha digital. En F. Soto y J. Rodríguez (eds), Tecnología, educación y diversidad: retos y realidades de la inclusión digital, Murcia, Consejería de Educación y Cultura.

11. Camargo, M. I. G. (1990). Metodología para auditar la seguridad operativa de Instalaciones, Hardware y Software en centros de cómputo en México. México: Universidad Iberoamericana.

12. Pritchard, C. (2014). Risk Management, concepts and guidance. (Fifth Edition). EUA: CRS Press.

13. Castells, M. (2001). La Galaxia Internet. Reflexiones sobre Internet, empresa y sociedad. Madrid: Areté.

14. Castells, M. (1995). La ciudad informacional. Tecnologías de la Información, reestructuración económica y el proceso urbano-regional. Madrid: Alianza Editorial

15. Castells, M (2005). La Era de la Información. Vol. I: Economia, Sociedad y Cultura. La sociedad red. España: Alianza Editorial.

16. Castells, M (2013). La Era de la Información. Vol. II: Economia, Sociedad y Cultura. El poder de la identidad. España: Alianza Editorial.

17. Castells, M (2006). La Era de la Información. Vol. III: Economia, Sociedad y Cultura. Fin de milenio. España: Alianza Editorial.

18. Dulzaides, M., y Molina, A. (2004). Análisis Documental y de información: dos componentes de un mismo proceso. Articulo. Cuba: ACIMED-SCIELO.

19. Glendinning E., McEwan J. (2006). Information Technology. EUA: Oxford University Press.

20. Gómez A. (2011). Auditoria de Seguridad Informática. España: Starbook Editorial

21. Gonzalo A. (2006). Seguridad en Internet. España: Nowtilus

22. Hernádez, R., Fernández, C., y Baptista, M. (2010). Metodología de la investigación (5ta ed.). México: McGraw-Hill.

23. Leon A., y Leon M. (2009).Fundamentals of Information Technology. (2nd Edition). EUA: Vikas Publishing

24. Lévy-Leboyer, C. (2005). Administración de las organizaciones. Francia: Ediciones de Gestión

25. Martínez, F. (2007). La sociedad de la Información. La tecnología desde el campo de estudios CTS. Madrid. McGraw-Hill.

26. Martínez, F. y Solano, I. (2003). El proceso comunicativo en situaciones virtuales, en redes de comunicación en la enseñanza. Barcelona: Paidós

27. Mengo, O. (2009). Tema 3: Investigación Documental. Venezuela: Universidad Central de Venezuela. Facultad de Agronomía. Instituto de economía agrícola y ciencias sociales. Introducción a la metodología de la investigación científica y documental.

28. Whitman, M. y Mattord, H. (2012). Principles of Information Security. (4th Edition) EUA: Cengage Learning

29. Whitman, M. y Mattord, H. (2016). Management of information Security. (Fifth Edition). EUA: Cengage Learning

30. Mumford, M. D. (2000). Leadership skills for a changing world: Solving complex social problems. Journal: Leadership Quarterly

31. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy. (2nd Edition). EUA: Elsevier

32. Reynolds G. (2011). Ethics in Information Technology. (4th Edition). EUA: Course Technology

33. Stallings, W. (2013). Network Security Essentials: Applications and Standards. (4th Edition). EUA: Prentice Hall

34. Sterling, B. (1992). The Hacker Crackdown. EUA: Bantam Books

35. Téllez, J. (2004). Derecho informático. (3ª. Edicion). México: McGraw-Hill

Anexos

1. BS. (2013) Information security management systems. Requirements, ISO/IEC 27001:2013. Recuperado de: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

2. Arbor Networks. (2016). WorldWide Infrastructure Security Report. (Volumen XI). Recuperado de: https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf

3. CYBSEC. (2016) Los desafíos de la ciberseguridad y la ciberdefensa. Recuperado de: http://www.cybsec.com/ES/articulos/default.php

4. Department of Justice. (2013). Prosecuting Computer Crimes. Recuperado de: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

5. ISACA. (2009). The Risk IT Framework Excerpt. Recuperado de: http://www.isaca.org/knowledge-center/research/documents/risk-it-framework-excerpt_fmk_eng_0109.pdf

6. Comisión de Comunidades Europeas. (2001). Comunicación de la Comisión al Consejo y al Parlamento Europeo; Tecnologías de la información y de la comunicación en el ámbito del desarrollo. El papel de Las TIC en la política comunitaria de desarrollo. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52001DC0770&from=ES

7. Consejo Superior de Administración Electrónica. (2010). MAGERIT. Versión 3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de: http://administracionelectronica.gob.es/ctt/magerit#.V0-aCuSLXdc

8. Diario oficial de la federación (DOF). (2016) MAAGTICSI. Manual Administrativo de Aplicación General en Tecnologias de la información y comunicación en seguridad informática. Recuperado de: http://www.gob.mx/cidge/acciones-y-programas/politica-tic-maagticsi

9. World Economic Forum. (2016). What the G7 must do for internet growth and security. Recuperado de: https://www.weforum.org/agenda/2016/05/what-the-g7-must-do-for-internet-growth-and-security

