INSTITUTO POLITÉCNICO NACIONAL

UNIDAD PROFESIONAL INTERDISCIPLINARIA
DE INGENIERÍA Y CIENCIAS SOCIALES
Y ADMINISTRATIVAS

PROPUESTA DE BASELINE DE SEGURIDAD INFORMÁTICA CON BASE EN MEJORES PRÁCTICAS PARA ÁREAS INFORMÁTICAS DE EMPRESAS DE RECIENTE CREACIÓN

T E S I N A

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN CIENCIAS DE LA INFORMÁTICA

P R E S E N T A N
OMAR CUITLÁHUAC FARFÁN CHÁVEZ
JOSÉ EDUARDO FRANCO LUNA
HUGO ENRIQUE GACHUZ MONTAÑO
JORGE JIVAN HERNÁNDEZ VIQUEZ
JORGE ALBERTO LOZANO ORTEGA

CIUDAD DE MÉXICO 2017

N° de registro C.7.1698

ÍNDICE

Resumen

El procesamiento de información se ha vuelto cada vez más importante en el curso óptimo de desarrollo de las empresas, esto es debido a la velocidad con la cual se puede acceder y compartir datos entre equipos de trabajo y a la gran cantidad de medios y formatos en los que se maneja la información. Pero esto conlleva un relevante riesgo latente: la información es tan valiosa que es susceptible de perderse o robarse con facilidad.

Actualmente los incidentes relacionados a la pérdida de información son más frecuentes y de mayor impacto que en años pasados, además de que la diversificación de los incidentes complica la protección y respuesta para los responsables de los datos. Sin embargo, mientras son un riesgo considerable los agentes externos, la gran mayoría de los incidentes que sufren las empresas se deben al personal mal capacitado o pobremente preparado.

El objetivo de este trabajo es el de proporcionar un documento de referencia basado en buenas prácticas y estándares de seguridad informática para empresas que recientemente se formaron y cuyos recursos son escasos, además de una propuesta de evaluación de personal para su aplicación en conjunto.

Introducción

Hoy en día es común tener acceso a grandes cantidades de información, ya sea personal o proveniente de nuestro ambiente laboral; esto también refleja la importancia que tiene la información que generamos diariamente; para las empresas es aún más importante, ya que se puede tener acceso a ella en casi cualquier momento para la toma de decisiones.

Al ser de vital importancia el manejo de la información para la toma de decisiones se requiere que las empresas tengan medidas de protección para su resguardo, así como de personal capacitado para aplicar y dar mantenimiento a dichas medidas. Es común escuchar sobre hackeos a sistemas de información en todo tipo de empresas, donde información de sus actividades, contraseñas, información del personal, y hasta cuantas bancarias están implicadas.

Estos ataques obviamente son un golpe duro no solo a las actividades de la empresa de forma interna para sus actividades, sino también un golpe duro para su prestigio ante sus clientes actuales y futuros. Al pensar en esto lo primero que viene a la mente son empresas grandes con robustos sistemas, los que son más propensos a una serie de ataques donde la información que resguardan son el objetivo, sin embargo es común que cualquiera sea blanco del robo de información inclusive las empresas o negocios pequeños.

Las empresas pequeñas recientemente creadas, no tienen acceso a recursos como sistemas extremadamente robustos y mucho menos el personal necesario para manejarlos, pero eso no implica que están exentos de procedimientos para manejar y resguardar la información que manejan , no solo para la configuración delos equipos que usen , sino también para el personal que interactúa con ella, ya que muchos de los problemas de fuga de información, son originados por el mismo personal por desconocimiento o mala capacitación de los procedimientos para manejar información.

El objetivo de este trabajo es presentar a este tipo de empresas, una guía con los procedimientos básicos mínimos que pueden seguir los empleados responsables de manejar y resguardar la información en la empresa, que les permita generar una primer base de conocimientos ante posibles amenazas, misma que pueda servir como referencia para mejorar sus procesos al manejar la seguridad de su información.

Capítulo I Marco metodológico.

1.1 Planteamiento del problema.

La protección de la información es actualmente el tema de mayor relevancia para las empresas debido a lo rápido que cambian las Tecnologías de la Información y la Comunicación (TICs; recursos y herramientas utilizados para procesar, administrar y compartir datos mediante soportes tecnológicos); por este motivo es imperativo mantenerse actualizado en cuanto al desarrollo e implementación de dedicadas a la protección de datos.

Mientras se siguen desarrollando nuevas herramientas y procedimientos informáticos, es vital que su uso también evolucione para poder responder eficazmente a las nuevas amenazas que surgen: cibercriminales (hackers), software malicioso (malware), extorsión digital (ransomware), suplantación de identidad (phishing), etc.

Esto propicia que surjan diversas preguntas: ¿son las empresas consientes de los riesgos de pueden afectar a sus datos?, ¿dedican los recursos suficientes para implementar soluciones de seguridad informática?, ¿los empleados de las empresas están capacitados para atender incidentes de seguridad?, etc.

En México, las TICs han demostrado ser uno de los sectores de mayor crecimiento para la economía nacional, considerando tanto las áreas funcionales de las empresas, así como a las empresas especializadas en el ramo. En el 2015 esta industria sumó un crecimiento del 5% anual, equivalente a $60,000 millones de dólares, según datos presentados el 2015 por la Asociación Mexicana de la Industria de Tecnologías de Información, A.C. (AMITI).

Desafortunadamente, en el país no se ha fomentado correctamente el tener procesos de seguridad informática en la organización.

Según un informe de 2016 por International Data Corporation (IDC; empresa dedicada a investigación, análisis y consultoría de mercados) durante el 2015 sólo el 28% de las empresas mexicanas incrementaron su gasto anual en TICs mientras que el 49% lo mantuvieron y desafortunadamente el 23% lo disminuyeron.

Cambio en el Gasto para TICs en México el 2016

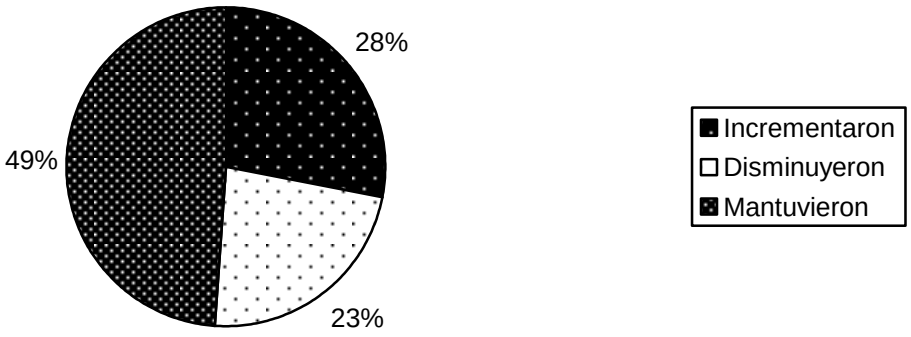

Ilustración 1

Lo anterior expone porque en el país se le está dando mayor importancia a la inversión en TICs, sin embargo, la seguridad informática no ha recibido el mismo ímpetu por las empresas ya que sólo le destinan el 1% de sus presupuestos, de acuerdo con Jerónimo Piña (gerente de investigación de IDC) en el foro de seguridad Next-Gen Security 2016.

En la Convención Nacional de la Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías (2016) Víctor Lagunes, jefe de la Unidad de Innovación y Estrategia Tecnológica de la Presidencia de la República, dijo que México pierde 3,000 millones de dólares por ciberdelitos al año. Además, se considera que, según estadísticas del 2016 de la Comisión Nacional de Seguridad, ocurrieron más de 81,000 incidentes informáticos de los cuales el 57% se relacionan con malware y el 14% con el fraude cibernético.

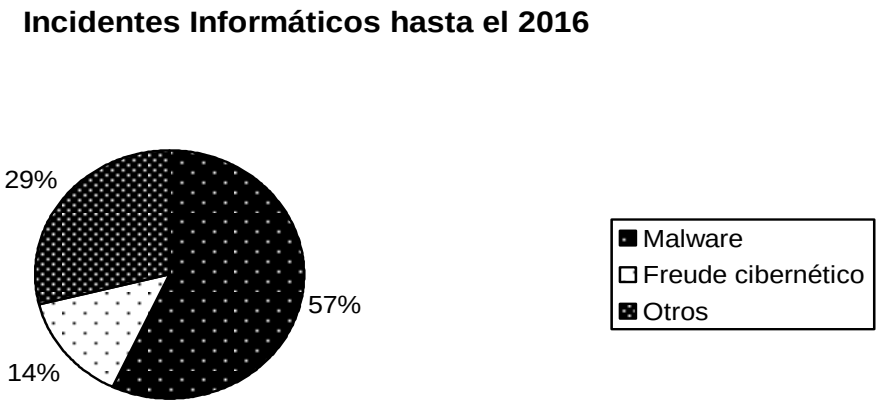

Ilustración 2

Por lo otro lado, existe la amenaza interna de ciberseguridad ya sea por una acción con dolo o por una falta de capacitación de los empleados de la organización. De acuerdo a un estudio del 2015 realizado por la empresa especializada en software de seguridad Symantec, el 10% de los incidentes de seguridad fue relacionado a robo interno, mientras que un 22% correspondió publicaciones o divulgaciones accidentales.

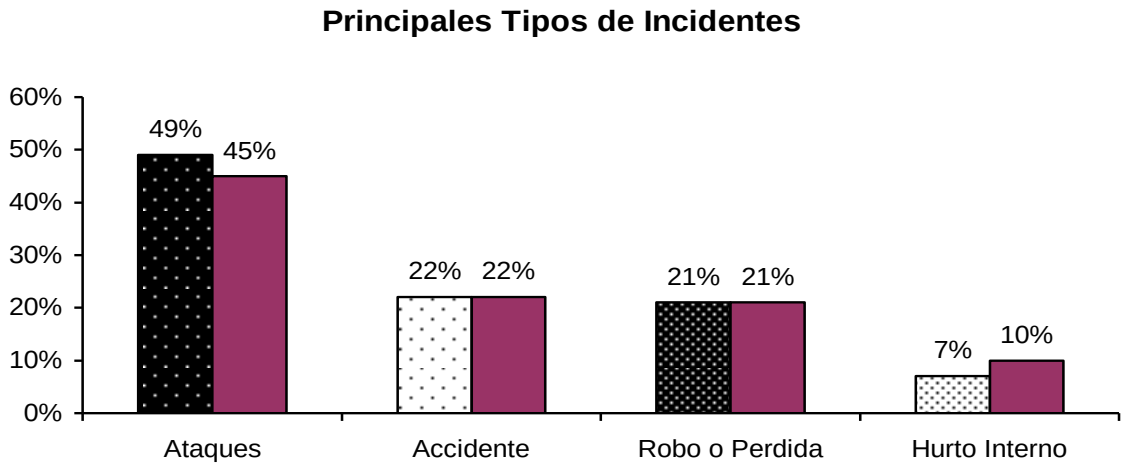

Ilustración 3

Los incidentes de seguridad informática generan pérdidas monetarias y materiales, además de daño en la reputación de las empresas. Una encuesta de riesgo reputacional realizada por Deloitte en 2014 reflejó que las empresas consideran 3 los principales factores de riesgo reputacional: productos o servicios con 43%, integridad y ética con 55% y seguridad con 45%.

Asimismo, este estudio indica que las empresas consideran a sus empleados como un aspecto preponderante de afectación a la seguridad, lo que fortalece considerar a la falta de educación básica en seguridad informática como problemática.

Por este motivo han surgido programas que ofrecen actualización y especialización en estrategias que buscan agilizar la transición hacia un ciberespacio seguro en el que sea posible aprovechar al máximo los beneficios que generan los nuevos procesos de la información.

Según un reporte del 2015 de Ernst & Young (firma multinacional de servicios de aseguramiento, consultoría y asesoramiento), en México el 19% de las empresas tienen programas de seguridad informática, contra 40% a nivel global.

De acuerdo al 2016 Cost of Data Breach Study del Instituto Ponemon, la determinación de costos de los incidentes es un análisis basado en actividades y su asignación de costo por uso. Según esta metodología, las actividades típicas a realizar al descubrir y dar atención son:

- Conducir una investigación y análisis forense para descubrir las causas.
- Determinar las posibles víctimas.
- Organizar un equipo de repuesta.
- Acatar actividades de relaciones públicas.
- Preparación de documentación de avisos a los usuarios sobre la situación.

1.1.1 Problema.

Los datos sensibles y críticos de las empresas enfrentan muchos riesgos debido a que éstas centran sus políticas y recursos en otras áreas de interés y no en las amenazas externas e internas que enfrentan contra su información y sus equipos computacionales.

La cultura laboral, en especial el comportamiento de los empleados, constituye el eslabón más débil de la cadena de seguridad de la información, convirtiéndose en una creciente fuente de riesgos originados más por el desconocimiento y la falta de cuidado que por la malicia; ellos esperan que los mecanismos de seguridad implementados por la organización se ocupen de todo y no son reflexivos del verdadero peligro y naturaleza de las amenazas.

Un creciente número de empleados cree que las políticas de seguridad frenan la innovación y la colaboración, complicando el correcto desempeño de sus tareas y, como consecuencia, estos

deciden ignorar dichas políticas. Los trabajadores no identifican este comportamiento como una amenaza a la seguridad de la información.

Falta de conciencia y desconocimiento.

La mayor amenaza interna es consecuencia de la relajación de la cultura laboral: mientras algunos empleados responsabilizan sólo a la empresa de proteger la información, otros se sienten ajenos al alcance de las amenazas, en general piensan que su comportamiento tiene un impacto de mínimo en la seguridad.

Las políticas de seguridad tampoco tienen el rigor o la implementación necesarios, dejando a la organización casi igual de vulnerable que sin ellas; lo peor de esta situación es cuando los empleados no saben si existen.

Es así como el equilibrio entre la facilidad de operación y la protección requiere de acercamientos especiales, adaptables a las necesidades y al comportamiento de los usuarios, enfocándose tanto en las amenazas como en la simplicidad a la hora de gestionar las soluciones implantadas.

Los responsables de las áreas de informática requieren generar políticas y procedimientos de seguridad cada vez más centrados en el perfil de los usuarios, para tratar de evitar la pérdida de datos y sus costosas consecuencias.

1.2 Objetivo general.

Crear un baseline de seguridad informática para las áreas de TICs de empresas de reciente formación y la aplicación de buenas prácticas informáticas.

1.3 Objetivos específicos.

- Analizar cuáles son las normas y buenas prácticas de seguridad informática mínimas recomendables.
- Analizar la situación actual en seguridad informática para empresas de reciente formación.
- Redactar el baseline que propicie beneficios en seguridad informática con un conjunto de controles mínimos requeridos.
- Generar un prototipo de campaña de difusión que complemente la óptima implementación del baseline en áreas de TICs.

1.4 Justificación.

Tradicionalmente se consideraba que las empresas cuentan con 3 tipos de recursos: los humanos, los materiales y los financieros. Pero actualmente la información que se maneja toma cada vez mayor importancia y valor para el óptimo funcionamiento de la organización, desde sus actividades diarias hasta sus relaciones sociales y comerciales.

Para que la información sea de utilidad debe de ser confiable, íntegra y accesible; por éste motivo la organización está obligada a invertir en su protección para disminuir las vulnerabilidades presentes en su gestión.

Debido a que las TICs se actualizan de manera constante es fácil pasar por alto el ámbito de la seguridad informática por desconocimiento o por malas prácticas, y con la creciente tendencia de mudar las interacciones humanas a Internet el problema aumenta de forma exponencial.

En México, la inversión en materia de seguridad informática es mínima aun cuando después de un incidente sus pérdidas son mucho mayores en sus distintos tipos de recursos. Esto deja ver que la necesidad de implantar y mejorar la seguridad de la información de las empresas, involucrando a los empleados con especial interés.

Esta investigación será renovable ya que lo desarrollado en este caso de estudio en particular servirá como base para iniciar nuevos proyectos de seguridad o para mejorar los ya establecidos.

La Licenciatura en Ciencias de la Informática permite realizar una evaluación del estado de seguridad de los sistemas informáticos, en base a estándares y buenas prácticas en relación a la seguridad informática.

1.5 Hipótesis.

- Las empresas en México no tienen una cultura en seguridad informática.
- Las empresas no son conscientes de los procesos informáticos más vulnerables que envuelven a su operación.

En base a la investigación que se realizará, se disminuirán significativamente los riesgos informáticos de los datos de la organización.

1.5.1 Pregunta de Investigación

- ¿Por qué las empresas son vulnerables en el ámbito de la seguridad informática?

Capítulo II Tendencias de seguridad informática en México.

2.1 Importancia de la seguridad informática en las empresas.

La seguridad informática es un tema relevante en un mundo donde la tecnología forma parte importante de la vida cotidiana de las personas y tanto en su uso personal como en el empresarial existe el riesgo de sufrir ciberataques, extorsión, robo de identidad y demás delitos. Cuando se habla de las empresas evidentemente se multiplican el volumen y el tipo de información que se maneja, incrementando también la intensidad y la diversidad de los riesgos debido a las vulnerabilidades de los sistemas utilizados.

En el libro *Informática y comunicaciones de la empresa,* Carmen de Pablos describe su importancia como: “La creciente dependencia de las empresas, y de la sociedad en general, de las *TICs*, así como el entorno cada vez más complejo en que estas se desarrollan, ha provocado la aparición de vulnerabilidades en los recursos utilizados que las empresas deben minimizar con las medidas de seguridad oportunas”.

Son muchos los riesgos y los ataques a los que una empresa debe que hacer frente: ingresos no autorizados a los sistemas de información, fisgones y piratas informáticos, robo, destrucción o daños a los datos, correo basura o no solicitado, ocupación indebida de direcciones; desvío de información o espionaje industrial; virus o malware.

La redacción de este libro data del año 2004 y se puede observar que desde entonces el tema ya era muy importante para las empresas, haciendo especial énfasis en los virus informáticos, los cuales se encontraban en apogeo y para las empresas era fundamental el protegerse de ellos con software dedicado y campañas de mejora de sus procesos.

Las empresas desarrolladoras de antivirus *ESET* y *Kaspersky* realizaron en conjunto en el 2014 la encuesta *Allianz risk barometer on business risk* en la que se expone que los ciberataques están entre los 10 primeros lugares dentro de los riesgos que enfrentan las empresas a nivel global:

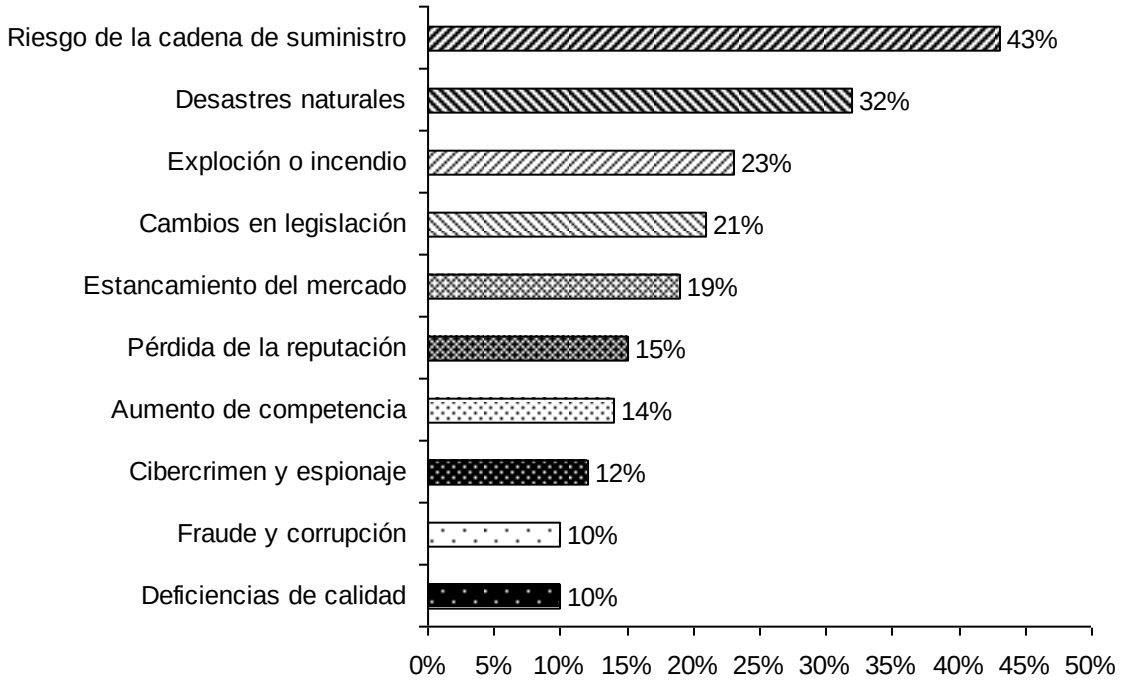

Ilustración 4

2.1.1 Ataques destacados.

La siguiente tabla muestra ejemplos, por cada mes del año 2016, de los ciberataques más representativos a nivel mundial, entre los que se observan diferentes tipos de empresas, diferentes formas de ataque y múltiples maneras en que los usuarios de dichas empresas fueron afectados.

Esto muestra un panorama en el cual los incidentes informáticos no son fácilmente anticipados, mucho menos sus resultados, dando pie a que la mejor forma que tiene una empresa de protegerse es la prevención en forma de capacitación y de concientización.

Empresa	Fecha	Descripción
	Enero	*ESET* advierte a los usuarios de *WhatsApp* que no hagan clic en un correo electrónico que simula ser de *WhatsApp* pero que infecta con un troyano. *ESET* recomienda precaución ya que pueden exponer a ransomware, que bloquea archivos y exige rescate monetario por ellos.

	*BTCC*, el mercado de divisas digital basado en *Shanghai*, China, sufrió un ataque distribuido de denegación de servicio (*DDoS*). El ataque obstaculizó el acceso de *BTCC* a sus APIs y a otros servicios durante un período lo cual evito el acceso de los usuarios a sus cuentas.
Febrero	
	Miles de enlaces con supuestos videos exclusivos de la aerolínea que contenían malware.
Marzo	
	Agujero de seguridad encontrado en OpenSSL (proyecto de software libre), unos 200.000 sistemas siguen siendo susceptibles a Heartbleed más de dos años después de que se revelara la vulnerabilidad.
Abril	
	Ataque que comprometió bases de datos con contraseñas privadas de los clientes. Los hackers siguen explotando las vulnerabilidades XSS almacenadas en eBay en 2014.
Mayo	
	Diversos engaños y amenazas contra los usuarios de internet del portal del organismo.
Junio	
	Fallo que permitía acceder a cuentas de usuarios. El problema se debió a una vulnerabilidad de falsificación de solicitudes cruzadas (CSRF) que existía en PayPal.me, un sitio que la compañía lanzó el 2015 para permitir a sus usuarios solicitar dinero.
Julio	
	Un atacante infiltró un repositorio utilizado para registrar errores relacionados con el navegador Firefox y robó información relacionada a vulnerabilidades sin parches en productos de Mozilla.
Agosto	
	Desde el 2014, colecciones de fotografías privadas de varias celebridades fueron difundidas en sitios web y redes sociales. El acceso ilegal fue ganado vía ataques phishing apuntados a usuarios de iCloud.
Septiembre	

	Octubre	Vulnerabilidad descubierta en el protocolo de comunicación SSL v3.0. La vulnerabilidad se utiliza como parte del marco de seguridad utilizado para el cifrado a través de Internet.
	Noviembre	Amenazas de malware, infectar sistemas y robar información en equipos Windows no actualizados apropiadamente.
	Diciembre	Fuga de información sensible y filtración de películas sin estrenar de los estudios Sony.

Tabla 1 – Listado de ataques destacados.

Ubicándonos en México como ambiente local de esta investigación se toma como ejemplo destacado el reportado por el periódico *El Financiero*, en el cual menciona que la empresa *Liverpool* el 2016 tuvo pérdidas debido a un ciberataque, entre daños a sus clientes y eventuales multas, de al menos $88.5 millones de pesos, tomando en cuenta los ingresos de la compañía.

Asimismo, dicho ataque, calificado de bajo riesgo por la compañía ante la *Bolsa Mexicana de Valores* (BMV), podría tener consecuencias de otra índole, incluso jurídicas, debido a la cantidad de datos filtrados por el grupo criminal *SicKillers,* entre los que se encuentran datos de los clientes, por lo que habrían violado la *Ley Federal de Protección de Datos Personales*.

De acuerdo con el *H. Congreso de la Unión*, las multas por violar dicha ley pueden ascender a $18 millones de pesos y tener consecuencias civiles y penales. A pesar de que no se detalla cuántos registros fueron robados, los datos de las víctimas pueden estar expuestos en foros, blogs y sitios web; entre los datos que podrían estar incluidos figuran los números telefónicos, los *RFCs*, las direcciones y las cuentas de crédito de la empresa.

Por su parte, los clientes afectados podrían ser víctimas de suplantación de identidad, robo a las cuentas bancarias publicadas, acoso e incluso extorsión, por la naturaleza de los datos que son ahora públicos y que en otros incidentes registrados

En 2014 según información de *Kaspersky Lab,* el número de ciberataques contra empresas y corporaciones de 55 países fue de aproximadamente 4 mil 400, mientras que en el 2013 estos sólo llegaban a los mil 800. En tanto que, en México, 100 mil PyMES sufrieron este tipo de ataques, de acuerdo con estimaciones de *Trend Micro* en México, ya en 2013, en todo el país las pérdidas provocadas por ciberdelincuentes ascendieron a $39,000 millones de pesos.

Los ataques más comunes fueron dirigidos a los bancos y a sus usuarios, gracias al auge de la banca en línea, cuyos incidentes de robo de dinero sumaron 2 millones de casos el 2014.

2.2 Riesgos de seguridad informática.

En la actualidad, la gran mayoría de las actividades cotidianas que las personas realizan se puede encontrar la intervención de la tecnología; desde consultar el estado del tiempo hasta el manejo de las cuentas de ahorro bancarias. Esta nueva forma de hacer de las cosas no solo parece que se ha incorporado en la vida del ser humano, si no que la tendencia del desarrollo acelerado de las nuevas tecnologías indica que cada vez más irá en aumento.

Este mismo esquema puede ser traducido a nivel de una organización mediante el uso de TICs para la gestión de sus actividades y no solo limitándose a las funciones operativas y financieras, si no a casi el total de las tareas en una empresa, principalmente al manejo de información que le permite poner en marcha sus actividades productivas.

Todas las cosas que existen ya sean derivadas de una invención o propias de la naturaleza, son perfectibles y las de TI no son la excepción, si bien su principal propósito es el de brindar un factor de beneficio también son acreedoras a tener vulnerabilidades o debilidades ante posibles eventos internos o externos a su uso.

Un riesgo de seguridad de la información se define como: “Potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupos de activos, causando así daños a la organización”. El mencionar este concepto implica incluir la definición de dos términos que faciliten la comprensión de riesgo:

1. Amenaza: Se refiere a una situación que puede desencadenar en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información.
2. Vulnerabilidad: Es referente a la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información.

La clasificación de riesgos dentro de las *TICs* puede representar distintos niveles o conceptos dependiendo de los puntos vista de cada organización o individuo y la importancia estos les asignen en el ambiente en el que desempeña la organización evaluada. De forma general se pueden destacar los siguientes términos:

- **Riesgo de negocio**: se refiere a una circunstancia o factor que puede tener un impacto negativo o positivo sobre el funcionamiento o la rentabilidad de una empresa determinada.
- **Riesgo inherente**: es el tipo de riesgo presente por la actividad económica o giro empresarial del negocio.
- **Riesgo operativo**: es el riesgo derivado de posibles fallas en los sistemas de administración, procedimientos internos e incluyendo errores humanos, ya sean intencionales o no.
- **Riesgo financiero**: es la posibilidad de pérdida relacionada con las operaciones financieras que puedan afectar los estados financieros de la empresa.

Sin lugar a dudas, estos deberían de ser los puntos más relevantes para las empresas hoy en día. Tal es el caso que, de acuerdo a un artículo publicado por *Forbes México* en abril de 2015, un fraude relacionado con información de clientes puede implicar una pérdida promedio de $2.6 millones de dólares para las empresas en este país. Asimismo, la situación se agrava tomando en cuenta que el 66% de las PyMEs mexicanas consideran que no se encuentran expuestas a una estafa de este tipo, siendo que de acuerdo al *Instituto Nacional de Estadística y Geografía* (INEGI), en 2016 este tipo de empresas representan a más del 95% del total de compañías del país.

Asimismo, un estudio de la empresa especializada en seguros *AIG* reveló que el 87% de las firmas carece de un protocolo de protección de datos. Estas cifras demuestran la problemática actual de las empresas en cuanto a administración de riesgos de tecnología y seguridad de la información.

Existen diversos estándares y buenas prácticas enfocadas en la administración y control de incidentes de seguridad de la información, cada uno orientado a diversas vertientes de protección dependiendo del giro que le imprime cada organismo rector. Estas normativas permiten identificar, clasificar y gestionar incidentes en TI pero para poder implementarlos es necesario un enfoque sistemático de análisis que permita primeramente identificar las necesidades del negocio y sus componentes vitales de operación para posteriormente desarrollar un *Sistema de Gestión de la Seguridad de la Información* (SGSI).

Asimismo, el manejo de este SGSI se debe establecer como parte integral de las actividades de una empresa desde que éste se forma hasta su operación continua futura, sin importar la cantidad

de recursos o de personal que pueda invertir la organización; lo ideal es que la seguridad esté siempre presente para que la información sea protegida más de forma proactiva que reactiva.

El SGSI consiste principalmente en la identificación y el análisis lo que puede suceder a la información y quién lo puede materializar (*amenaza*) y cuáles son las posibles consecuencias que estos provocan (*impacto*), para posteriormente establecer las acciones a realizar dentro de un periodo acordado con el objetivo de r esponder (*mitigar*) al riesgo hasta niveles aceptables.

Esto va de la mano con establecer posteriormente una etapa de seguimiento o monitoreo del tratamiento que se realizó para medir la eficacia de los planes de acción implementados y, en caso de ser necesario, se apliquen acciones correctivas que mejoren paulatinamente la seguridad. De igual manera, es indispensable capacitar a todo el personal involucrado acerca de los incidentes y de las acciones tomadas sobre estos, desde aquellos en la alta dirección hasta el área operativa.

Este procedimiento puede ser aplicado a la organización completa, a determinadas áreas o a ciertos sistemas; un SGSI, así como cualquier proceso de gestión de riesgos, se componen de ciertas etapas que no pueden ser ignoradas, como son el establecimiento del contexto, la evaluación de la seguridad, el tratamiento de los incidentes, la aceptación de los resultados, la comunicación de los objetivos, el monitoreo del proceso y revisión del mismo.

Cabe señalar que para poder iniciar la implementación de un SGSI se deben de desarrollar ciertos criterios para lograr evaluar correctamente la situación, estos pueden ser: el valor estratégico de la información, el nivel crítico de los activos, los requisitos legales y reglamentarios que operan sobre la organización, las obligaciones contractuales (entre empresas, individuos y gobiernos), la importancia de la confidencialidad, integridad y disponibilidad de la información para las operaciones, y las consecuencias sobre la reputación de los involucrados.

De igual manera, se cuenta con ciertos factores para medir el nivel del impacto como son: clasificación de los activos, brechas de seguridad de la información, posibles operaciones afectadas, alteración de planes y fechas límites, daños a la reputación. Asimismo, es de suma importancia establecer puntos de aceptación de riesgos como son: definición de umbrales con una meta definida, relación costo-beneficio, niveles de cumplimiento contractual o legal y compromiso de aplicación de acciones futuras con fechas compromiso.

Por otro lado, es importante mencionar los principales riesgos de seguridad de la información a los que se enfrentan las empresas en la actualidad. Si bien, la definición y el tratamiento de los riesgos dependen de los recursos y criterios propios de cada organización, existen ciertas amenazas comunes que se presentan en cualquier empresa sin importar el negocio o industria. Una encuesta

global sobre seguridad de la información realizada en 2015 por la firma *Ernest & Young* reflejó que las empresas identifican dos principales vulnerabilidades: los empleados descuidados o inconscientes y la arquitectura o controles obsoletos.

En cuanto a la actualidad de las empresas de México, una firma de consultoría dedicada a la auditoría de sistemas de TI concluyó que aproximadamente en un 90% de las compañías evaluadas en el año fiscal 2016 se presentaron deficiencias en controles de TI relacionados a riesgos de seguridad de accesos, cambios o modificaciones en programas críticos en los sistemas y en configuraciones de seguridad robustas en los mismos.

Específicamente, las áreas de oportunidad identificadas corresponden a controles de accesos lógicos en los sistemas críticos de las compañías que alojan información financiera relevante, principalmente en el aprovisionamiento de usuarios, como cuentas no removidas o deshabilitadas oportunamente de empleados que concluyeron su relación laboral con la compañía, de las cuales aproximadamente en un 10% se identificó actividad posterior en los aplicativos, lo que nos indica una materialización del riesgo.

Asimismo, otra observación relevante es el tema de la segregación de funciones, lo cual se origina en el contar con usuarios con accesos adicionales a los requeridos para ejecutar sus actividades, es decir, existen cuentas en los sistemas con permisos que pueden ocasionar conflictos en las actividades críticas.

Esta problemática puede ser originada de varios factores, como desconocimiento de los administradores de los sistemas de este tipo de conflictos, una configuración inicial no adecuada al momento de implementar el sistema falta de cocimiento técnico o competencia para ejecutar la depuración de estos conflictos, falta de personal para monitorear las acciones, entre otras.

Continuando con el tema de seguridad en accesos, la ausencia de una revisión periódica de los usuarios y permisos existentes en los sistemas y en su infraestructura es otro factor que afecta los dos puntos previamente mencionados; lo que nos indica que no solo se cuenta con el riesgo de contar con accesos no autorizados, si no que no se aplican acciones correctivas o se evalúan de forma adecuada los riesgos.

Como se mencionó previamente, el área de control es otro factor importante, ya que la tendencia manifestó que no se cuenta con una segregación entre el personal de desarrollo de sistemas, quien implementa los cambios en el ambiente productivo y en muchas ocasiones también en el responsable de autorizar estas modificaciones, permitiendo la aplicación de desarrollos no

autorizados o no adecuados directamente en los programas relacionados con información relevante para la alta dirección.

Otro hecho se debe a contar con equipos obsoletos o no actualizados con los últimos parches de seguridad liberados por el proveedor. El principal factor se debe a que la administración tiene la preferencia de no contar con una posible afectación en la operación del sistema derivada de la aplicación de estos parches; sin embargo, esto crea la brecha de aumentar la vulnerabilidad de los aplicativos dado que cada día surgen nuevas amenazas de posibles intentos de ciberataques, o aplicación de algún tipo de malware.

Finalmente, una problemática adicional existe en la transferencia de riesgos a terceros. Si bien existe cierto acuerdo contractual y niveles de servicio y responsabilidades, no se cuenta con un monitoreo o aseguramiento por parte de la compañía hacia las actividades que ejecuta el proveedor sobre la configuración de sus sistemas relevantes.

La incorporación de nuevos métodos y dispositivos tecnológicos nace en conjunto con el problema de las vulnerabilidades y debilidades que alguien está dispuesto a identificar, detonar y aprovechar para beneficio propio, aunque esto implique desarrollar acciones con dolo a los dueños de la información o a terceros.

2.3 Impacto de la inseguridad informática.

Aunado a la lamentable situación de inseguridad que guarda nuestro país, debe sumarse en términos productivos que las amenazas informáticas y la falta de previsión en las empresas merman la expansión de las actividades de las *PyMEs*, tanto geográficamente como en la mejora en los servicios a sus clientes.

Gilberto Vicente, Responsable de Canales de *McAfee* México, explicó que de acuerdo a estudios internos y externos de la firma que representa, la seguridad de la información debe ser una prioridad de las *PyMEs* que usan *TICs*, que en estos tiempos casi todas los hacen debido a que los datos que guardan son de carácter esencial para el negocio, tales como facturas, clientes e inventarios entre otros; pero dicha prioridad va acompañada del conocimiento de amenazas, las cuales limitan el crecimiento de los negocios.

Los grandes inhibidores del crecimiento son expuestos por las caídas de los servicios debido a la cibercriminalidad, a lo cual Felipe Canale, responsable de socios de negocio de *McAfee*

Latinoamérica atribuye a que las *PyMEs* no cuentan con un departamento o experto en tecnología, lo cual implica una vulnerabilidad o limitante a la hora de responder a los incidentes.

Por ejemplo, las empresas que piensan expandir sus operaciones de forma territorial mediante oficinas regionales, una fuerza de ventas o también aquellas que lanzarán una serie de productos para sus clientes, lo pueden hacer de manera segura a través de soluciones informáticas en términos de movilidad y modernización.

Con anterioridad, cuando una empresa apostaba por tecnificarse, el factor seguridad era el último elemento de la cadena, hoy toda empresa debe recurrir a ofertas integrales de seguridad, las cuales deben contar con costos accesibles y que sean compatibles, además de considerar elementos de red, nube y estación de trabajo, de acuerdo con Gilberto Vicente.

2.3.1 Índice de ciberseguridad en México.

En 2016 en México se registraron 65.5 millones de usuarios de internet, los cuales representaron alrededor de 60% de la población mexicana y un crecimiento de 5% respecto al año anterior. Por otro lado, 47% de los hogares de los 15.7 millones cuentan con conexión a internet, mientras que el año anterior este indicador era del 39.2%.

México cuenta con herramientas cuyo objetivo consiste en prevenir y combatir las ciberamenzas y los incidentes informáticos; una de ellas es la colaboración internacionalmente en seguridad a través del *Equipo de Respuesta a Incidentes de Seguridad Cibernética* (CERT-MX) el cual prepara al país contra cibertataques relacionados con infraestructura crítica y gestiona respuestas ante estos ataques, además de que la *Policía Federal* cuenta con la *División Científica* de la cual deriva la *Unidad Especializada para la Atención de Delitos Cibernéticos* que atiende solicitudes de apoyo a este tipo de delitos.

La *Unión Internacional de Telecomunicaciones* (UIT) publicó el *Índice de Ciberseguridad Global* (ICG) 2017 que mide el grado de compromiso de 193 estados en torno a la ciberseguridad; en este indicador se le otorgó a México la calificación de 0.66, colocándolo en la posición 28 entre países como Bélgica (0.671) y Uruguay (0.647).

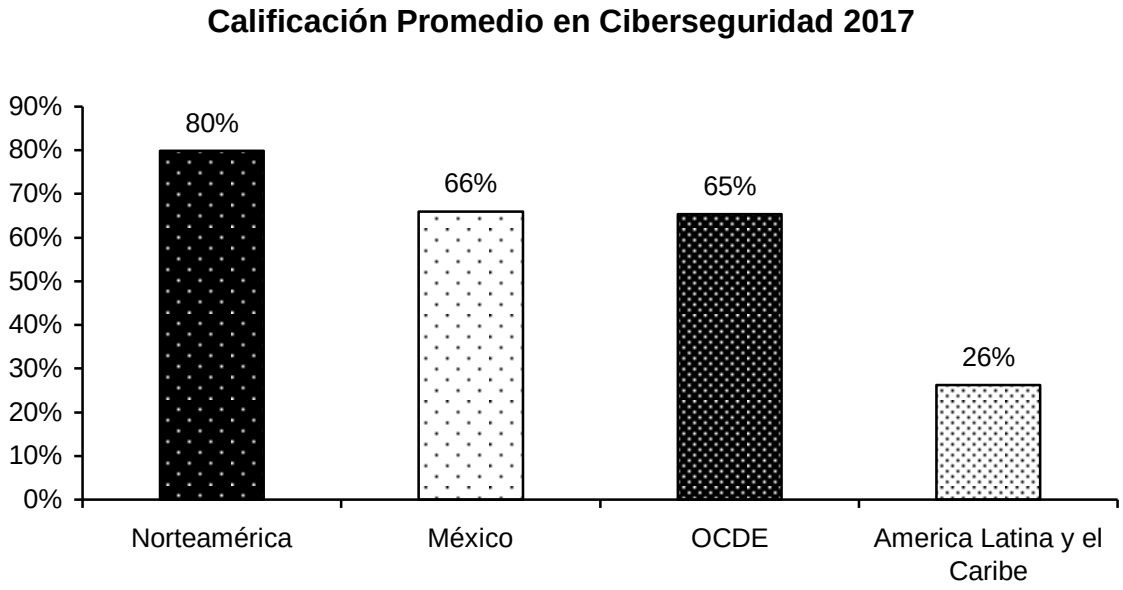

Ilustración 5

Sin embargo, el ICG ubicó a México en el primer lugar entre los países de América Latina y el Caribe y en el tercer lugar en Norteamérica, muy por debajo de Estados Unidos (0.91) y Canadá (0.81). Lo que resulta alentador en respuesta a los esfuerzos por mejorar la seguridad informática en el país, es que el resultado es muy similar al promedio de los países de la *Organización para la Cooperación y el Desarrollo Económicos* (OCDE) el cual es 0.65.

El índice se compone de 25 indicadores integrados en 5 pilares, los cuales ayudan a medir tanto las fortalezas como las debilidades de los estados en cuanto a su compromiso con la seguridad informática. Estos cinco pilares se encuentran representados en la gráfica siguiente acompañado de sus respectivas evaluaciones.

En este sentido, México muestra fortalezas en las medidas legales donde ya se registran instituciones y marcos legales destinados a combatir el cibercrimen en sus diferentes variantes, proteger la privacidad de los datos personales y las transacciones electrónicas entre individuos y entre empresas. Asimismo, se muestran resultados positivos en cuanto al pilar técnico, al contar con instituciones técnicas dedicadas a la ciberseguridad.