10. ITU. (2003). La Seguridad de las Telecomunicaciones y las Tecnologías de la información. Recuperado de: http://www.itu.int/itudoc/itu-t/85097-es.pdf

11. National Institute of Standards and Technology, U.S. Department of Commerce. (2008). National Vulnerability Database. Recuperado de: http://nvd.nist.gov/

12. Price Waterhouse Coopers (PWC). (2012). Encuesta global de la seguridad de la información 2012 elaborada por pwc. Recuperado de: http://www.pwc.es/es/sala-prensa/notas-prensa/2011/encuesta-seguridad-informacion-2012-pwc.html

13. Ernest & Young. (2015). Encuesta global sobre seguridad de la información EY de 2015. Recuperado de: http://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015/$FILE/ey-encuesta-global-seguridad-informacion-2015.pdf

14. Deloitte. (2016). Panorama de Ciber Seguridad en México para 2016-2017. Recuperado de: http://www2.deloitte.com/mx/es/pages/risk/articles/ciber-seguridad-ciso-mty.html

15. Verizon. (2011). Verizon 2011 Payment Card Industry Compliance Report. Recuperado de: http://www.verizonenterprise.com/resources/reports/rp_2011-payment-card-industry-compliance-report_en_xg.pdf

16. CISCO. (2016). Informe anual de seguridad de cisco 2016. Recuperado de: http://globalnewsroom.cisco.com/es/la/press-releases/informe-anual-de-seguridad-de-cisco-revela-una-dis-1239705

17. CEPAL. (2010). Acelerando la revolución digital: Banda ancha para América Latina y el Caribe. Recuperado de: http://archivo.cepal.org/pdfs/ebooks/LCR2167.pdf

18. http://www.elfinanciero.com.mx/tech/aumentan-ciberataques-en-mexico.html

19. http://www.elfinanciero.com.mx/empresas/hackeo-a-liverpool-podria-costarle-mas-de-100-mdp-estiman.html

20. http://eleconomista.com.mx/tecnociencia/2015/01/20/geopolitica-tecnologia-nuevo-dilema-ciberseguridad

21. http://diarioti.com/la-gran-amenaza-informatica-en-2015-sera-el-robo-de-informacion-confidencial-de-las-empresas/84909

22. http://diarioti.com/los-12-principales-incidentes-de-seguridad-en-2014/84996

23. http://www.elfinanciero.com.mx/sponsor/como-funciona-la-economia-de-los-hackers.html

24. http://eleconomista.com.mx/infografias/ciberataques/2015/04/10/infografilia-tecno-ataque-cibernetico-tv5monde

25. http://eleconomista.com.mx/tecnociencia/2015/04/28/amenazas-ciberneticas-mundo-digital-fisico

26. http://eleconomista.com.mx/industrias/2014/06/03/crimenes-ciberneticos-viven-su-auge-mexico

27. http://eleconomista.com.mx/tecnociencia/2014/06/11/ciberseguridad-buenos-estamos-perdiendo-hp

28. http://eleconomista.com.mx/tecnociencia/2015/02/09/amenazas-ciberseguridad-modifican-estrategias-proteccion

29. http://eleconomista.com.mx/tecnociencia/2015/04/29/mexico-blanco-top-ciberataques

30. http://eleconomista.com.mx/tecnociencia/2015/04/24/kaspersky-hara-investigacion-forense-digital-mexico

31. http://eleconomista.com.mx/tecnociencia/2014/06/03/empresas-piensan-medias-seguridad-digital

32. http://eleconomista.com.mx/tecnociencia/2015/07/05/organizaciones-cuentan-bajos-niveles-seguridad-emc

33. http://eleconomista.com.mx/tecnociencia/2014/04/20/mexico-sufre-12-ataques-ciberneticos-cada-segundo-0

34. http://www.infosec.gov.hk/english/technical/guidelines.html

35. http://administracionelectronica.gob.es/pae_Home/pae_OBSAE/pae_Informes.html

36. https://www.securityforum.org

37. http://www.iso.org/iso/iso-survey

38. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

39. http://www.seguridad.unam.mx/index.html

40. http://expansion.mx/tecnologia/2015/09/22/pymes-pagan-38000-dolares-para-salir-de-hackeos

41. http://revista.seguridad.unam.mx/numero23/tic-internet-y-ciberterrorismo

42. http://www.elfinanciero.com.mx/tech/mexico-esta-rezagado-en-tics-critica-amiti.html

43. https://www.us-cert.gov

44. http://www.itu.int/es/pages/default.aspx

45. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

46. http://www.inegi.org.mx/est/contenidos/proyectos/encuestas/establecimientos/otras/entic/default.aspx

47. http://amiti.org.mx/dir-empresas?letra=

48. https://www.fbi.gov/about-us/investigate/cyber

49. http://www.iso27000.es/sgsi_implantar.html#home

50. http://www.iso27001security.com/html/27001.html

51. http://www.ietf.org/

52. http://www.first.org/

53. http://asi-mexico.org/sitio/