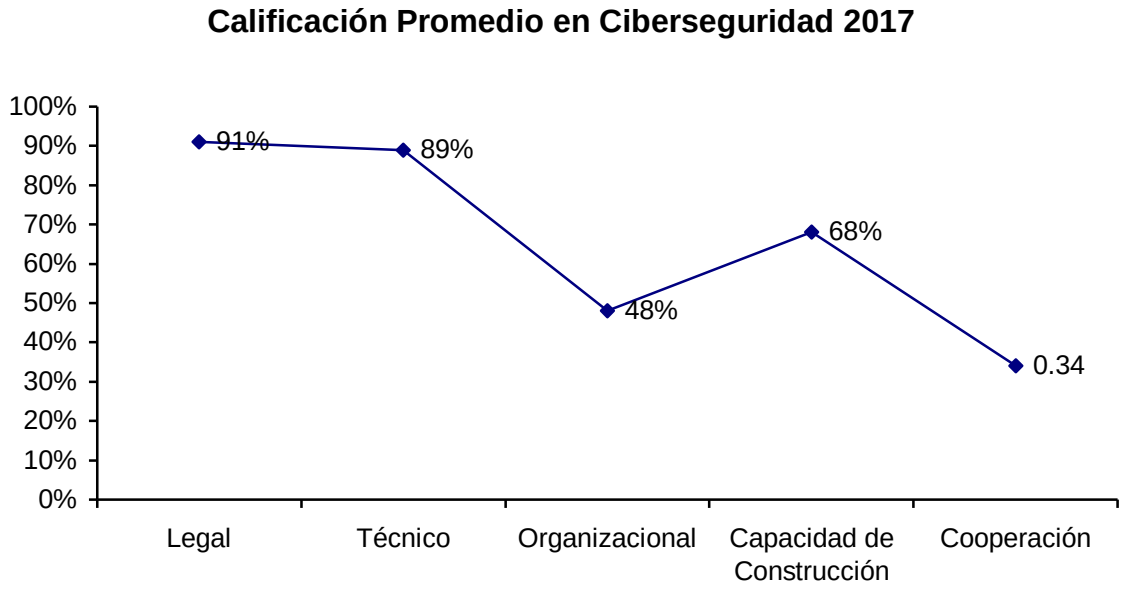

Ilustración 6

También es importante señalar que el resultado de las medidas organizacionales responde a que aún se carece de una estrategia nacional competente que coordine los esfuerzos gubernamentales en torno a este tema. Finalmente, en la cooperación aún se requiere de impulso ya que queda pendiente el desarrollo de marcos colaborativos y redes de información compartida.

La poca prevención ante delitos informáticos, así como la extorsión y el robo son algunos de los problemas que impactan en las *PyMEs*, afectando directamente sus utilidades u operaciones.

“Más de 50% de las *PyMEs* en México considera que la cantidad que tiene que invertir en seguridad informática es muy elevada y no justifica el riesgo, por lo cual no ven como prioritario la protección en el área”, explicó Bernardo López, encargado del área de *Volumen Trend Micro*.

Indicó también que actualmente una pequeña empresa que quiera estar protegida con programas como antivirus, antimalware y filtrados URL, tiene que pagar en promedio $8,000 pesos mensuales; el costo puede variar dependiendo del tamaño de la empresa y de la cantidad de información además de contar con el personal capacitado para implementarlo.

Esto muestra que, aunque en el país hay un esfuerzo general por mejorar la seguridad informática, a nivel local las empresas tienen problemas para encontrar herramientas que les permitan proteger su información sin ver afectadas sus finanzas o sus operaciones.

2.3.2 Objetivo atractivo.

Según estudios realizados por firmas tecnológicas, 85% de las empresas de menor tamaño nacionales no se visualizan como un objetivo atractivo para ciberataques, lo cual las hace más vulnerables ante los criminales informáticos. En la *Encuesta 2011 sobre Preparación ante Desastres en las PyMEs* realizada por *Symantec* y aplicada a 1,840 empresas en 23 países, entre los cuales se encuentra México, se detalla que 54% de esos negocios no cuentan con un plan contra desastres en *TICs*.

"Las *PyMEs* sufren en promedio 6 irrupciones anuales por distintas causas, entre las que se encuentran paros técnicos por ciberataques, y estos incidentes afectan directamente los ingresos de las empresas", comentó Leandro Oliver, gerente de Ingeniería de *Symantec* de México.

Agregó que en promedio los costos por los periodos de inactividad ante estos desastres son de $12,500 dólares por día y de $3,000 dólares a sus clientes en el promedio nacional. El directivo detalló: "Menos del 50% de las empresas encuestadas realizan una copia de seguridad de su información todas las semanas o más seguido y sólo el 23% respalda su información diariamente".

Mario Arroyo, especialista en política criminal del *Colectivo de Análisis de la Seguridad con Democracia (Casede)*, explicó que las *PyMEs* no sólo deben de optar por medidas de protección con cámaras de seguridad también deben:

- Implementar soluciones completas que atiendan sus necesidades, que cuiden la información financiera y los datos de los clientes.
- Involucrar a los empleados para que sepan cómo protegerse cotidianamente y qué deben hacer en caso de pérdida de información.
- Realizar simulacros para definir cómo proteger la información y qué hacer ante un ciberataque o un incidente.

2.3.3 ¿Cómo protegerse ante la inseguridad informática empresarial?

Las amenazas de seguridad informática de hoy en día abarcan un amplio espectro de esquemas de ingeniería social, hackers y amenazas internas. Los criminales cibernéticos están en todas partes, creando nuevas amenazas día tras día y en todo el mundo.

Frente a esto, las compañías deberían contar con una estrategia de seguridad que difícilmente tienen. Una encuesta de IDC, realizada en 2014, arrojó que 9 de cada 10 compañías no tienen una estrategia de seguridad definida ni planes de seguridad.

Eso no es todo, si bien se considera que las empresas de mayor tamaño tienen los recursos para montar una defensa cibernética más importante, los resultados de la encuesta indican que el tamaño no es un factor determinante para alcanzar una madurez de seguridad cibernética potente y más del 70% de los encuestados informó niveles insuficientes de madurez en seguridad.

2.4 Legislación de seguridad informática en México.

2.4.1 Antecedentes.

Regulación Internacional de Internet.

El uso generalizado de Internet como una importante herramienta para la sociedad y los gobiernos ha propiciado al mejoramiento de las comunicaciones, al intercambio efectivo de información, a la comercialización de productos y servicios en mayores mercados, al acercamiento de sitios geográficos de forma virtual, a la realización de trámites gubernamentales a distancia, etc.

Esto ha llevado a la mayoría de los Estados a adoptar una postura emergente sobre este tema, el cual por su naturaleza de evolución constante ha resultado rezagado en todos los marcos jurídicos internos y que por lo tanto requiere de un tratamiento especial que tienda a establecer las reglas básicas para su tratamiento.

Lo anterior resulta imperioso al observar que a nivel internacional no existe ningún tratado dedicado particularmente a la regulación del Internet y que, por consiguiente, pueda dotar a los gobiernos de los instrumentos jurídicos necesarios para la tipificación de delitos, para establecer claramente las responsabilidades de las empresas prestadoras del servicio y los usuarios, el acceso a la información, la clase de información que circula en la Red y que sirva principalmente de guía a los Estados sobre cómo manejar el Internet a nivel interno.

Organismos Internacionales.

Respecto a la regulación internacional cabe señalar los Organismos Internacionales trabajan en forma conjunta, aunque tienen objetivos particulares a seguir.

Para la *Organización para la Cooperación Económica en Asia-Pacifico* (APEC) la regulación de los *Proveedores de los Servicios de Internet* (ISPs); se enfoca al examen de las tarifas de cobro de los ISPs (de acuerdo a la región en la que laboren, el desarrollo, funcionalidad y condiciones de los proveedores) y lo relacionado al tráfico de los flujos de información.

Para la *Comisión de Regulación de Telecomunicaciones de Colombia* (REGULATEL) la seguridad es el tema de interés dentro de la normatividad que promueve.

La *Unión Internacional de Telecomunicaciones* (UIT) trata de englobar todos los problemas como órgano máximo en materia de telecomunicaciones. Se enfoca principalmente en los problemas del sistema de nombres de dominio.

La OCDE es la más activa, aborda en términos generales la problemática del ciberespacio, esto es, desagrega todos los componentes del fenómeno y los estudia por partes y por países, identifica los puntos clave, elabora propuestas y las ofrece a sus países

2.4.2 Legislación y regulación Nacional de Internet.

En un principio, se pensó que la asignación de direcciones de Internet (como lo son .com, .gob, .edu, .net, .org, para los sitios comerciales, los gubernamentales, los educativos, los relacionados con la red y los de organizaciones civiles, respectivamente) sería la única esfera de Internet susceptible de ser regulada.

No obstante, a medida que ganó presencia social y cultural y sobre todo una significativa influencia económica, surgieron los conflictos en torno a la red y, para algunos de sus usuarios, especialmente en los gobiernos, la sensación de que hacían falta reglas específicas para ordenar el disperso universo que es la red de redes, lo mismo en el empleo de recursos como el correo electrónico y los servicios web.

La legislación nacional mexicana respecto del Internet presenta un grave problema; cualquier cosa, situación, actividad, etc., con posibilidades de ser regulada legalmente, debe ser, necesariamente definida antes de que se visualice en las leyes, es decir, nada puede ser objeto de legislación si no se tiene un concepto claro del objeto.

En el caso del Internet, este no es definido en alguna ley mexicana, sin embargo, se dice que el Internet ingresa en los términos genéricos de ‘Medio Electrónico’ e ‘Informática’; Internet no está comprendido en esa categoría, no podemos asegurar por completo que el Internet tenga un cuerpo

jurídico que lo regule. Las diferentes leyes mexicanas que ingresan el término Medio Electrónico o Informática son:

- Código Civil Federal.
- Código de Comercio.
- Código Penal Federal.
- Ley Federal del Derecho de Autor.
- Ley Federal de Telecomunicaciones.
- Ley de Información Estadística y Geografía.

Órganos Nacionales encargados de regular de actividad en internet.

- Network Information Center - México, (NIC-México).

Es la organización encargada de la administración del nombre de dominio territorial (ccTLD, country code Top Level Domain) .MX, el código de dos letras asignado a cada país según el ISO 3166. Entre sus funciones están el proveer los servicios de información y registro para .mx, así como la asignación de direcciones de IP y el mantenimiento de las bases de datos respectivas a cada recurso. Este nace el 1º de febrero de 1989, cuando el *ITESM Campus Monterrey* establece conexión directa a Internet.

- Policía Cibernética*.*

Ejerciendo sus atribuciones legales y para garantizar la presencia de la autoridad en la supercarretera de la información, la *Policía Federal Preventiva* desarrolló en México la primera *Unidad de Policía Cibernética*, que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados.

A continuación, se listan algunas de las referencias en las leyes antes mencionadas, que consideramos nos servirán de base para la elaboración de este trabajo, que contemplan actividades mediante uso de medios informáticos y en su caso también mencionan las sanciones estipuladas por la ley en caso de no ser cumplidas:

Normativa	Regulación
Código Penal Federal	**Artículo 211**.- Acceso ilícito a sistemas y equipos de informática. • *Bis 1*.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrá de 6 meses a 2 años de prisión y de 100 a 300 días de multa. • *Bis 2*.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrá de 1 a 4 años de prisión y de 200 a 600 días de multa. • *Bis 3*.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrá de 2 a 8 años de prisión y de 300 a 900 días de multa. • *Bis 4*.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran en el sistema financiero protegidos por algún mecanismo de seguridad, se le impondrá de 6 meses a 4 años de prisión y de 100 a 600 días de multa.
	Artículo 426.- Se le impondrá de 6 meses a 4 años de prisión y de 300 a 3,000 días de multa: • a quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y • a quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.
	Titulo Quinto.- Delitos en materia de vías de comunicación y de correspondencia.

	• **Artículo 174**.- No se considera que obren delictuosamente los padres que abran o intercepten las comunicaciones escritas dirigidas a sus hijos menores de edad, y los tutores respecto de las personas que se hallen bajo su dependencia, y los cónyuges entre sí. • **Artículo 176**.– Al empleado de telégrafo, estación telefónica o estación inalámbrica que conscientemente dejare de transmitir un mensaje que se le entregue con ese objeto, o de comunicar al destinatario el que recibiere de otra oficina, si causare daño, se le impondrá de 15 días a 1 año de prisión o de 30 a 180 días de multa. • **Artículo 177.-** A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le impondrá de 6 a 12 años de prisión y de 300 a 600 días de multa.
	Artículo 282.- Se impondrá de 3 días a 1 año de prisión o de 180 a 360 días de multa: • al que de cualquier modo amenace a otro con causarle un mal en su persona, en sus bienes, en su honor o en sus derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado con algún vínculo, y • al que por medio de amenazas de cualquier género trate de impedir que otro ejecute lo que tiene derecho a hacer.
Código Civil Federal	**Artículo 1803**.- El reconocimiento del consentimiento otorgado a través de medios electrónicos adquiere validez jurídica al ser incorporado dentro del concepto de consentimiento expreso.
Ley de Información Estadística y Geografía	**Artículo 2, Fracción V**.- Establece que una de sus funciones es: "…regular el desarrollo y la utilización permanente de la informática…" en el desarrollo de su labor estadística. Es decir, la informática es considerada en tanto un medio de trabajo como un objeto de estudio, si se habla de que las conexiones a Internet son un indicador importante a considerar en los censos.
Ley Federal de Telecomunicaciones	**Artículo 71.-** Las infracciones a lo dispuesto en esta Ley, se sancionarán por la Secretaría de conformidad con lo siguiente:

	• Con multa de 10,000 a 100,000 salarios mínimos por:
	  ○ (...)
	  ○ Interceptar información que se transmita por las redes públicas de telecomunicaciones, …
	• Con multa de 4,000 a 40,000 salarios mínimos por:
	  ○ (...)
	  ○ Cometer errores en la información de base de datos de usuarios, de directorios, y en el cobro de los servicios de concesionarios de redes públicas, no obstante el apercibimiento de la Secretaría, ...

Ley de Instituciones de Crédito	Autoriza a las mismas a "pactar la celebración de sus operaciones y la prestación de servicios con el público, mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos". Determina asimismo, que en los contratos respectivos deben de establecerse cuáles serán los medios para identificar al usuario y para hacer constar la creación, transmisión, modificación o extinción de los derechos y obligaciones inherentes a las operaciones de que se trate, otorgándoles validez y valor probatorio a los medios de identificación que se establezcan en sustitución de la firma autógrafa. **Artículo 112 Bis**.- Al que altere el medio de identificación electrónica y acceda a los equipos electromagnéticos del sistema bancario, con el propósito de disponer indebidamente de recursos económicos (fracción III); y a quien obtenga o use indebidamente la información sobre clientes u operaciones del sistema bancario, y sin contar con la autorización correspondiente (fracción IV), se le impondrá de 3 a 9 años y de 30,000 a 300,000 días de multa.
Ley Federal del Derecho de Autor	**Artículo 230.** Las infracciones en materia de derechos de autor serán sancionadas por el Instituto con arreglo a lo dispuesto por la *Ley Federal de Procedimiento Administrativo* con multa de 5,000 hasta 15,000 días de salario mínimo en los casos previstos en las fracciones I, II, III, IV, XI, XII, XIII y XIV del artículo anterior, y se aplicará multa adicional de hasta 500 días de salario mínimo por día, a quien persista

	en la infracción.
Ley de Firma Electrónica Avanzada	Tiene por objeto regular, el uso de la firma electrónica avanzada en los actos previstos en esta Ley y la expedición de certificados digitales a personas físicas o morales; los servicios relacionados con la firma electrónica avanzada, y la homologación de la firma electrónica avanzada con las firmas electrónicas avanzadas reguladas por otros ordenamientos legales, en los términos establecidos en esta Ley.
Código de Comercio	**Capítulo IV, Artículo 48**.- Afirma que tratándose de las copias de las cartas, telegramas y otros documentos que los comerciantes expidan, así como de los que reciban que no estén incluidos en el artículo siguiente, el archivo podrá integrarse con copias obtenidas por cualquier medio: mecánico, fotográfico o electrónico, que permita su reproducción posterior íntegra y su consulta o compulsa en caso necesario. La que se considera la parte más importante del código es el **Título Segundo, Capítulo I** que habla de los mensajes de datos en los actos de comercio y que en la formación de estos podrán emplearse medios electrónicos, ópticos o cualquier otra tecnología.

Tabla 2 – Legislación informática mexicana.

Capítulo III Marco teórico.

Antes de iniciar con la redacción del baseline se debe definir un marco referencial con el cual se puedan seleccionar y establecer los controles de seguridad informática necesarios para mitigar los posibles riesgos que afectan a los activos informáticos de las empresas.

De esta forma se tendrá en cuenta una jerarquía organizacional modelo y los servicios informáticos comunes que utilizan las empresas en proceso de formación o de establecimiento, para después proceder a asignar los controles pertinentes en el baseline para que las empresas sean conscientes de ellos y de las vulnerabilidades a las que posiblemente ya están expuestos.

Para realizar la selección de los controles se utilizarán como base primordial las normas *ISO/IEC 27001 y* la *ISO/IEC 27002*.

3.1 ISO/IEC 27001:2013 - ISO/IEC 27002:2011.

La norma ISO/IEC 27001 especifica formalmente un *SGSI*, una serie de actividades relacionadas con la gestión de los riesgos de la información. El SGSI es un marco general de gestión mediante el cual la organización identifica, analiza y aborda sus riesgos de información. Este garantiza que los arreglos de seguridad se ajusten para adaptarse a los cambios en las amenazas de seguridad, las vulnerabilidades y los impactos empresariales, aspecto importante en un campo tan dinámico y una ventaja clave de la flexibilidad de ISO27k.

El estándar cubre todos los tipos de organizaciones, todos los tamaños, y todas las industrias o los mercados. Este es claramente un informe muy amplio.

ISO**/**IEC 27001 no obliga formalmente a los controles específicos de la seguridad de la información desde los controles que se requieren varían notablemente entre la amplia gama de organizaciones que adoptan el estándar. Los controles de seguridad de la información de la norma ISO/IEC 27002 se indican en el anexo A de la norma ISO/IEC 27001, más bien como un menú. Las organizaciones que adoptan la norma ISO/IEC 27001 son libres de elegir el que más controles de seguridad de la información específicos son aplicables a sus riesgos de información particulares, a partir de los que se enumeran en el menú y, potencialmente, complementándolos con otras opciones a la carta (a veces conocidos como conjuntos de control extendido).

Al igual que con la norma ISO/IEC 27002, la clave para la selección de los controles aplicables es llevar a cabo una evaluación exhaustiva de los riesgos de información de la organización, que es una parte vital del SGSI.

Además, la administración puede optar por evitar, transferir o aceptar riesgos de información en lugar de mitigarlos a través de controles, una decisión de tratamiento de riesgos dentro del proceso de administración de riesgos.

3.1.1 Estructura de la norma.

ISO/IEC 27001: 2013 tiene las siguientes secciones:

0. **Introducción** - el estándar utiliza un enfoque basado en procesos.
1. **Ámbito de aplicación** - que especifica los requisitos del SGSI genéricos adecuados para organizaciones de cualquier tipo, tamaño o naturaleza.
2. **Referencias normativas** - solamente la norma ISO/IEC 27000 se considera absolutamente esencial para los usuarios de 27001: las normas ISO27k restantes son opcionales.
3. **Términos y definiciones** - un breve glosario formalizado, para luego ser reemplazadas por la norma ISO / IEC 27000.
4. **Contexto de la organización** - la comprensión del contexto de la organización, las necesidades y expectativas de las 'partes interesadas', y definir el alcance del SGSI. La Sección 4.4 establece muy claramente que "La organización debe establecer, implementar, mantener y mejorar continuamente" un SGSI compatible.
5. **Liderazgo** - alta dirección debe demostrar su liderazgo y compromiso con el SGSI, impone políticas y asignar información de seguridad funciones, responsabilidades y autoridades.
6. **Planificación** - describe el proceso para identificar, analizar y planificar para el tratamiento de riesgos de la información, y clarificar los objetivos de seguridad de la información.
7. **De apoyo** - adecuada, los recursos deben ser asignados competentes, mayor sensibilización, la documentación preparados y controlados.
8. **Funcionamiento** - un poco más de detalle sobre evaluación y tratamiento de riesgos de la información, gestión de cambios, y la documentación de las cosas (en parte para que puedan ser auditados por los auditores de certificación).
9. **Evaluación del rendimiento** - controlar, medir, analizar y evaluar / auditoría / revisar los controles de seguridad de la información, los procesos y el sistema de gestión con el fin de hacer mejoras sistemáticas en su caso.
10. **Mejora** - abordar los resultados de auditorías y revisiones, realizar mejoras continuas.

11. **ANEXO A** - los objetivos de control y controles de referencia - poco más en el hecho de que una lista de títulos de las secciones de control en la norma ISO/IEC 27002. El anexo es normativo, lo que implica que se espera que las organizaciones certificadas lo utilicen, pero son libres de desviarse o complementarlas para abordar sus riesgos particulares de información.
12. **Bibliografía** - puntos lectores a cinco estándares relacionados, además de la parte 1 de las Directivas ISO/IEC, para más información. Además, ISO/IEC 27000 se identifica en el cuerpo de la norma como una normativa estándar y hay varias referencias a la norma ISO 31000 de gestión de riesgo.

3.1.2 El alcance del SGSI y el Estado de Aplicación (SoA).

Mientras que la norma está destinada a impulsar la implementación de un SGSI en toda la empresa, lo que garantiza que todas las partes de la organización beneficiarse de hacer frente a sus riesgos de la información de una manera apropiada y sistemáticamente administrado, las organizaciones pueden alcance su ISMS tan amplia o restringida como se - la determinación del alcance es una decisión crucial para la alta dirección (cláusula 4.3). Un ámbito ISMS documentado es uno de los requisitos aplicables a la titulación.

A pesar de la Declaración de aplicabilidad (SOA) no se define explícitamente, es un requisito obligatorio de la sección 6.1.3. Este término común se refiere a la salida de las evaluaciones de riesgo de información y, en particular, las decisiones sobre el tratamiento de esos riesgos. El SoA, por ejemplo, puede adoptar la forma de una matriz que identifica los distintos tipos de riesgos de la información en un eje y las opciones de tratamiento del riesgo por otro, mostrando cómo se deben tratar los riesgos en el cuerpo y quién es responsable de ellos.

Por lo general, hace referencia a los controles pertinentes de ISO/IEC 27002, pero la organización puede utilizar un marco diferente, como *NIST SP800-55*, el estándar *ISF*, *BMIS* y/o COBIT o un enfoque personalizado. Los objetivos de control de seguridad de información y controles de ISO / IEC 27002 se proporcionan como una lista de comprobación en el Anexo A con el fin de evitar con vistas a los controles necesarios.

El alcance del SGSI y el SO son cruciales si un tercero tiene la intención de atribuir cualquier dependencia al certificado de conformidad ISO/IEC 27001 de una organización. Del mismo modo, si por alguna gestión razón decide aceptar los riesgos de malware sin la implementación de controles antivirus convencionales, los auditores de certificación pueden también impugnar una afirmación audaz, pero, siempre que los análisis y las decisiones asociadas eran sólidos, que por

sí sola no sería justificación para negarse a certificar la Ya que los controles antivirus no son de hecho obligatorios.

3.1.3 Métricas.

En efecto (sin utilizar realmente el término "métricas"), la edición de 2013 de la norma requiere el uso de métricas sobre el rendimiento y la eficacia de los controles de seguridad de información y SGSI de la organización. La sección 9, "Evaluación del desempeño", requiere que la organización determine e implemente métricas de seguridad adecuadas... pero sólo proporciona requisitos de alto nivel.

Cuando se libera la versión revisada, la norma ISO/IEC 27004 ofrecerá consejos sobre qué y cómo medir con el fin de satisfacer el requisito. Mientras tanto, se recomienda el enfoque descrito en las métricas de seguridad. Este estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

Se consideran los lineamientos contenidos en este documento ya que según explica el mismo, pueden servir como referencia general de objetivos de seguridad de la información, esto permite a cada organización generar un propio marco de referencia según sus objetivos organizacionales. Cada control define su finalidad, lineamientos propuestos para aplicar los mismos, y sugerencias sobre el alcance de aplicación.

Este estándar contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridades principales y una clausula introductoria que presenta la evaluación y tratamiento del riesgo.

La norma ISO 27002:2013 fue publicada originalmente como un cambio de la norma ISO 17799. En el año 2000 la *Organización Internacional de Normalización y la Comisión Electrotécnica Internacional* publicaron el estándar ISO/IEC 17799:2000, con el título de *Information technology - Security techniques - Code of practice for information security management.*se publicó en el año 2005 el documento fue modificado ISO/IEC 17799:2005.

Nombre	Métricas/Medidas
Documentación de la Política de Seguridad de Información. [5.1.1]	• Porcentaje de total requerido de políticas, procedimientos de concientización y capacitación que se han desarrollado. • Porcentaje del total requerido de Políticas de Contingencia con procedimientos de implementación que se han desarrollado.
Revisión de la Política de Seguridad de la Información. [5.1.2]	• Frecuencia de las revisiones gerenciales de seguridad. • Frecuencia de las revisiones de la política de seguridad.
Compromiso Gerencial a la seguridad de la información. [6.1.1]	• Porcentaje del total requerido de políticas de seguridad y procedimientos de planificación de seguridad que se han desarrollado.
Coordinación en seguridad de la información. [6.1.2]	• Porcentaje del total requerido de políticas de seguridad y procedimientos de planificación de seguridad que se han desarrollado.
Asignación de Responsabilidades de seguridad de la información. [6.1.3]	• Porcentaje del total requerido de políticas de seguridad y procedimientos de planificación de seguridad que se han desarrollado.
Acuerdos de confidencialidad. [6.1.5]	• Porcentaje del total requerido de políticas de seguridad y procedimientos de planificación de seguridad que se han desarrollado. • Porcentaje del total de personas que tienen acceso a información organizacional y de los sistemas de información que han sido filtradas antes de garantizársele dicho acceso.
Revisión independiente de la seguridad de la información. [6.1.8]	• Porcentaje del total requerido de políticas de seguridad y procedimientos

	de planificación de seguridad que se han desarrollado.
Roles y Responsabilidades. - Selección. [8.1.1 - 8.1.2]	• Porcentaje del total de proveedores de servicios de sistemas de información a los que se les estableció requisitos de seguridad incluyendo roles y responsabilidades.
Términos y condiciones de empleo. - Responsabilidad Gerencial. [8.1.3 - 8.2.1]	• Cantidad de cuentas abiertas de usuarios que ya no tienen relación laboral. • Porcentaje del total de personas que tienen acceso a información organizacional y de los sistemas de información que han sido filtradas antes de garantizársele dicho acceso.
Concientización, formación y entrenamiento en seguridad de la información. [8.2.2]	• Porcentaje del total del personal a los que se impartió concientización en seguridad. • Frecuencia de actualización de los planes de capacitación.
Concientización, formación y entrenamiento en seguridad de la información. - Proceso disciplinario. [8.2.2 - 8.2.3]	• Porcentaje del total del personal con roles y responsabilidades significativos que ha recibido capacitación en seguridad antes de permitirles acceso a los sistemas. • Porcentaje del total de proveedores de servicios de sistemas de información a los que se les estableció requisitos de seguridad incluyendo roles y responsabilidades. • Porcentaje del total del personal a los que se impartió concientización en seguridad. • Frecuencia de actualización de los planes de capacitación.

Remoción de derechos de acceso. [8.3.3]	• Porcentaje del total de puntos de acceso remoto desde los que se hayan logrado registro no autorizado.
Remoción de derechos de acceso. - Perímetro de seguridad física. [8.3.3 - 9.1.1]	• Cantidad de cuentas abiertas de usuarios que ya no tienen relación laboral.
Aceptación de sistemas. [10.3.2]	• Porcentaje del total del Personal con roles y responsabilidades significativos que ha recibido capacitación en seguridad antes de permitirles acceso a los sistemas.
Aceptación de sistemas. - Controles contra código malicioso. [10.3.2 - 10.4.1]	• Porcentaje del total de sistemas de alto y medio impacto en los que se ha probado exitosamente en el último período los planes de contingencia. • Porcentaje del total del personal a los que se impartió concientización en seguridad antes de permitirles acceso a los sistemas. • Cantidad de controles del software y contenido de datos usados en procesos críticos. • Cantidad de violaciones detectadas a la bajada de archivos sin pruebas de contenido malicioso. • Porcentaje del total del Personal a los que se impartió concientización respecto del uso, reportes y recuperación de ataques de código malicioso.
Respaldo de la Información. - Controles de Red. [10.5.1 - 10.6.1]	• Porcentaje del total de sistemas de alto y medio impacto en los que se ha probado los RTO y RPO correspondientes en restauración.
Registración de usuarios. [11.2.1]	• Porcentaje del total de puntos de acceso remoto desde los que se hayan logrado registro no autorizado.

Gestión de contraseñas de usuarios. - Revisión de derechos de acceso de usuarios. [11.2.3 - 11.2.4]	• Porcentaje del total de puntos de acceso remoto desde los que se hayan logrado registro no autorizado.
Computación y comunicaciones móviles. [11.7.1]	• Cantidad de accesos inalámbricos que se han usado para lograr accesos no autorizados. • Porcentaje del total de notebooks, PDA, etc. que usan protección física. • Porcentaje del total de notebooks, PDA, etc. que tienen información encriptada. • Frecuencia de back up de información crítica en dispositivos portátiles y móviles. • Porcentaje del total del personal que ha recibido capacitación especial para dispositivos portátiles y móviles.
Control de vulnerabilidades técnicas. [12.6.1]	• Cantidad de valuaciones realizadas.
Reportes de eventos de seguridad de la información. - Reportes de debilidades de seguridad. [13.1.1 - 13.1.2]	• Porcentaje del total del personal con roles y responsabilidades significativos que ha recibido capacitación en seguridad antes de permitirles acceso a los sistemas. • Porcentaje del total de incidentes que han sido informados dentro del tiempo previsto para la categoría correspondiente en cada caso.
Inclusión de la Seguridad de la Información en el proceso de gestión de continuidad de negocios. [14.1.1]	• Porcentaje del total requerido de Políticas de Contingencia con procedimientos de implementación que se han desarrollado.
Desarrollo e implementación de planes de continuidad que incluyan seguridad de la información. [14.1.3]	• Porcentaje del total requerido de Políticas de Contingencia con procedimientos de implementación que se han desarrollado.
Protección de registros de la organización. -	• Porcentaje del total del Personal a los

Protección de datos y privacidad de la información personal. [15.1.3 - 15.1.4]	que se impartió concientización en seguridad antes de permitirles acceso a los sistemas.

Tabla 3 – Métricas ISO/IEC 27002:2013

3.2 NIST 800-50.

La *Publicación Especial NIST 800-50, Construyendo un Programa de Concienciación y Capacitación en Seguridad de las Tecnologías de la Información*, brinda orientación para la construcción de un programa de seguridad de tecnología de la información efectivo.

El documento identifica los cuatro pasos críticos en el ciclo de vida de un programa de concientización y capacitación en seguridad de TI: 1) diseño de programas de concientización y capacitación (Sección 3); 2) desarrollo de material de sensibilización y capacitación (Sección 4); 3) la implementación del programa (Sección 5); Y 4) post-implementación (Sección 6). El documento es una publicación complementaria a la *Publicación Especial NIST 800-16*, Requisitos de Capacitación en Seguridad de las Tecnologías de la Información: un modelo basado en funciones y rendimiento.

Las dos publicaciones son complementarias: la SP 800-50 trabaja a un nivel estratégico más alto, discute cómo construir un programa de capacitación y concienciación sobre seguridad de TI, mientras que la SP 800-16 está en un nivel táctico inferior, describiendo un enfoque de seguridad de TI basada en roles formación. Este documento proporciona pautas para crear y mantener un programa integral de concientización y capacitación, como parte del programa de seguridad de TI de una organización.

El documento incluye orientación sobre cómo los profesionales de la seguridad de TI pueden identificar las necesidades de concientización y capacitación, desarrollar un plan de capacitación y obtener apoyo organizacional para financiar los esfuerzos del programa de concientización y capacitación. Este documento también describe cómo: Seleccionar temas de concientización y capacitación; Buscar fuentes de información y material de capacitación; Implementar materiales de concienciación y capacitación, utilizando una variedad de métodos; Evaluar la efectividad del programa; Y actualizar y mejorar el enfoque como la tecnología y las prioridades de la organización cambian.

Describe las políticas de seguridad informática, procedimientos y directrices, que son publicadas por el Instituto Nacional de Estándares y Tecnología, que contiene 130 documentos. Al igual de la

serie de normas ISO 27000, la serie SP 800 proporciona información que cubre la gestión y las prácticas operativas de seguridad de la información, pero en un mayor número de documentos. Para facilitar una guía específica para realizar la integración de la gestión de riesgos de seguridad de la información con las operaciones de la empresa, la serie SP NIST 800 tiene el documento SP 800-39- Gestión de Riesgos de Seguridad.

Para realizar la evaluación de los riesgos, la serie SP 800 tiene un conjunto de documentos que han sido creados utilizando la metodología de riesgo en seis pasos: Categorizar: se debe dar prioridad a los sistemas de información que se basan en la evaluación del impacto.

- **Seleccionar**: se deben definir los controles que se deben aplicar, en base a la evaluación del impacto y las bases de SP 800-53, siendo un documento de referencia para este paso.
- **Poner en práctica**: implementar los controles y la elaboración de los documentos.
- **Evaluar**: la confirmación de que los controles se implantan de forma correcta, operar según lo previsto, y producir los resultados deseados.
- **Autorizar**: la aceptación del escenario de riesgo, y la autorización para la operación de los sistemas de información y utilización.
- **Monitorear**: se acompaña de forma continua de los sistemas de información y el entorno operativo para establecer la eficiencia y el cumplimiento de los controles.

La serie SP 800 tiene muchos estándares que cubren hasta 256 salvaguardas. Aquí es donde SP 800-53 es muy útil, ya que organiza todas las salvaguardas en 18 categorías. Algunos documentos útiles de la serie SP 800 que hacen referencia SP 8001-53, son:

- **SP 800-61**: directrices para detectar, analizar, priorizar y gestionar los incidentes de responder a ellas de forma eficiente y eficaz.
- **SP 800-50**: pautas para el diseño, desarrollo, implantación y evaluación de un programa de sensibilización y formación.
- **SP 800-116**: es el riesgo basado en la selección de los mecanismos de autenticación apropiados para gestionar el acceso físico.
- **SP 800-46**: prácticas para mitigar los riesgos asociados con las tecnologías utilizadas para el teletrabajo.
- **SP 800-122**: orientaciones para la protección de la confidencialidad de la información de identificación de personal con el apoyo de los sistemas de información.
- **SP 800-161**: una guía para identificar, evaluar, seleccionar e implantar la gestión de riesgos y controles para gestionar los riesgos e la cadena de suministro.
- **SP 800-92**: orientación sobre el desarrollo, implantación y mantenimiento de las prácticas de gestión de riesgos eficientes para apoyo.

- **SP 800-88**: recomendaciones para la implantación de un programa de saneamiento de los medios, teniendo en cuenta las técnicas y controles para la desinfección y eliminación de la información confidencial.
- **SP 800-83**: orientación sobre la prevención de ataques de este tipo y responder a los incidentes de malware.
- **SP 800-64**: descripción de las funciones de seguridad y responsabilidades clave necesarios en el desarrollo de los sistemas de información, y la información sobre la relación entre la seguridad de la información y el ciclo de vida del software de desarrollo.
- **SP 800-45**: proporciona prácticas de seguridad para el diseño, implantación y sistemas de correo electrónico de funcionamiento en las redes públicas y privadas de apoyo.
- **SP 800-44**: presenta las prácticas de seguridad para el diseño, implantación y operación de los servidores web de acceso público e infraestructura de la red relacionada.
- **SP 800-41**: proporciona una guía durante el desarrollo de las políticas y la selección de firewall, configuración, prueba, implantación y administración de servidores de seguridad.
- **SP 800-34**: proporciona información sobre el sistema de información de la planificación e contingencia y otros tipos de planes de seguridad y emergencia de contingencia.

3.3 MAAGTICSI.

El Manual contiene, en tres grupos, los nueve procesos necesarios para propiciar la operación ágil y oportuna de las actividades de TIC de las Instituciones. Para cada área de conocimiento se utilizan los principales estándares y mejores prácticas relacionadas.

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 (EDN) en materia de Tecnologías de la Información y Comunicaciones*, y en 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 t 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 de la *Administración Pública Federal* 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.

Es una normatividad para la eficiencia operativa gubernamental de las operaciones del área de tecnologías de la información y comunicaciones emitido por la secretaria de función pública en la que se establece el acuerdo por el que se expide el manual administrativo de aplicación general en materia de tecnologías de la información y comunicaciones por decreto presidencial; cuyo ámbito de aplicación y alcance está definido para implementarse en las instituciones a través de sus correspondientes unidades administrativas responsables de proveer infraestructura y servicios de tecnologías de la información y comunicaciones; regulado bajo el marco jurídico aplicable a reglamentos, lineamientos, leyes, decretos y seguridad de la información.

Su objetivo general 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 operaciones con las que cuenten.

Sus objetivos específicos son enfocar el monitoreo y control sobre las actividades vinculadas con las TIC, en un esquema de gobernanza, organización y entrega.

Fortalecer el control sobre los recursos de TIC y mantener alineada la planeación estratégica de las instituciones al programa, a la EDN, las bases de colaboración celebradas por la institución y a las disposiciones que de estos instrumentos emanen. Mantener indicadores orientados a resultados basados en el ejercicio del presupuesto y en la entrega de servicios de valor.

3.3.1 Procesos MAAGTICSI

- Gobernanza
    - *PE: Proceso de Planeación Estratégica*. - Mantener la operación de un modelo de gobierno de TIC en la Institución, para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC, la planeación estratégica de TIC y asegurar la adecuada organización al interior de la UTIC.
    - *APCT: Administración del Presupuesto y las Contrataciones*.- Coordinar las acciones para el ejercicio del presupuesto destinado a las TIC, a fin de maximizar su aplicación en las contrataciones de TIC requeridas por la Institución, así como las acciones para efectuar el acompañamiento necesario a las unidades facultadas para realizar los procedimientos de contrataciones en la Institución, de manera que

se asegure su ejecución en tiempo y forma, alineado al presupuesto autorizado; así como el seguimiento a los contratos que se celebren.

- Organización
    - *ADS: Proceso de Administración de Servicios*. - Definir los compromisos y costos de los servicios de TIC necesarios para mantener el adecuado funcionamiento de la Institución, así como identificar iniciativas de servicios de TIC que aporten beneficios importantes en el cumplimiento de los objetivos estratégicos de la Institución, con apego a la EDN y efectuar su instrumentación.
    - *ACNF: Proceso de Administración de la Configuración*.- Establecer y actualizar un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas de la UTIC, como elementos de configuración, con la finalidad de facilitar su acceso a los involucrados en los procesos de la UTIC, cuando éstos así lo requieran para la operación del proceso respectivo.
    - *ASI: Proceso de Administración de la Seguridad de la Información*. - Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional.

- Entrega
    - *ADP: Proceso de Administración de Proyectos*. - Administrar la cartera operativa de proyectos de TIC, a fin de optimizar la aplicación de los recursos y obtener mayores beneficios para la Institución.
    - *APRO: Proceso de Administración de Proveedores*. - Establecer un mecanismo que permita verificar el cumplimiento de las obligaciones derivadas de los contratos celebrados para la adquisición, arrendamiento o servicios de TIC.
    - *AOP: Proceso de Administración de la Operación*. - Entregar a los usuarios los servicios de TIC, conforme a los niveles de servicio acordados y con los controles de seguridad definidos.
    - *OPEC: Operación de Controles de Seguridad de la Información y del ERISC* (equipo de respuesta a incidentes de seguridad en Tic en la institución). - Implementar y operar los controles de seguridad de la información de acuerdo al programa de implementación del SGSI, así como los correspondientes a la capacidad de respuesta a incidentes.

Capítulo IV Desarrollo de baseline.

Basados en los diferentes documentos relacionados a buenas prácticas existentes, estos pueden ser aplicados a cualquier tipo de empresa, y dependerá del alcance de sus objetivos y tamaño de la misma una aplicación en mayor o menor grado de especialización para mejorar las actividades de la empresa.

Sin embargo, nuestro objetivo serán empresas de reciente creación las cuales pueden o no tener un alto grado de experiencia en seguridad de la información o no tener conocimiento alguno sobre el tema.

En este capítulo se busca simplificar y elegir los controles que consideramos básicos y mínimamente necesarios que se puedan requerir en una empresa para reducir los riesgos de seguridad informática con un documento que sirva como referencia para crear y aplicar controles necesarios de seguridad para reducir los riesgos de seguridad que puedan ocurrir y afectar las actividades de la empresa.

Agruparan los controles contenidos en ISO 27001:2013 e 27002:2013 eligiendo aquellos que consideremos más necesarios.

Para ello es necesario evaluar la organización en cuanto a tamaño y tipo actividad que llevan a cabo para tener claros que controles serán necesarios ser aplicados.

4.1 Identificación de las divisiones funcionales de las áreas de TI.

Para poder catalogar los controles que formarán parte de nuestro baseline, es necesario tener identificadas las áreas hacia las cuales estarán dirigidos. Por ese motivo, tomamos como base tres organigramas y tomar las áreas básicas que conformará nuestra propuesta.

1. Empresa mexicana con 68 años de experiencia en soluciones integrales de infraestructura. Con una presencia en México, Latinoamérica y Estados Unidos.
   De este primer organigrama consideramos en color azul las partes de las gerencias que forman la estructura base de nuestro organigrama, como tal, no se necesita un coordinador dado que nuestro baseline está bajo el supuesto de una organización que comienza su área de TI.

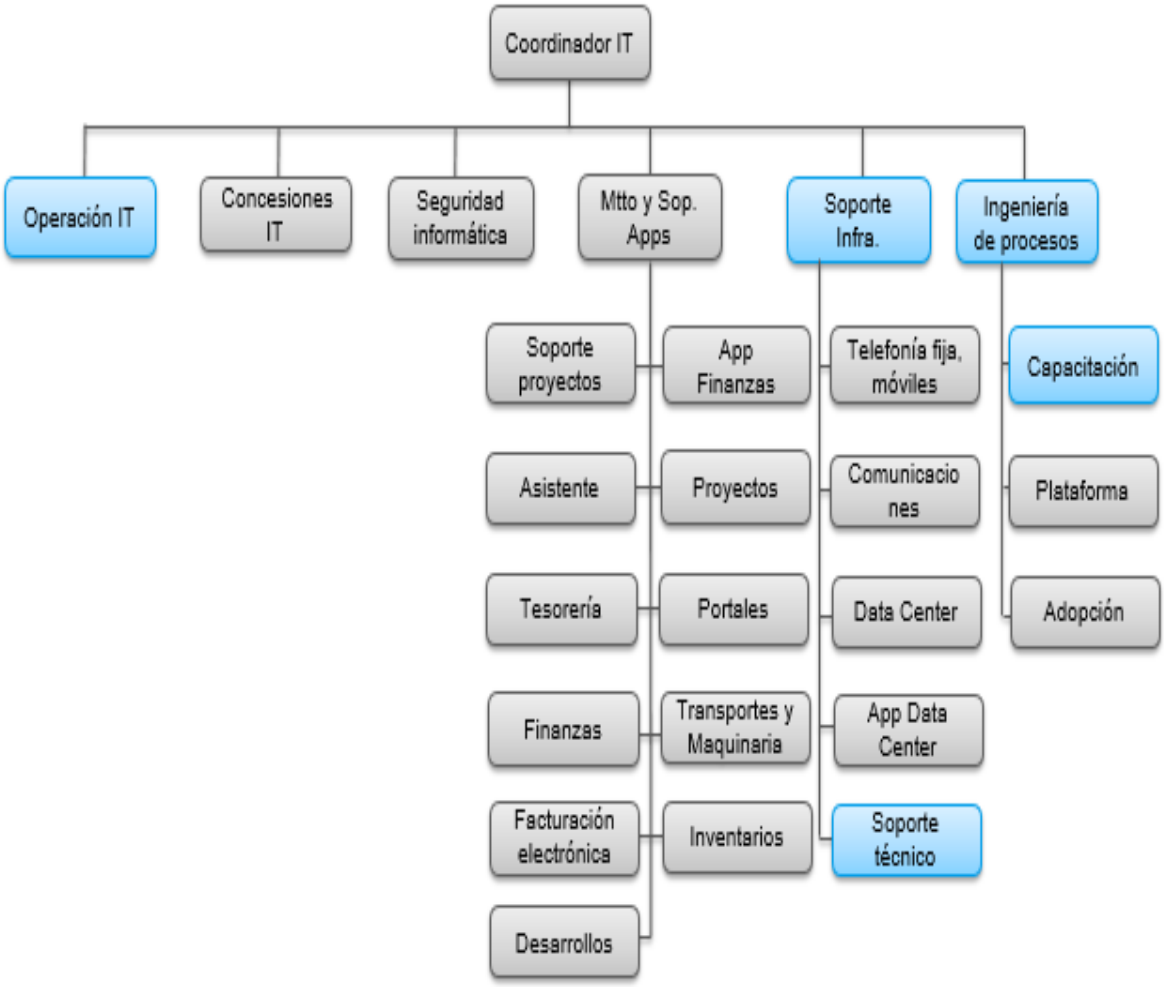

Ilustración 7

2. Conglomerado mexicano de empresas correspondientes al sector industrial, construcción e infraestructura. Sus operaciones se desarrollan en más de 45 países. Fundada en 1952, tiene cuatro líneas principales de negocios: metales, construcción, sistemas, cemento y plásticos.

   De este organigrama tomamos al director como base, ya que es importante que coordine la gerencia a nivel operativo, de aplicación y de infraestructura, así como los gestores de cada área que trabajan en conjunto con el director

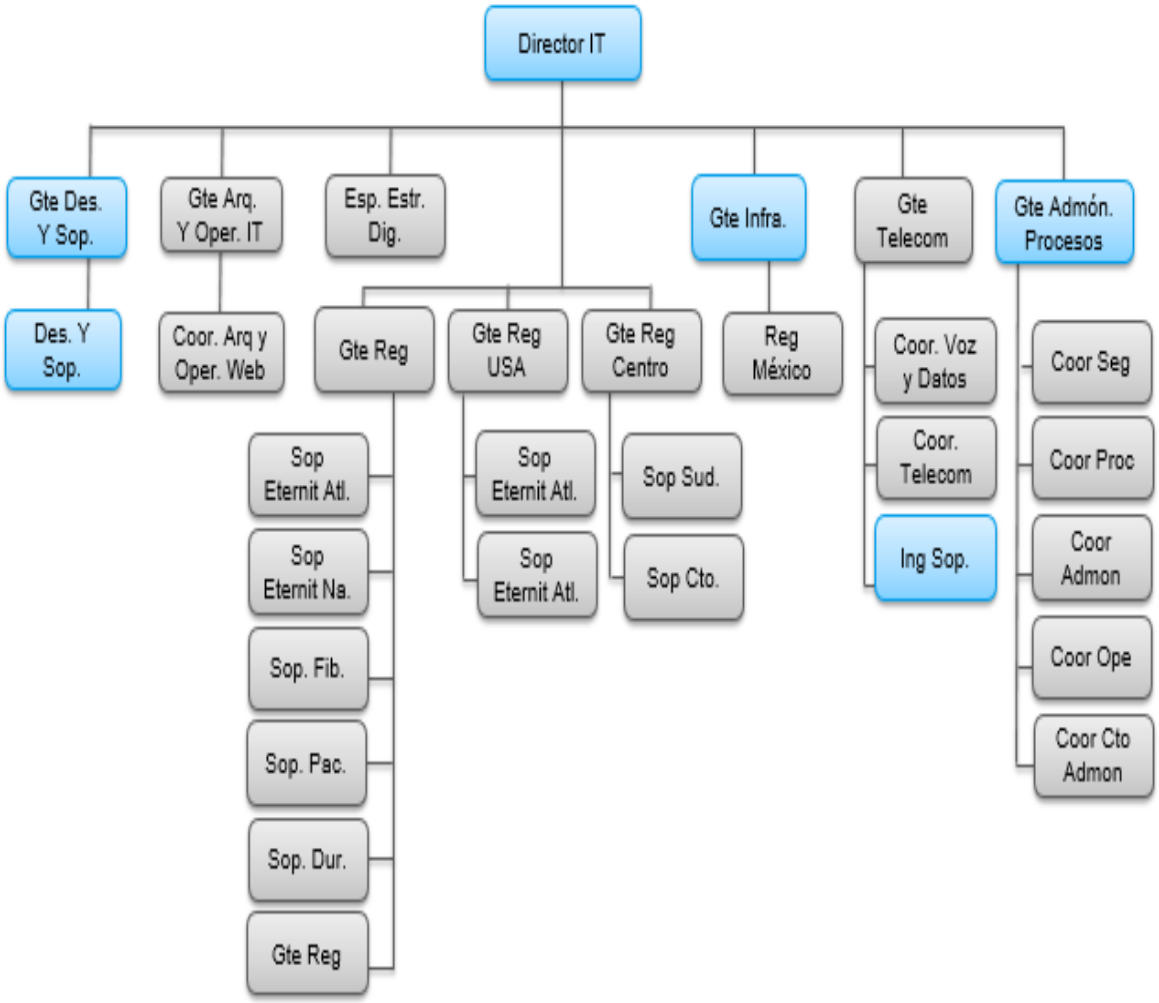

Ilustración 8

3. Empresa dedicada a la producción, embotellado, distribución y venta de refrescos en México. La empresa ofrece bebidas no carbonatadas y agua purificada. La compañía tiene su sede en Zapopan, México.

   De este esquema tomamos más definiciones para la parte de la operación y los encargados de ejecutar y dar soporte a todas las entidades que conforman al negocio.

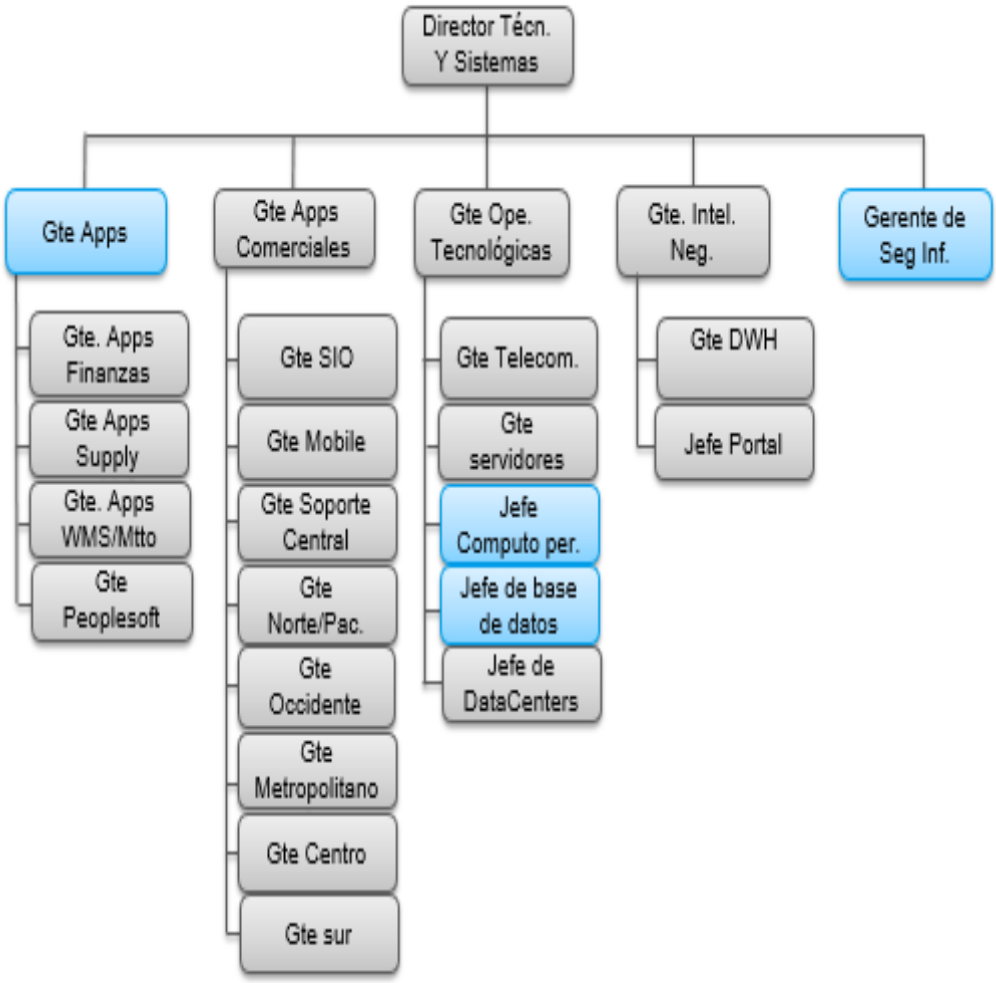

Ilustración 9

4. Organigrama propuesto. - Como resultado de estos tres organigramas, proponemos la siguiente estructura:

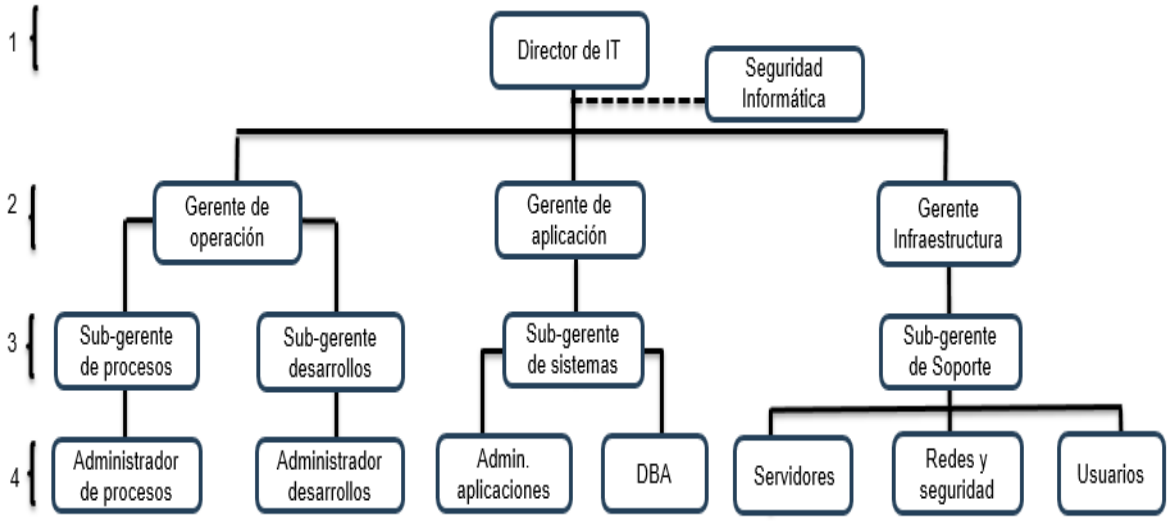

Ilustración 10

- **1er nivel**:
  - **Director de TI**: Es el responsable de llevar a cabo la coordinación de las actividades, asegurar que no haya contratiempos y que sean eficientes todas las áreas que componen las tecnologías de la información y alcanzar los objetivos y metas que se plantean a corto, mediano y largo plazo.
- **2do nivel**:

Puesto	Reporta a:
Gerente de operación	Director de TI
Gerente de aplicación	
Gerente de infraestructura	

  - **Gerente de operación**: La gestión de la operación es responsable de cumplir con la ejecución de procesos del negocio, así como proposición de mejoras o modificación de estos.
  - **Gerente de aplicación**: Esta gestión es encargada de las aplicaciones que la organización tiene implementadas, además de realizar una planeación estratégica de actualizaciones que requiera el negocio, o implementación de nuevas tecnologías según se requiera.
  - **Gerente de infraestructura**: La persona con la responsabilidad de esta área, debe de llevar control de la infraestructura y servicios con los que el personal de la empresa cuenta. Así mismo, debe de planificar ventanas de mantenimiento que deben aplicarse periódicamente.

- **Externo/Seguridad informática**: Esta entidad debe de proporcionar las recomendaciones con base en las mejores prácticas, ISOs, controles, protocolos que se adapten a las necesidades de la empresa.

- **3er nivel**: Encargadas de la supervisión de las áreas ejecutoras, este nivel debe de asegurar el cumplimiento de los objetivos de cada una de sus responsabilidades.

Puesto	Reporta a:
Sub-gerente de procesos	Gerente de operación
Sub-gerente de desarrollos	
Sub-gerente de sistemas	Gerente de aplicación
Sub-gerente de soporte	Gerente de infraestructura

  - **Sub-gerente de procesos**: Personal con la encomienda de llevar el control de los procesos que deben ser ejecutados por el administrador y asegurar que se cumplan los tiempos de ejecución de los mismos.
  - **Sub-gerente de desarrollos**: Encargado de la revisión del progreso de los programas planeados para los procesos del negocio y planeación de nuevos desarrollos, así como su documentación para la creación de estos programas.
  - **Sub-gerente de sistemas**: Persona delegada de monitorear y asegurar la estabilidad de las aplicaciones y bases de datos que constituyen a la empresa, así como tener en bitácora las expiraciones de la licencia, la duración del soporte y planificar aplicación de parches.
  - **Sub-gerente de soporte**: La función de este personal, es verificar que las áreas de comunicación y la disponibilidad de los servidores presenten el menor número de caídas o incidencias. Certificar que los protocolos están aplicados en las áreas solicitadas y que el personal cuente con los recursos de acuerdo con su nivel jerárquico.

- **4to nivel**: Consideradas como áreas ejecutoras de la operación, infraestructura, aplicación, son las encargadas de llevar a cabo las funciones básicas que aseguran la continuidad del negocio en las distintas áreas de TI.

Puesto	Reporta a:
Administrador de procesos	Sub-gerente de procesos
Administrador de desarrollos	Sub-gerente de desarrollos

Administrador de aplicaciones	Sub-gerente de sistemas
DBA	
Servidores	Sub-gerente de soporte
Redes y seguridad	
Usuarios	

A continuación, se enuncian las principales actividades de cada área:

- **Administrador de procesos**: Se encarga del monitoreo de la operación del negocio, generalmente en horarios 24/7 o de acuerdo con las necesidades de la organización. Su principal función es asegurar el inicio y término exitoso de los procesos. En caso de incidentes mayores, estos pasan a segundo nivel.
- **Administrador de desarrollos**: Su función en sí, es ser el ejecutor mediante un lenguaje de programación utilizado por la organización que se cumplan las especificaciones funcionales que darán continuidad del negocio en los tiempos requeridos.
- **Administrador de aplicaciones**: Encargado de la disponibilidad de los sistemas con los que lleva a cabo sus funciones el negocio. Debe de ejecutar monitoreo de primer nivel, es decir, documentar el comportamiento de las aplicaciones, tener identificadas los intervalos de estrés de las aplicaciones y generar un reporte.
- **DBA**: Persona delegada de garantizar que los espacios de las bases de datos utilizadas por el negocio estén configurados de acuerdo a las mejores prácticas del proveedor del software, así como planificar en conjunto con su jefe inmediato los horarios y fechas de la ejecución de respaldos online y offline.
- **Servidores**: Personal con la responsabilidad de dar mantenimiento, aplicación de parches, planear en conjunto con su superior los snapshots, administración de servidores tanto físicos como virtuales, y asegurar su alta disponibilidad.
- **Redes y seguridad**: El elemento de redes y seguridad, debe tener acceso a un monitor general de todos los servicios que están conectados a la intranet de la organización. Verificar que los protocolos y puertos que se encuentran implementados cumplan las necesidades de seguridad en el negocio.
- **Usuarios**: Grupo encargado de la administración de recursos informáticos (activos) para el personal de la organización, así como ejecutores del soporte para los usuarios (hardware y software).

4.1.1 Identificación de activos.

- Procesos y actividades empresariales.
    - Procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización.
    - Procesos que contienen procesos secretos u otros procesos que involucran tecnología patentada.
    - Procesos que, si se modifican, pueden afectar en gran medida el cumplimiento de la misión de la organización.
    - Procesos que son necesarios para que la organización cumpla con los requisitos contractuales, legales o regulatorios.
- Información.
    - Información vital para el ejercicio de la misión o negocio de la organización.
    - Información personal, como se puede definir específicamente en el sentido de las leyes nacionales en materia de privacidad.
    - Información estratégica necesaria para alcanzar los objetivos determinados por las orientaciones estratégicas.
    - Información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión requieren mucho tiempo y/o implican un alto costo de adquisición.

Los activos de apoyo, en los que se basan los elementos primarios del ámbito de aplicación:

- **Hardware**.
    - *Equipo de procesamiento de datos*. - Equipo automático de procesamiento de información que incluye los elementos necesarios para operar independientemente.
    - *Medio de datos*. - Son medios electrónicos para almacenar datos o funciones. Un medio de información que se puede conectar a una computadora o a una red informática para el almacenamiento de datos. A pesar de su tamaño compacto, estos medios pueden contener una gran cantidad de datos, pueden utilizarse con equipos informáticos estándar.
    - *Medios de comunicación estáticos y no electrónicos que contienen datos*. - El software consta de todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos.
    - *Sistema operativo*. - Incluye todos los programas de una computadora que constituyen la base operacional desde la cual se ejecutan todos los demás programas (servicios o aplicaciones). Incluye un kernel y funciones o servicios básicos. Dependiendo de la arquitectura, un sistema operativo puede ser

monolítico o compuesto de un micro núcleo y un conjunto de servicios del sistema. Los principales elementos del sistema operativo son todos los servicios de gestión de equipos (CPU, memoria, disco e interfaces de red), servicios de gestión de tareas o procesos y servicios de gestión de derechos de usuario.

- *Software de paquete o software estándar*. – Estos programas informáticos son productos completos comercializados como tales con medio, liberación y mantenimiento. Proporcionan servicios para usuarios y aplicaciones, pero no son personalizados ni específicos en la forma en que son las aplicaciones de negocio.

- **Aplicación de negocios**. - Se trata de software comercial diseñado para brindar a los usuarios acceso directo a los servicios y funciones que requieren de su sistema de información en su contexto profesional. Hay una gama muy amplia, teóricamente ilimitada, de campos.
- **Medio y soportes**. - Los medios o equipos de comunicaciones y telecomunicaciones se caracterizan principalmente por las características físicas y técnicas del equipo (punto a punto, emisión) y por los protocolos de comunicación (enlace o red - niveles 2 y 3 del OSI Modelo de 7 capas).
- **Personal**. - Consiste en todos los grupos de personas involucradas en el sistema de información. Los tomadores de decisiones son los dueños de los activos primarios (información y funciones) y los administradores de la organización o del proyecto.
  - *Usuarios*. - Los usuarios son el personal que maneja elementos sensibles en el contexto de su actividad y que tienen una responsabilidad especial a este respecto. Pueden tener derechos especiales de acceso al sistema de información para llevar a cabo sus tareas cotidianas.
  - *Personal de Operación / Mantenimiento*. - Son los encargados de operar y mantener el sistema de información. Tienen derechos especiales de acceso al sistema de información para llevar a cabo sus tareas cotidianas.
  - *Desarrolladores*. - Están a cargo de desarrollar las aplicaciones de la organización. Tienen acceso a parte del sistema de información con derechos de alto nivel, pero no toman ninguna acción sobre los datos de producción.
  - *Site*.- El tipo de sitio comprende todos los lugares que contienen todo o parte del ámbito y los medios físicos necesarios para que funcione.
- **Ubicación**.
  - *Locales*. - Este lugar está delimitado por el perímetro de la organización directamente en contacto con el exterior. Esto puede ser un límite físico de protección obtenido mediante la creación de barreras físicas o medios de vigilancia alrededor de los edificios.

- *Zona*. - Una zona está formada por un límite físico de protección que forma particiones dentro de las instalaciones de la organización. Se obtiene creando barreras físicas alrededor de las infraestructuras de procesamiento de información de la organización.
- *Servicios esenciales*. - Todos los servicios necesarios para que los equipos de la organización funcionen. Servicios y equipos de telecomunicaciones proporcionados por un operador.
- *Utilidades*. - Servicios y medios (fuentes y cableado) necesarios para suministrar energía a equipos de tecnología de la información y periféricos. Abastecimiento de agua. Eliminación de residuos. Servicios y medios (equipos y control) para enfriar y purificar el aire.
- *Organización*.- El tipo de organización describe el marco organizativo que consiste en todas las estructuras de personal asignadas a una tarea y los procedimientos que controlan estas estructuras.
- *Autoridades*.- Son entidades de las que la organización estudiada deriva su autoridad, pueden ser legalmente afiliados o externos. Esto impone limitaciones a la organización estudiada en términos de reglamentos, decisiones y acciones. Consiste en las diversas ramas de la organización, incluyendo sus actividades multifuncionales, bajo el control de su gestión.
- *Organización del proyecto o del sistema*.- Se refiere a la organización establecida para un proyecto o servicio específico.

4.2 Selección de controles óptimos.

La selección de los controles se realiza con base a los dominios contemplados en el ISO 27002:2013.

6. Organización de la seguridad de la información.- Con el fin de establecer controles debidamente enfocados a cumplir los objetivos de la organización en cuanto a la seguridad de la información es necesario tener un responsable que coordine las actividades relacionadas en cuanto a seguridad de la información se refiere.

Esto permite a la organización prevenir actividades sin la debida autorización o inapropiadas. No necesariamente se requiere que se cree un área para realizar estas actividades, pero si tener un responsable de cada activo que se haga responsable de su cuidado y resguardo. Sin importar el tamaño de la organización, la información que genera día a día en sus actividades deben ser

protegidas del acceso a terceras personas ajenas a la organización para minimizar riesgos, para ello se deben definir los procedimientos necesarios para brindar información a terceros.

- **6.1.3 Asignación de las responsabilidades de la seguridad de la información**.- Se tiene que establecer una estructura de gestión donde se controle toda la implementación de Seguridad de la Información dentro de la organización. Tienen que encontrase perfectamente identificados todos los activos y los procesos de seguridad. Tiene que nombrarse al responsable de cada activo o proceso de seguridad. Debe definirse y documentarse todos los niveles de autorización.
- **6.1.4 Autorización de proceso para facilidades procesadoras de información**.- Se deberá checar el hardware y software para asegurar que son compatibles con otros componentes del sistema. Las autorizaciones deberán ser obtenidas del gerente responsable del ambiente de seguridad de información para asegurar que todos los requerimientos de seguridad relevantes son cumplidos.
- **6.1.5 Acuerdos de confidencialidad**.- Se deberá definir la información a protegerse, se deberán tener condiciones para el retorno o destrucción de la información una vez que se termina el acuerdo.
- **6.2.1 Identificación de los riesgos relacionados con los grupos externos**.- Se deberán tener los medios de procesamiento de información y los medios de procesamiento de información: acceso físico, acceso lógico, conectividad de red y si es acceso se da fuera o dentro de la empresa.
- **6.2.2 Tratamiento de la seguridad cuando se lidia con clientes**.- Se deberán considerar los términos de seguridad antes de proporcionar a los clientes acceso a cualquier activo de la organización. Procedimiento para proteger los activos información y software y el manejo de vulnerabilidades. Se deberá tener restricciones en el copiado y divulgación de la información.

8. Gestión de activos.- Consideramos como activos para la seguridad de la información, como cualquier información o sistemas que son de valor para la organización. Algunos de los activos que pueden ser considerados son:

- software y licencias
- equipo de cómputo (hardware)
- bases de datos
- documentos
- instalaciones
- servicios informáticos y comunicaciones
- personal

Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el resguardo del mismo, aunque no necesariamente se encargara de su mantenimiento. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.
En este dominio relacionado con la identificación y clasificación de activos de acuerdo con su y nivel de confidencialidad.

El inventario de activos tiene que incluir toda la información que resulte necesaria con el fin de recuperarse ante un desastre, en que se incluya el tipo de activo, el formato, la ubicación, la información de respaldo, la información de licencia y el valor de negocio. Es decir, se encargará de llevar un registro de los detalles del activo para genera una clasificación dentro de la organización que permita conocer su estado, ubicación y tipo. Una manera de clasificar estos detalles seria:

- tipo de activo
- ubicación
- responsable
- descripción general

El propósito es verificar si son utilizados de manera correcta, tanto como sea posible y poder recuperar los mimos en caso de una emergencia, en base a su importancia dentro de la organización y el impacto que estos recursos tienen en las actividades de la empresa. Por ejemplo, según el tamaño de la organización, podría ser de más peso los registros en papel archivados en un cajón, que una laptop que solo se usa para enviar mails. Otro aspecto que puede identificarse de este inventario de activos es conocer cuál es el valor total de los activos con los que trabaja la empresa y conocer cuáles son los costos de recuperación de cada uno de ellos.

- **7.1.1 Inventario de los activos**.- Se deberá identificar la importancia del activo, su valor comercial y su clasificación de seguridad.
- **7.1.2. Propiedad de los activos**.- Se deberá asegurar que la información y los activos asociados con los medios de procesamiento sean clasificados apropiadamente. Se deberá definir y revisar periódicamente las restricciones y clasificaciones de acceso tomando en cuenta las políticas de control de acceso aplicables.
- **7.1.3 Uso aceptable de los activos**.- Se deberán de poner reglas para la utilización del correo electrónico e Internet. Así como también lineamientos para el uso de dispositivos móviles, especialmente para el uso fuera del local de la organización.

7. Seguridad de recursos humanos.- La finalidad de este dominio, es asegurar que cada uno de los empleados conozcan sus responsabilidades con el equipo e información que manejan y entiendan

sus responsabilidades y sean adecuados para las funciones que efectúan, con el fin de reducir el riesgo de robo, fraude o mal uso de las instalaciones.

La adición de una persona a una empresa o el ascenso implica un nuevo nivel de acceso a otras partes del sistema de la organización.

Se deben considerar controles y programas de inducción a los controles y procedimientos de seguridad con los que estará involucrado cada uno de los empleados según su rol y actividades.

La gestión de la seguridad de la información depende principalmente de las personas que componen la Organización y se debe definir las responsabilidades de la gerencia para que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro de la organización, a su vez debe definir cuáles son las acciones disciplinarias que se deben llevar a cabo en caso de que algún empleado no cumpla con sus responsabilidades en cuanto a seguridad se refiere.

Así también la salida de empleados con lleva un riesgo, ya que se debe considerar todas aquellas acciones necesarias para asegurar que la persona que deja la organización no tenga acceso nuevamente a información relevante de la organización y a las instalaciones, así también se haya devuelto todo el equipo con el que haya tenido contacto.

- **8.1.1 Roles y responsabilidades**.- Se deberán de dar roles para implementar y actuar en concordancia con las políticas de seguridad de la información de la organización. Se deberán proteger los activos contra el acceso, divulgación, modificación no autorizada y asegurar que se asigne a la persona la responsabilidad por las acciones tomadas.
- **8.1.3 Términos y condiciones del empleo**.- Se deberá tener un acuerdo para empleados, contratistas y terceros que tienen acceso a la información sensible en el cual se tenga que firmar un acuerdo de confidencialidad o no divulgación antes de otorgarles el acceso.
- **8.2.1 Responsabilidades de la gerencia**.- El gerente deberá estar apropiadamente informado sobre sus roles y responsabilidades de seguridad antes de otorgarles acceso a información confidencial o a los sistemas de información. Deberá de lograr un nivel de conciencia sobre seguridad relevante para sus roles y responsabilidades dentro de la organización a sus usuarios empleados, contratistas y terceras personas.
- **8.2.2 Conocimiento, educación y capacitación en seguridad de la información**.- Se deberá de comenzar con un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios. La capacitación deberá ser constante y deberá de incluir los requerimientos de seguridad, responsabilidades legales y controles comerciales.

- **8.3.1 Responsabilidades de terminación**.- Deberá de incluir requerimientos de seguridad constantes y responsabilidades legales y cuando sea apropiado las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad y los términos y condiciones de empleo continuando durante un periodo después de terminado el empleo del usuario empleado, contratista o tercera persona.
- **8.3.2 Devolución de los activos**.- Se deberá ser formalizado para incluir la devolución de todo software documento corporativo y equipo entregado previamente. También se deberá devolver otros activos organizacionales como dispositivos móviles, tarjetas de acceso, software, e información almacenada en electrónicos.
- **8.3.3 Retiro de los derechos de acceso**.- Se deberá reconsiderar los derechos de acceso de una persona a los activos asociados con los sistemas y servicio de informacion.se deberán de retirar los derechos de acceso para los activos de información y los medios de procesamiento de información antes de la terminación o cambio de empleo dependiendo de la evaluación de los factores de riesgo.

11. Seguridad física y ambiental.- La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema de información, y es que los factores ambientales pueden afectar se igual manera que lo haría un hacker o un empleado que hace mal uso de su acceso a la información, provocando pérdidas no solo de información sino también de equipo que implica un costo para la organización, esto no necesariamente de controles excesivamente especializados, como sistemas costosos, como se haría en empresas grandes; en empresas pequeñas cuyos recursos no sean bastos, bastara con definir un ambiente controlado como la buena organización de los equipos de cómputo por sencillos que sean, como el buen acomodo del cableado o la simple limpieza de los equipos.

A su vez es necesario que la organización considere controles de acceso a sus equipos que fuera del uso de contraseñas para el acceso al sistema, es considerar el acceso a las instalaciones donde se encuentre el equipo, y un registro que contemple quienes tienen acceso a las áreas de la organización con equipo e información importante para la empresa con información de las actividades de la misma el control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a permitir o negar acceso basado en restricciones de tiempo, área dentro de una empresa o institución.

- **9.1.2 Controles de ingreso físico**.- Se deberá de registrar la fecha y la hora de entrada y salida de los visitantes y todos los visitantes deberían ser supervisados a no ser que su acceso haya sido previamente aprobado, se deberá restringir y controlar el acceso a las áreas sensibles solo para personas autorizadas. Se deberá requerir a todos los visitantes, empleados, contratistas a que usen una identificación visible.

- **9.2.1 Ubicación y protección del equipo**.- Los equipos de trabajo se deberán de ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo. Se deberán de adaptar controles de riesgo para minimizar amenazas potenciales como robo, fuego, humo, agua, etc.
- **9.2.3 Seguridad del cableado**.- Se deberá tener de manera subterránea o estar sujetas a una alternativa de protección adecuada las líneas de energía y telecomunicaciones que van con medios de procesamiento de información.
- **9.2.4 Mantenimiento de equipo**.- Se deberá definir un plan de mantenimiento preventivo y correctivo periódico para la infraestructura y equipos de cómputo relevantes con el objetivo de asegurar su disponibilidad e integridad, contando con un registro de este plan que contemple los incidentes identificados y acciones correctivas implementadas.

12. Gestión de las comunicaciones y operaciones.- Se busca asegurar la eficiente operación de los medios de procesamiento de información, estableciendo responsabilidades y desarrollando procedimientos que logren mitigar la negligencia y el mal uso deliberado.

- **10.1.4 Separación de los medios de desarrollo, prueba y operación**.- Se deberá contar con ambientes de desarrollo y/o pruebas segregados del ambiente productivo de los aplicativos, considerando que estos entornos alternos puedan emular en lo más posible al ambiente principal evitando incluir información considerada como confidencial. Asimismo, se deberá implementar una segregación de tareas entre el personal encargado del desarrollo, el personal encargado de implementar cambios en el ambiente productivo y los usuarios con acceso e a este último entorno con el objetivo de evitar modificaciones no autorizadas o no adecuadas que comprometan la confidencialidad e integridad de la información.
- **10.2.2 Monitoreo y revisión de los servicios de terceros**.- Se debe considerar ejecutar un monitoreo o revisión periódica sobre el nivel de servicios brindados por proveedores de servicios contratados, considerado que esta revisión contemple niveles de servicios, registros y solución de incidencias y eventos de seguridad, así como monitoreo de las actividades que puedan comprometer la seguridad de la información de la entidad manejado por las terceras partes.
- **10.5 Respaldo o Back-Up**.- Se deberá establecer un procedimiento periódico de ejecución y restauración de copias de respaldo de la información relevante de los sistemas de información con el objetivo de asegurar la integridad y disponibilidad de esta información en caso de un desastre o falla en los medios de almacenamiento. Este procedimiento deberá considerar lineamientos como el nivel y tipo de información a respaldar, frecuencia de ejecución de los respaldos con base en los requerimientos del negocio y de seguridad, procedimientos para restaurar la información y ejecución de pruebas periódicas,

almacenamiento de las copias de seguridad en ubicaciones alternas y con mecanismos suficientes para prevenir daños físicos y ambientales, y periodos de retención de la información respaldada.

- **10.6.2 Seguridad de los servicios de la red**.- Se debe considerar ejecutar un monitoreo o revisión periódica sobre el nivel de servicios brindados por proveedores de servicios contratados, considerado que esta revisión contemple niveles de servicios, registros y solución de incidencias y eventos de seguridad, así como monitoreo de las actividades que puedan comprometer la seguridad de la información de la entidad manejado por las terceras partes.
- **10.7.1 Gestión de medios removibles**.- Se deben establecer medidas para la eliminación de medios que ya no sean requeridos y que contengan información sensible de la entidad, con el objetivo de asegurar que la información no puede ser recuperable. Estas medidas pueden incluir definir método de borrado seguro, acuerdos de confidencialidad y establecimiento de controles en caso de contratar a una organización de servicios encargada de ejecutar esta actividad.
- **10.8.4 Mensajes electrónicos**.- Es deber implementar controles para proteger la información divulgada a través de mensajes electrónicos. Como establecer técnicas y medios seguros de transmisión de información que aseguren la confidencialidad y disponibilidad de la información, consideraciones legales locales, política de uso de medios públicos externos y niveles robustos de autenticación y transmisión a través de estos.

9. Control del acceso.- Se busca regular el acceso a la información, a sus medios de procesamiento y a los procesos comerciales basándose en los requerimientos comerciales y de seguridad. Las reglas a establecerse deben de considerar las políticas para divulgación y autorización.

- **11.2.1 Registro del usuario**.- Se debe establecer un procedimiento para la gestión del aprovisionamiento de usuarios para el registro, modificación y revocación de accesos en los sistemas. Específicamente considerar lo siguiente:
    - Asignar y utilizar IDs de usuario únicos, siendo definidos con la nomenclatura definida por la administración. En caso de requerir cuentas genéricas o compartidas, estas deben contar con una razón de negocio y deben ser documentadas para ser otorgadas.
    - Asegurar que antes de la creación/modificación de un usuario se tenga las autorizaciones correspondientes por el área de negocio o gerente inmediato y por al administrador del sistema.

- Validar que los accesos solicitados para un usuario nuevo o modificado sean los apropiados de acuerdo con su puesto y en la organización y con base en sus tareas asignadas por el negocio, no comprometiendo la segregación de funciones.
- Contemplar el alcance de los controles de autorización para usuarios de sistemas y de proveedores o cualquier otro tipo de empleados externos.
- Ejecutar una revisión periódica de los usuarios activos con el objetivo de validar que la vigencia y los niveles de acceso de las cuentas sean los correctos.
- Deshabilitar oportunamente los accesos de los empleados que hayan cambiado de puesto/función o que hayan concluido su relación laboral con la organización.
- Asegurar no asignar más de un ID de usuario a un solo empleado.

- **11.2.2 Gestión de privilegios**.- Se deberán establecer controles sobre la asignación de accesos con privilegios de administración en los sistemas que contemplen lo siguiente:
  - Contar con un flujo de autorización de este tipo de permisos en cada componente de tecnología como sistema de aplicación, bases de datos, sistemas operativos y especificar los usuarios que contarán con estos privilegios.
  - Asignar los altos privilegios con restricción a los accesos mínimos que requerían los usuarios con base en sus funciones en la organización.
  - Asignar los altos privilegios en un ID de usuarios distinto de aquellos utilizados para uso normal del negocio.
- **11.2.3 Gestión de las claves secretas de los usuarios**.- Se deberán establecer controles sobre el uso y políticas de seguridad de contraseñas en los sistemas que contemplen lo siguiente:
  - Establecer un acuerdo de confidencialidad y uso de las contraseñas con los usuarios y asegurar la aceptación del mismo por medio de la firma de los empleados.
  - Implementar una configuración que obligue a los usuarios a realizar el cambio de la contraseña inicial asignada por el administrador del aplicativo.
  - Modificar las contraseñas iniciales o por defecto de cuentas de proveedor inmediatamente después concluir la instalación de sistemas o paquetes de software.
- **11.2.4 Revisión de los derechos de acceso del usuario**.- Se debe establecer un procedimiento de revisión periódica de los usuarios activos en los sistemas considerando los siguientes lineamientos:
  - Validar semestralmente que la vigencia y los niveles de acceso de las cuentas sean los correctos con base en sus funciones.

- Validar individualmente los accesos cuando se presente un cambio de función o de puesto de un usuario en la organización y asignar los nuevos permisos correspondientes.
- Validar cada 3 meses que la vigencia y los niveles de acceso de las cuentas con altos privilegios o de administración sean los correctos con base en sus funciones.

- **11.3.1 Uso de claves secretas**.- Se deberán implementar controles que fomenten el uso de buenas prácticas para la sección y uso de contraseñas, como son:
  - Mantener la confidencialidad de las contraseñas.
  - Evitar registros de las claves de acceso en medio no seguros como papel y archivos en texto plano.
  - Modificar de forma inmediata las contraseñas en caso de identificar un posible incidente de seguridad que completa la confidencialidad de estas claves.
  - Seleccionar contraseñas con una longitud mínima suficiente para ser fácil de recordar, que no contengan información personal básica de identificar como números telefónicos, nombre de familiares, fechas de nacimiento, entre otros; que no contengan palabras incluidas en diccionarios y que no se encuentren conformadas por caracteres consecutivos idénticos.
  - Definir cambios periódicos de las claves de acceso, considerando una mayor frecuencia para las contraseñas de cuentas de administración, y evitar el reciclaje o reutilización de claves antiguas.
  - Evitar compartir las contraseñas individuales.
- **11.3.2 Equipo del usuario desatendido**.- Comunicar a los usuarios los requerimientos de seguridad y los lineamientos a seguir para proteger su equipo desatendido, como son:
  - Cerrar las sesiones una vez que se haya concluido la actividad. Implementar mecanismos/políticas para asegurar que este lineamiento se cumpla, por ejemplo, protectores de pantallas o bloqueo automático por sesión inactiva.
  - Implementar control de acceso en los servidores o equipos de cómputo por medio de contraseñas individuales al iniciar una sesión.
- **11.4.6 Control de conexión a la red**.- Se deberá implementar mecanismos que permitan restringir la capacidad de usuarios para conectarse a la red, especialmente en conexiones externas de la red corporativa. Asimismo, se deberán limitar servicios como correo electrónico, transferencia de archivos y acceso remotos a las aplicaciones.
- **11.5.2 Identificación y autenticación del usuario**.- Se deberá contar con IDs únicos de usuario e implementar métodos de autenticación para restringir el acceso a los recursos tecnológicos. Este control debe ser aplicado para todos los tipos de usuarios como personal de soporte técnico, operadores, cuentas genéricas o compartidas, usuarios de

proveedor, administradores de aplicación, sistemas operativos y bases de datos, y usuarios regulares.

14. Adquisición, desarrollo y mantenimiento de los sistemas de información.- Se busca identificar y avalar los requerimientos de seguridad como parte integral del desarrollo de sistemas de información, en los cuales el diseño y la implementación pueden ser cruciales.

- **12.6.1 Control de las vulnerabilidades técnicas**.- Se deberá implementar un proceso de gestión y control de vulnerabilidades técnicas identificadas que afecten a los activos declarados que contemple lo siguiente:
    - Definir roles y responsabilidades asociada con la gestión y monitoreo de las vulnerabilidades y los activos asociadas a los mismos.
    - Definir acciones y tiempos de tratamiento sobre de las vulnerabilidades potenciales identificadas.
    - Aplicar las acciones sobre las vulnerabilidades con base en el control de cambios y siguiendo el proceso de gestión de incidentes de seguridad definido por la entidad.
    - Evaluar e implementar una etapa de pruebas en la implementación de parches de seguridad antes de ser instalados en los ambientes principales de los sistemas.

16. Gestión de un incidente en la seguridad de la información.- Se busca certeza de que los eventos y debilidades de seguridad de la información sean comunicados oportunamente para que los involucrados estén al tanto de los procedimientos para el reporte debiera requerir que reporten cualquier evento y debilidad de la seguridad de la información lo más rápidamente posible en el punto de contacto designado.

- **13.1.1 Reporte de eventos en la seguridad de la información**.- Se deberá establecer un procedimiento formal para el reporte de eventos de seguridad de información, que involucre un procedimiento de respuesta y priorización y tipificación de los incidentes. Asimismo, se debe concientizar a todos los empleados, proveedores y terceros de identificar y reportar cualquier evento de seguridad de la información.

18. Cumplimiento.- Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad. El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales. Se debiera buscar la asesoría sobre los requerimientos legales específicos de los asesores legales de la organización o profesionales legales calificados adecuados. Los requerimientos legislativos varían de un país a otro y pueden variar para la información creada en un país que es transmitida a otro país (es decir, flujo de data inter-fronteras).

- **15.1.1 Identificación de la legislación aplicable**.- Se deberán identificar y definir los requerimientos estatales, reguladores o contractuales relevantes y asegurar que el enfoque de la organización logre satisfacer estos requerimientos para cada sistema de información de la entidad.
- **15.1.4 Protección de la data y privacidad de la información personal**.- Se deberá asegurar la protección y privacidad de los datos personales con base en los requerimientos estatales, reguladores o contractuales relevantes para la entidad y asegurar la divulgación y comunicación a todo el personal involucrado. Asimismo, se debe asignar a un responsable del funcionamiento de estas actividades a través de establecer procedimientos específicos que cumplan con las regulaciones y legislaciones relevantes.

4.3 Redacción del baseline.

Baseline de Seguridad It

Propósito

El presente documento es un baseline de seguridad informática de aplicación en todas las áreas funcionales de la organización en sus actividades relacionadas al manejo de la información y los equipos computacionales.

Está dirigido a todo el personal sin importar su nivel jerárquico o roles a desempeñar, desde los directivos hasta el personal operático, por lo cual es responsabilidad de la organización difundir este documento a todos los involucrados y capacitar a aquellos en los controles relacionados a sus funciones. El objetivo por cumplir es que la seguridad informática esté presente en todas las actividades que realiza la organización.

Alcance

Este documento aborda consideraciones de seguridad en las siguientes áreas:

- Responsabilidades de la dirección
- Seguridad física
- Seguridad de control de acceso
- Seguridad de datos
- Seguridad de la aplicación
- Seguridad de redes y comunicaciones

En concordancia a la correcta aplicación y seguimiento de este baseline, se recomienda la asignación de la figura de Oficial de Seguridad de TI, quien será responsable de dar seguimiento a la aplicación de los controles y programas de seguridad informática dentro de la organización con el siguiente rol (complementario a sus roles laborales previos):

- Revisar regulaciones y proponer cambios al presente baseline y al reglamento interno, en relación con seguridad de TI
- Definir encargados y funciones específicas relacionadas a tareas de seguridad.
- Brindar orientación al personal y supervisar la aplicación de la normativa de seguridad (incluyendo este documento).
- Coordinar actividades encaminadas a la difusión y capacitación, además de promover la concientización de la seguridad informática.
- Mantener un inventario de registros, informes y evidencias resultantes de la aplicación de controles de seguridad de TI que permitan responder a posibles incidentes futuros.

Definiciones

Para efectos de este baseline, tomando las definiciones incluidas en el Manual Administrativo de Aplicación General en Materia de Tecnologias de la Informacion y Comunicaciones en su Anexo Único, se entenderá por:

- **Activo de información**: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
- **Activos de proceso**: Los elementos de información que son parte de un proceso y que reflejan características específicas del mismo.
- **Activo de soporte**: El que apoya o complementa a un activo primario en su función.
- **Ambiente de trabajo**: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.
- **Amenaza**: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.
- **Arquitectura tecnológica**: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.
- **Bitácora de seguridad**: El registro continúo de eventos e incidentes de seguridad de la información que ocurren a los activos de información.

- **Cambios administrados**: La integración controlada, eficiente, segura y oportuna de componentes y/o activos de TIC, aplicativos de cómputo, soluciones tecnológicas o servicio de TIC, que modifican el ambiente operativo de la UTIC; mediante criterios técnicos y mecanismos para la planeación y ejecución de dichos cambios, a fin de que éstos sean efectuados satisfactoriamente sin exponer el ambiente operativo y la operación de los servicios de TIC.
- **Confidencialidad**: La característica o propiedad por la cual la información sólo es revelada a individuos o procesos autorizados.
- **Disponibilidad**: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.
- **Evento**: El suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.
- **Funcionalidad**: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.
- **Impacto**: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.
- **Incidente**: A la afectación o interrupción a los activos de TIC, a las infraestructuras de información esenciales y/o críticas, así como a los activos de información de la Institución, incluido el acceso no autorizado o no programado a éstos.
- **Integridad**: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso.
- **Problema**: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.
- **Recursos de TIC**: La infraestructura, los activos, el recurso humano en la UTIC y el presupuesto de TIC.
- **Requerimientos funcionales**: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.
- **Riesgo**: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras de información esenciales y/o críticas y activos de información de la Institución.
- **Usuarios**: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.
- **Vulnerabilidades**: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a

las infraestructuras de información esenciales y/o críticas, así como a los activos de información.

- **SGSI**: El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información.

Controles

Organización de la seguridad de la información.-

- **Asignación de las responsabilidades de la seguridad de la información**.- Se establece una estructura de gestión que controla la Seguridad de la Información, identificando plenamente todos los activos y los procesos y nombrando al responsable de cada activo o proceso de seguridad, además de definirse y documentarse los niveles de autorización.
- **Autorización de proceso para facilidades procesadoras de información**.- Checar hardware y software para asegurar su compatibilidad con otros componentes del sistema. Las autorizaciones se obtienen del gerente responsable del ambiente.
- **Acuerdos de confidencialidad**.- Definir la información a protegerse, además de las condiciones para el retorno o destrucción de esta una vez que se termina su utilidad.
- **Identificación de los riesgos relacionados con los grupos externos**.- Tener los medios de procesamiento de información necesarios y de forma optima.
- **Tratamiento de la seguridad cuando se lidia con clientes**.- Considerar los términos de seguridad antes de proporcionar a los clientes acceso a los activos. Tener restricciones en el copiado y divulgación de la información.

Gestión de activos.-

- **Inventario de los activos**.- Identificar la importancia de los activo, su valor comercial y su clasificación de seguridad.
- **Propiedad de los activos**.- Asegurar que la información y los activos asociados con los medios de procesamiento sean clasificados apropiadamente, definiendo y revisando periódicamente las restricciones y clasificaciones de acceso de acuerdo a las políticas.
- **Uso aceptable de los activos**.- Poner reglas para la utilización del correo electrónico e Internet, así como también lineamientos para el uso de dispositivos móviles, especialmente para el uso fuera del local de la organización.

Seguridad de recursos humanos.-

- **Roles y responsabilidades**.- Asignar roles para implementar y actuar en concordancia con las políticas de seguridad para proteger los activos contra el acceso, divulgación y modificación no autorizada, asignando también a un responsable.
- **Términos y condiciones del empleo**.- Tener un acuerdo para empleados, contratistas y terceros que tienen acceso a información sensible en el cual se firmar un acuerdo de confidencialidad o no divulgación antes de otorgar el acceso.
- **Responsabilidades de la gerencia**.- El gerente debe estar apropiadamente informado sobre sus roles y responsabilidades de seguridad antes de otorgar acceso a información o a los sistemas de información. Debe buscar cierto nivel de capacitación sobre seguridad relevante para sus roles y responsabilidades en sus empleados y contratistas.
- **Conocimiento, educación y capacitación en seguridad de la información**.- Comenzar un proceso de inducción formal diseñado para exponer las políticas y expectativas de seguridad antes de otorgar accesos. La capacitación debe ser constante y debe de incluir los requerimientos de seguridad, responsabilidades legales y controles comerciales.
- **Responsabilidades de terminación**.- Incluir requerimientos de seguridad constantes y responsabilidades legales, cuando sea apropiado a las responsabilidades contenidas dentro del acuerdo de confidencialidad y de los términos y condiciones de empleo durante un periodo después de terminado el empleo del empleado, contratista o tercera persona.
- **Devolución de los activos**.- Formalizar la devolución de todo software, documento corporativo y equipo entregado previamente al empleado. Se deben devolver todos los activos organizacionales.
- **Retiro de los derechos de acceso**.- Se deberá reconsiderar los derechos de acceso de una persona a los activos asociados con los sistemas y servicio de informacion.se deberán de retirar los derechos de acceso para los activos de información y los medios de procesamiento de información antes de la terminación o cambio de empleo dependiendo de la evaluación de los factores de riesgo.

Seguridad física y ambiental.-

- **Controles de ingreso físico**.- Se deberá de registrar la fecha y la hora de entrada y salida de los visitantes y todos los visitantes deberían ser supervisados a no ser que su acceso haya sido previamente aprobado, se deberá restringir y controlar el acceso a las áreas sensibles solo para personas autorizadas. Se deberá requerir a todos los visitantes, empleados, contratistas a que usen una identificación visible.
- **Ubicación y protección del equipo**.- Los equipos de trabajo se deberán de ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo. Se deberán de

adaptar controles de riesgo para minimizar amenazas potenciales como robo, fuego, humo, agua, etc.

- **Seguridad del cableado**.- Se deberá tener de manera subterránea o estar sujetas a una alternativa de protección adecuada las líneas de energía y telecomunicaciones que van con medios de procesamiento de información.
- **Mantenimiento de equipo**.- Se deberá definir un plan de mantenimiento preventivo y correctivo periódico para la infraestructura y equipos de cómputo relevantes con el objetivo de asegurar su disponibilidad e integridad, contando con un registro de este plan que contemple los incidentes identificados y acciones correctivas implementadas.

Gestión de las comunicaciones y operaciones.-

- **Separación de los medios de desarrollo, prueba y operación**.- Se deberá contar con ambientes de desarrollo y/o pruebas segregados del ambiente productivo de los aplicativos, considerando que estos entornos alternos puedan emular en lo más posible al ambiente principal evitando incluir información considerada como confidencial. Asimismo, se deberá implementar una segregación de tareas entre el personal encargado del desarrollo, el personal encargado de implementar cambios en el ambiente productivo y los usuarios con acceso e a este último entorno con el objetivo de evitar modificaciones no autorizadas o no adecuadas que comprometan la confidencialidad e integridad de la información.
- **Monitoreo y revisión de los servicios de terceros**.- Se debe considerar ejecutar un monitoreo o revisión periódica sobre el nivel de servicios brindados por proveedores de servicios contratados, considerado que esta revisión contemple niveles de servicios, registros y solución de incidencias y eventos de seguridad, así como monitoreo de las actividades que puedan comprometer la seguridad de la información de la entidad manejado por las terceras partes.
- **Respaldo o Back-Up**.- Se deberá establecer un procedimiento periódico de ejecución y restauración de copias de respaldo de la información relevante de los sistemas de información con el objetivo de asegurar la integridad y disponibilidad de esta información en caso de un desastre o falla en los medios de almacenamiento. Este procedimiento deberá considerar lineamientos como el nivel y tipo de información a respaldar, frecuencia de ejecución de los respaldos con base en los requerimientos del negocio y de seguridad, procedimientos para restaurar la información y ejecución de pruebas periódicas, almacenamiento de las copias de seguridad en ubicaciones alternas y con mecanismos suficientes para prevenir daños físicos y ambientales, y periodos de retención de la información respaldada.

- **Seguridad de los servicios de la red**.- Se debe considerar ejecutar un monitoreo o revisión periódica sobre el nivel de servicios brindados por proveedores de servicios contratados, considerado que esta revisión contemple niveles de servicios, registros y solución de incidencias y eventos de seguridad, así como monitoreo de las actividades que puedan comprometer la seguridad de la información de la entidad manejado por las terceras partes.
- **Gestión de medios removibles**.- Se deben establecer medidas para la eliminación de medios que ya no sean requeridos y que contengan información sensible de la entidad, con el objetivo de asegurar que la información no puede ser recuperable. Estas medidas pueden incluir definir método de borrado seguro, acuerdos de confidencialidad y establecimiento de controles en caso de contratar a una organización de servicios encargada de ejecutar esta actividad.
- **Mensajes electrónicos**.- Es deber implementar controles para proteger la información divulgada a través de mensajes electrónicos. Como establecer técnicas y medios seguros de transmisión de información que aseguren la confidencialidad y disponibilidad de la información, consideraciones legales locales, política de uso de medios públicos externos y niveles robustos de autenticación y transmisión a través de estos.

Control del acceso.-

- **Registro del usuario**.- Se debe establecer un procedimiento para la gestión del aprovisionamiento de usuarios para el registro, modificación y revocación de accesos en los sistemas. Específicamente considerar lo siguiente:
    - Asignar y utilizar IDs de usuario únicos, siendo definidos con la nomenclatura definida por la administración. En caso de requerir cuentas genéricas o compartidas, estas deben contar con una razón de negocio y deben ser documentadas para ser otorgadas.
    - Asegurar que antes de la creación/modificación de un usuario se tenga las autorizaciones correspondientes por el área de negocio o gerente inmediato y por al administrador del sistema.
    - Validar que los accesos solicitados para un usuario nuevo o modificado sean los apropiados de acuerdo con su puesto y en la organización y con base en sus tareas asignadas por el negocio, no comprometiendo la segregación de funciones.
    - Contemplar el alcance de los controles de autorización para usuarios de sistemas y de proveedores o cualquier otro tipo de empleados externos.
    - Ejecutar una revisión periódica de los usuarios activos con el objetivo de validar que la vigencia y los niveles de acceso de las cuentas sean los correctos.

- Deshabilitar oportunamente los accesos de los empleados que hayan cambiado de puesto/función o que hayan concluido su relación laboral con la organización.
- Asegurar no asignar más de un ID de usuario a un solo empleado.

- **Gestión de privilegios**.- Se deberán establecer controles sobre la asignación de accesos con privilegios de administración en los sistemas que contemplen lo siguiente:
  - Contar con un flujo de autorización de este tipo de permisos en cada componente de tecnología como sistema de aplicación, bases de datos, sistemas operativos y especificar los usuarios que contarán con estos privilegios.
  - Asignar los altos privilegios con restricción a los accesos mínimos que requerían los usuarios con base en sus funciones en la organización.
  - Asignar los altos privilegios en un ID de usuarios distinto de aquellos utilizados para uso normal del negocio.
- **Gestión de las claves secretas de los usuarios**.- Se deberán establecer controles sobre el uso y políticas de seguridad de contraseñas en los sistemas que contemplen lo siguiente:
  - Establecer un acuerdo de confidencialidad y uso de las contraseñas con los usuarios y asegurar la aceptación del mismo por medio de la firma de los empleados.
  - Implementar una configuración que obligue a los usuarios a realizar el cambio de la contraseña inicial asignada por el administrador del aplicativo.
  - Modificar las contraseñas iniciales o por defecto de cuentas de proveedor inmediatamente después concluir la instalación de sistemas o paquetes de software.
- **Revisión de los derechos de acceso del usuario**.- Se debe establecer un procedimiento de revisión periódica de los usuarios activos en los sistemas considerando los siguientes lineamientos:
  - Validar semestralmente que la vigencia y los niveles de acceso de las cuentas sean los correctos con base en sus funciones.
  - Validar individualmente los accesos cuando se presente un cambio de función o de puesto de un usuario en la organización y asignar los nuevos permisos correspondientes.
  - Validar cada 3 meses que la vigencia y los niveles de acceso de las cuentas con altos privilegios o de administración sean los correctos con base en sus funciones.
- **Uso de claves secretas**.- Se deberán implementar controles que fomenten el uso de buenas prácticas para la sección y uso de contraseñas, como son:
  - Mantener la confidencialidad de las contraseñas.

- Evitar registros de las claves de acceso en medio no seguros como papel y archivos en texto plano.
- Modificar de forma inmediata las contraseñas en caso de identificar un posible incidente de seguridad que completa la confidencialidad de estas claves.
- Seleccionar contraseñas con una longitud mínima suficiente para ser fácil de recordar, que no contengan información personal básica de identificar como números telefónicos, nombre de familiares, fechas de nacimiento, entre otros; que no contengan palabras incluidas en diccionarios y que no se encuentren conformadas por caracteres consecutivos idénticos.
- Definir cambios periódicos de las claves de acceso, considerando una mayor frecuencia para las contraseñas de cuentas de administración, y evitar el reciclaje o reutilización de claves antiguas.
- Evitar compartir las contraseñas individuales.

- **Equipo del usuario desatendido**.- Comunicar a los usuarios los requerimientos de seguridad y los lineamientos a seguir para proteger su equipo desatendido, como son:
  - Cerrar las sesiones una vez que se haya concluido la actividad. Implementar mecanismos/políticas para asegurar que este lineamiento se cumpla, por ejemplo, protectores de pantallas o bloqueo automático por sesión inactiva.
  - Implementar control de acceso en los servidores o equipos de cómputo por medio de contraseñas individuales al iniciar una sesión.
- **Control de conexión a la red**.- Se deberá implementar mecanismos que permitan restringir la capacidad de usuarios para conectarse a la red, especialmente en conexiones externas de la red corporativa. Asimismo, se deberán limitar servicios como correo electrónico, transferencia de archivos y acceso remotos a las aplicaciones.
- **Identificación y autenticación del usuario**.- Se deberá contar con IDs únicos de usuario e implementar métodos de autenticación para restringir el acceso a los recursos tecnológicos. Este control debe ser aplicado para todos los tipos de usuarios como personal de soporte técnico, operadores, cuentas genéricas o compartidas, usuarios de proveedor, administradores de aplicación, sistemas operativos y bases de datos, y usuarios regulares.

Adquisición, desarrollo y mantenimiento de los sistemas de información.-

- **Control de las vulnerabilidades técnicas**.- Se deberá implementar un proceso de gestión y control de vulnerabilidades técnicas identificadas que afecten a los activos declarados que contemple lo siguiente:
  - Definir roles y responsabilidades asociada con la gestión y monitoreo de las vulnerabilidades y los activos asociadas a los mismos.

- Definir acciones y tiempos de tratamiento sobre de las vulnerabilidades potenciales identificadas.
- Aplicar las acciones sobre las vulnerabilidades con base en el control de cambios y siguiendo el proceso de gestión de incidentes de seguridad definido por la entidad.
- Evaluar e implementar una etapa de pruebas en la implementación de parches de seguridad antes de ser instalados en los ambientes principales de los sistemas.

Gestión de un incidente en la seguridad de la información.-

- **Reporte de eventos en la seguridad de la información**.- Se deberá establecer un procedimiento formal para el reporte de eventos de seguridad de información, que involucre un procedimiento de respuesta y priorización y tipificación de los incidentes. Asimismo, se debe concientizar a todos los empleados, proveedores y terceros de identificar y reportar cualquier evento de seguridad de la información.

Cumplimiento.-

- **Identificación de la legislación aplicable**.- Se deberán identificar y definir los requerimientos estatales, reguladores o contractuales relevantes y asegurar que el enfoque de la organización logre satisfacer estos requerimientos para cada sistema de información de la entidad.
- **Protección de la data y privacidad de la información personal**.- Se deberá asegurar la protección y privacidad de los datos personales con base en los requerimientos estatales, reguladores o contractuales relevantes para la entidad y asegurar la divulgación y comunicación a todo el personal involucrado. Asimismo, se debe asignar a un responsable del funcionamiento de estas actividades a través de establecer procedimientos específicos que cumplan con las regulaciones y legislaciones relevantes.

Capítulo V Propuesta de concientización y entrenamiento.

5.1 Justificación e importancia la concientización y capacitación de la seguridad de la información.

Una de las principales problemáticas hablando en temas de estrategia de seguridad de la información, es sin duda la falta de esta, y en el mejor de los casos el poco nivel conocimiento sobre este tópico y su relevancia en una organización.

Lo anterior se presenta principalmente en gran medida a la falta de conciencia de la importancia por parte de los usuarios involucrados directa e indirectamente en la seguridad. Tal es el caso, que una encuesta global sobre seguridad de la información realizada en 2015 por la firma especializada en servicios profesionales *Ernest & Young*, reveló que el 44% de las empresas encuestadas consideran como una de las principales vulnerabilidades a los empleados inconscientes en materia de seguridad de la información y, asimismo, este mismo porcentaje de las empresas señalaron el *phishing*, como principal amenaza hacia sus activos, la cual es derivada de la falta de una educación y capacitación del personal en seguridad.

La implementación de un programa de seguridad de la información no puede ser puesta en marcha con la ausencia de un plan de educación que contemple la concientización y capacitación de los empleados sobre la seguridad; entendiendo como propósito de la concientización el centrar la atención de los usuarios en la seguridad permitiendo identificar asuntos relacionados con esta y cómo responder de manera adecuada, tomando como base una serie de términos, temas y conceptos. Mientras que la capacitación se enfoca en generar en los profesionales habilidades y competencias relevantes y necesarias en las distintas especialidades funcionales de la seguridad de TI, permitiendo ejecutar ciertas tareas específicas.

Debido a esto, radica la importancia de asegurar que todo el personal involucrado en la preservación de la confidencialidad, integridad y disponibilidad de la información comprenda sus roles y responsabilidades con base en la misión organizacional, entienda las políticas, los procedimientos y las prácticas de seguridad de TI, y tenga al menos el conocimiento adecuado de los diversos controles administrativos, operacionales y técnicos requeridos y disponibles para proteger los recursos o activos de TI de los que son responsables.

De acuerdo con la documentación del NIST, adaptamos un modelo que va dirigido al área de informática, tomando como base el organigrama propuesto con las principales áreas de TICs y que se complementa con el propósito y alcance de nuestro baseline.

5.2 Creación de campaña de difusión del baseline.

Estructura de concientización y programa de entrenamiento.

De acuerdo con el NIST Special Publication 800-50, para poder realizar el programa de entrenamiento y la estructura de organización, a continuación, se describen tres enfoques o modelos comunes:

- Modelo 1: Política centralizada, estrategia e implementación
- Modelo 2: Política centralizada y estrategia, implementación distribuida
- Modelo 3: Política centralizada, estrategia distribuida e implementación.

El modelo que se adopta y se establece para supervisar la actividad del programa de sensibilización y capacitación depende de:

- El tamaño y la dispersión geográfica de la organización.
- Definición de roles y responsabilidades.
- Asignaciones presupuestarias y autoridad (Dirección, Gerencias, etc., según amerite).

En relación a nuestro modelo de organización propuesto para el baseline, consideramos adaptar el primer modelo (ver siguiente Ilustración: Gestión de Programa Centralizado), para enfocarlo a los departamentos sugeridos en nuestro esquema organizacional del área de TI propuesto en el capítulo anterior a se adapta a las características del organigrama propuesto ya que va dirigido a una empresa que inicia su área de TI.

Este modelo centralizado de administración de programas es a menudo implementado por empresas que:

- Son relativamente pequeñas o tienen un alto grado de estructura y administración central de la mayoría de las funciones de TI.
- Tener, los recursos necesarios, la experiencia y el conocimiento de la (s) misión (es) y operaciones a nivel de departamento.
- Tener un alto grado de similitud en la misión y objetivos operacionales en todos sus componentes.

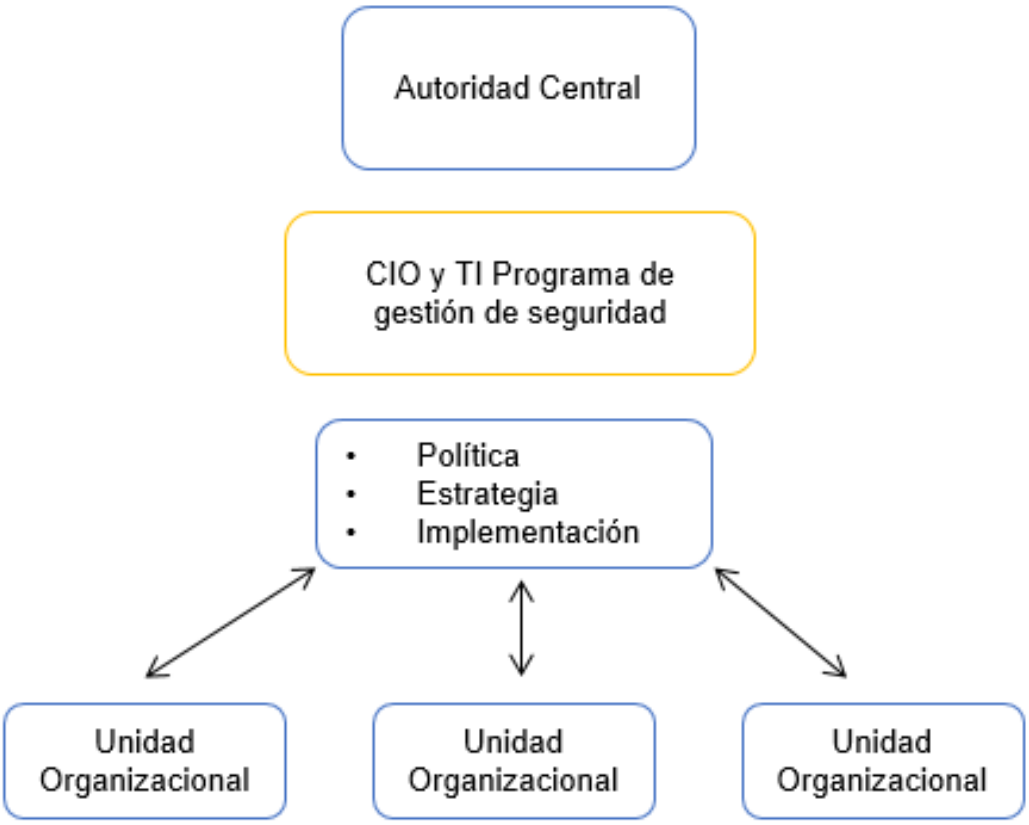

Ilustración 11

En este modelo, debe existir una autoridad central, la cual tiene la responsabilidad del control del presupuesto y generar los programas de concientización, de la misma manera ayuda a la evaluación de necesidades, ya que será la encargada de generar la planificación, así como crear los elementos para dar una inducción adecuada a todo el personal.

Deberá de existir una comunicación entre esta autoridad central y las unidades organizativas. La autoridad central transmitirá los planes de capacitación, los materiales y/o programas que se implementaran en las unidades organizativas, y a la vez, estas unidades proporcionaran la información necesaria para el cumplimiento de las tareas mencionadas. Todo con el fin de establecer la comunicación necesaria para lograr los objetivos de concientizar al personal agregando o eliminando material o modificando los métodos de implementación.

El modelo propuesto es ideal para empresas que están iniciando su área de TI, o tienen un alto grado de estructura y administración central en las tecnologías de la información.

Con base en el modelo seleccionado para la estructura de nuestra propuesta de programa de concientización y capacitación del baseline, sugerimos realizar una evaluación de las necesidades

de este programa. a continuación, se presenta un modelo adaptado de acuerdo con los departamentos definidos en el organigrama.

Ilustración 12

Debido a que nuestro baseline se encuentra enfocado para empresas pequeñas y de reciente creación, lo que conlleva a contar con una estructura centralizada y poco compleja, así como una solo misión definida, consideramos como adecuadas la implementación de las técnicas, propuestas por el estándar NIST 800-50 de entrevistas con el grupo de personal clave (dirección, gerencia, dueños/ de los sistemas y personal operativo) y la aplicación de un cuestionario en materia seguridad de la información para poder obtener métricas y determinar las principales necesidades de la propuesta de nuestro programa, y asimismo poder determinar qué se tiene actualmente implementado para cubrir esas necesidades, qué tan adecuadas son las acciones con las que ya se cuenta, y que más se puede hacer para fortalecer estas acciones. Nuestra propuesta de cuestionario diagnóstico es el siguiente:

Puesto: _____

Departamento: _____

Jefe inmediato: _____

Este cuestionario tiene como objetivo obtener información sobre las habilidades, conocimiento y experiencia, así como saber las actividades que usted desempeña cuando

utiliza los sistemas o la red de la organización. Los datos recabados servirán para diseñar una adecuada capacitación con las áreas de oportunidad que se expongan en este documento.

Parte 1

1. ¿Sabe usted que es la seguridad informática?

Sí ( ) No ( )

2. ¿Conoce los riesgos y amenazas a los que está expuesta la organización en seguridad informática?

Sí ( ) No ( )

3. ¿Conoce y/o utiliza herramientas para la protección de su equipo de cómputo?

Sí ( ) No ( )

4. De acuerdo a su puesto, ¿Usted requiere permisos de administrador en su usuario?

Sí ( ) No ( ) No lo sabe ( )

5. Sí la respuesta es no. ¿Sus actividades requieren permisos de administrador?

Sí ( ) No ( ) ¿Por qué?:

_____

6. ¿Cuenta con alguna capacitación en administración de sistemas o base de datos?

Sí ( ) No ( )

_____

(Escuela/Empresa) (Nombre de la capacitación) (Duración:Días) (Año)

7. ¿Cuenta con alguna certificación en seguridad de la información? (sí la respuesta es sí, llenar las líneas de abajo

Sí ( ) No ( )

_____

(Escuela/Empresa) (Nombre de la certificación) (Duración:Días) (Año)

8. ¿Está informado sobre los riesgos y amenazas informáticos de los que pude ser víctima la organización?

Sí ( ) No ( )

Parte 2

Por cada tarea de la columna A, marque con una X de la columna B la letra que indique el tiempo en que realiza la tarea: (N) Nunca, (A) Al menos una vez al mes, (M) Mensual, (S) Semanal (D) Diario.		Indica con ✓ la opción en donde aprendiste a realizar la tarea, si la respuesta es "Otro" especifica en donde	Por cada tarea indica con una ✓ el nivel de entrenamiento que crees necesitar (B) Básico, (I) Intermedio, (A) Avanzado
A	B		
Administración de procesos			
Monitoreo de la operación del negocio	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Ejecución de procesos	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Creación de procesos	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Gestión de procesos estándar	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Gestión de procesos personalizados	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Calendarización de pruebas unitarias	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A

Bitácora de las colas de procesos	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Administrador de desarrollos			
Desarrollar programas específicos	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Realizar pruebas de validación	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Desarrollo de memorias técnicas por programa.	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Ejecución de debugs	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Administrador de aplicaciones			
Generación de reportes	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Monitoreo de las aplicaciones	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Atención y documentación de tickets	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Planeación de backups	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio	( ) B ( ) I ( ) A

		( ) Otro:_____	
DBA			
Planificación y ejecución de respaldos	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Monitoreo de espacios de base de datos	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Garantizar disponibilidad de las bases	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Ajuste de parámetros	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Administrador de servidores			
Gestión de usuarios (contraseñas, roles y perfiles)	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Planeación de mantenimiento	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Aplicación de parches	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Administrador de servidores virtuales y físicos	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Monitoreo de servidores	N A M S D	( ) Escuela ( ) Trabajo	( ) B ( ) I

		( ) Autoestudio ( ) Otro:_____	( ) A
Administrador de redes y seguridad			
Monitoreo de disponibilidad y tráfico de red	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Monitoreo de los puertos de seguridad	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Realizar bitácora de puertos de seguridad activados	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Administrador de usuarios			
Inventario de equipos asignados y en bodega	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Planeación de mantenimiento de equipos	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Bitácora de licenciamiento de software	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A
Gestión de cuentas de usuario (contraseñas, roles y perfiles)	N A M S D	( ) Escuela ( ) Trabajo ( ) Autoestudio ( ) Otro:_____	( ) B ( ) I ( ) A

Parte 3

1. Está capacitado para instalar:

____ Cables de red

____ Servidores Físicos y virtuales

____ Software cliente/servidor

____ Protocolos de seguridad

____Otro

2. ¿Tu puesto laboral requiere conocimiento de cómo programar o escribir un shell?

Sí ( ) No ( )

¿En qué lenguajes?

_____

3. ¿Comparte las obligaciones con alguna de las siguientes áreas?

____ Administrador de base de datos

____ Administrador de sistema operativo

____ Administrador de aplicaciones

____Administrador de redes

____Otro

4. ¿Qué sistemas operativos y versiones has usado en otros sistemas? (Ejemplo. AIX 7.1 SL2)

_____

5. ¿Está certificado como administrador de sistema? Sí ( ) No ( )

Si la respuesta es sí, indique que cursos o entrenamientos en los que está certificado.

---

6. ¿Cuáles consideras que son tus áreas de oportunidad para certificarte en seguridad de sistemas de información?

A._____

B._____

Comentarios Adicionales:

_____

El propósito de los resultados es conocer el nivel de concientización, experiencia y conocimiento que tiene el personal de la empresa en relación con la seguridad de la información según el departamento al que pertenezca.

Esta evaluación ayudara a tener una escala, de que personal necesita tener una capacitación desde un nivel básico, intermedio o avanzado según sus resultados.

Sí las preguntas abiertas de la sección 1 son contestadas en un 80% de forma negativa, esto nos indicará que el personal necesita un curso avanzado. Sí tiene un 50% como respuesta negativa, se considera que tiene un nivel intermedio de conocimiento sobre seguridad informática y necesita una capacitación complementaria. Si las respuestas negativas son nulas o con un 10% se considera que el personal tiene el conocimiento adecuado sobre este tema.

En cuanto a las preguntas de opción múltiple sólo se medirá el nivel de conocimiento en seguridad de acuerdo con el departamento que pertenezca cada persona para determinar su nivel de conocimiento en su área.

5.3 Propuesta de capacitación basada en el baseline.

5.3.1 Definición del plan de concientización.

Como parte del programa de concientización de nuestro baseline, consideramos que se pueden abordar una serie de conceptos básicos que conforman dicho baseline, buenas prácticas y comportamientos esperados del uso adecuado de los sistemas, en conjunto con los principales problemas y consecuencias que se pueden ocasionar por la falta de estos, a través de una campaña de difusión por medio de carteles informativos, trípticos y correos electrónicos que permiten reforzar de forma periódica dichos conceptos para todos los empleados que conforman la organización. Nuestra propuesta de temas a abordar son los siguientes:

- Importancia de la seguridad de la información a través del baseline-implicaciones de incumplimiento.
- Uso de contraseñas-creación de contraseñas seguras, periodos de cambio, protección y no difusión de las mismas.
- Ingeniería social.
- Correos no deseados/Spam.
- Respuesta de incidentes-¿Qué hacer?, ¿A quién contactar?
- Aseguramiento de ejecución de respaldos de información.

- Uso del Internet-sitios permitidos versus sitios no autorizados.
- Uso del equipo de cómputo y sistemas de información.
- Restricción del uso de licencias de software.
- Proteger la información sujeta a preocupaciones de confidencialidad.

5.3.2 Definición del plan de entrenamiento

Para nuestra propuesta de entrenamiento, consideramos como base los lineamientos propuestos por la guía NIST 800-50, para genera un esquema guía o plantilla que sirva a las organizaciones como referencia para generar y documentar un plan inicial de entrenamiento y concientización en seguridad para el personal de tecnologías de la información.

Primeramente, consideramos que es recomendable realizar una agrupación de los empleados que componen la organización y agruparlos en base en sus roles o puestos.

Con la finalidad de definir una propuesta de plan de entrenamiento de seguridad de información basado en nuestro baseline, agrupamos los roles definidos en nuestro organigrama base en 3 grupos principales para determinar un nivel de entrenamiento adecuado. A continuación, se describen estas 3 sugerencias de roles:

Rol 1- Personal / Staff TI: Todo el personal del área; es importante asegurarse de que todo el personal entienda el propósito detrás de las políticas de seguridad de la organización. Debido a que los datos de la organización se encontraran en riesgo ya sean medios electrónicos o no, es recomendable establecer formas básicas para proteger dichos datos, por ejemplo, procedimientos para el almacenamiento, la trasmisión y la eliminación de la información, tanto para datos en formatos físicos, así como electrónicos.

El personal debe estar consciente de los métodos más comunes por los cuales un tercero (hackers, defraudadores) puede obtener información mediante ingeniería social, y estar atentos a posibles engaños que permitan el acceso a la información de la organización sin hacer uso de métodos electrónicos.

Rol 2 – Administradores y/o Dueños de la Aplicación: Involucra a sub gerentes de actividades especializadas. Los Administradores de sistemas, bases de datos y de red y otros miembros del personal con acceso privilegiado a sistemas informáticos necesitarán un entrenamiento de seguridad más detallado y técnico que incluya las configuraciones seguras del sistema, basados en las recomendaciones establecidas por el baseline propuesto.

Para funciones especializadas, como las que apoyan sistemas y redes, debe tener presentes las configuraciones seguras recomendadas para los sistemas que usa la organización. Los desarrolladores de aplicaciones, los desarrolladores de sistemas y el personal de pruebas que tienen acceso al código deben ser conscientes de sus responsabilidades y de seguir la política de seguridad de la organización, las prácticas de codificación seguras y los procedimientos de control de cambios.

Rol 3 – Gerencia Y Dirección: Involucrará a directores y gerentes. La administración debe entender no sólo las pérdidas monetarias de no proteger la información que generan, sino también el daño que puede generarse a la organización en su reputación. La gerencia necesita entender los requisitos de seguridad lo suficiente para discutirlos y tomar las decisiones necesarias para reforzarlos, y así alentar al personal a cumplir con los requisitos y políticas de seguridad.

El plan de entrenamiento y concientización para el personal en general requiere que sea claramente entendido por todos, el material generado para preparar al personal debe ser los suficientemente claro para que sea comprendido de forma rápida, y no persistan los riesgos por mal tratamiento de los datos por la mala comprensión, por lo que hay que poner especial atención a los comentarios generados por el personal después de la aplicación y distribución de los materiales de entrenamiento.

5.3.3 Plantilla para el plan de entrenamiento.

Como parte de nuestra propuesta, consideramos llevar un registro del plan de entrenamiento que se desea implementar, para llevar un registro puntal de avance en la aplicación del o los planes de difusión y entrenamiento del personal en el tema de seguridad.

A continuación, describimos una plantilla que sirva de referencia para tal fin:

Plantilla de Plan de Entrenamiento y Concientización

Propósito: Detallar el propósito del plan de difusión o el programa de entrenamiento que se aplicara.

Objetivos: Definir los objetivos que se desean alcanzar con el plan actual, estos objetivos pueden ser determinados después de realizar la evaluación al personal sobre las actividades que desempeñan y su conocimiento sobre sus responsabilidades con la información con la que trabajan.

Entrenamiento y educación.

Plan de trabajo **Rol 1 - Personal / Staff TI:**

Objetivos de aprendizaje:

• *Descripción de los objetivos que se desean alcanzar para el personal involucrado en este rol.*

Actividades:

Calendario de actividades:

• *Generar un calendario que ayude a dirigir cada etapa del entrenamiento y/o campaña de concientización.*

Criterios de evaluación:

•*Definir un esquema de evaluación según el programa de entrenamiento definido para el grupo de entrenamiento.*

Plan de trabajo **Rol 2 - Administradores y/o Dueños de la Aplicación:**

Objetivos de aprendizaje:

• *Descripción de los objetivos que se desean alcanzar para el personal involucrado en este rol.*

Actividades:

Calendario de actividades:

• *Generar un calendario que ayude a dirigir cada etapa del entrenamiento y/o campaña de concientización.*

Criterios de evaluación:

•*Definir un esquema de evaluación según el programa de entrenamiento definido para el grupo de entrenamiento.*

Plan de trabajo **Rol 3 - Gerencia Y Dirección:**

Objetivos de aprendizaje:

• *Descripción de los objetivos que se desean alcanzar para el personal involucrado en este rol.*

Actividades:

Calendario de actividades:

• *Generar un calendario que ayude a dirigir cada etapa del entrenamiento y/o campaña de concientización.*

Criterios de evaluación:

•*Definir un esquema de evaluación según el programa de entrenamiento definido para el grupo de entrenamiento.*

Además, a continuación se incluye una propuesta de calendarización de las actividades a realizar de acuerdo al baseline y a la capacitación propuesta, de forma que su implementación y desarrollo puedan ser seguidos a detalle para detectar a tiempo áreas de oportunidad, tanto en las medidas aplicadas como en el personal que participa:

		MES 1								MES 2								MES 3	
FASE	**ACTIVIDADES**	**SEMANA 1**		**SEMANA 2**		**SEMANA 3**		**SEMANA 4**		**SEMANA 5**		**SEMANA 6**		**SEMANA 7**		**SEMANA 8**		**SEMANA 9**	
Preparación	Levantamiento de informacion																		
Preparación	Análisis de Resultados																		
Realización	Clasificación de grupos (bás, inter, avan)																		
Realización	Inicio de capacitación grupo básico																		
Realización	Capacitación al 4to nivel																		
Realización	Capacitación al 3er nivel																		
Realización	Capacitación al 2do nivel																		
Realización	Evaluación de capacitación																		
Realización	Inicio de capacitación grupo intermedio																		
Realización	Capacitación al 4to nivel																		
Realización	Capacitación al 3er nivel																		
Realización	Capacitación al 2do nivel																		
Realización	Evaluación de capacitación																		
Realización	Inicio de capacitación grupo avanzado																		
Realización	Capacitación al 4to nivel																		
Realización	Capacitación al 3er nivel																		
Realización	Capacitación al 2do nivel																		
Realización	Evaluación de capacitación																		
Finalización	Análisis de Resultado grupo básico																		
Finalización	Análisis de Resultado grupo intermedio																		
Finalización	Análisis de Resultado grupo avanzado																		

Conclusiones

Después de la revisión, análisis y acotamiento de las distintas normatividades que contemplamos para la realización del baseline para una empresa sin una estructura en seguridad de la información. Consideramos como una best practice o punto de partida, la ejecución de un programa de evaluación y seguimiento de las personas que conforman el área de informática en una organización, recalcando el aspecto de seguridad y continuidad del negocio.

El objetivo, como lo mencionamos desde un principio, es el de concientizar y familiarizar el aspecto de seguridad en las empresas en su área de informática, haciendo de su conocimiento, de manera general, las vulnerabilidades, riesgos y amenazas de las que puede verse afectada la parte más esencial que es la información.

Con este baseline determinaremos los conocimientos en el ramo de la seguridad de la información del personal que compone el área de TI. Aplicando el cuestionario propuesto que ayudará a la organización a categorizar el nivel de conocimiento de los tres niveles.

Una vez aplicadas las evaluaciones, la organización podrá determinar qué nivel de formación tienen sus empleados mediante una clasificación (básico, intermedio y avanzado), y así poder programar las capacitaciones adecuadas, para mitigar los riesgos y amenazas en las que se puede tener un control sobre las actividades básicas de seguridad de la información.

Con base en nuestro trabajo, tenemos la firme idea de que este puede complementarse con un área dedicada a la seguridad de la información. La cuál puede dar un panorama particular para cada área de TI personalizado o especializado y de acuerdo con las necesidades de cada área.

El llevar este baseline a un segundo nivel implicaría revisar y analizar nuevas normatividades de acuerdo con las áreas o requerimientos que se especifiquen por parte de la organización

Bibliografía

- **Carmen de Pablos Heredero, José Joaquín López-Hermoso Agius, Santiago Martín-Romo Romero, Sonia Medina Salgado. 2004**. Informática y comunicaciones de la empresa. Madrid, España. ESIC Editorial, 2004.
- **Hernández Sampieri, Roberto. 2014**. Metodología de la Investigación. (Sexta Edición). México, Distrito Federal: McGraw-Hill.
- **AMITI**, (2 julio, 2015). *El mercado de TIC representará el 5% del PIB hacia el 2015 con un valor de 35 mil millones de dólares en México,* recuperado el 6 de febrero de 2017, de amiti.org.mx/4004/el-mercado-de-tic-representara-el-5-del-pib-hacia-el-2015-con-un-valor-de-35-mil-millones-de-dolares-en-mexico
- **Centro de Documentación, Información y Análisis Dirección de Servicios de Investigación y Análisis Subdirección de Política Exterior** (2016), recuperado el 14 de febrero de 2017 de www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-12-06.pdf- .
- **Código Penal Federal** (2016), recuperado el 07 de febrero del 2017 de www.diputados.gob.mx/LeyesBiblio/pdf/9_180716.pdf
- **Deloitte** (2014). *Estudio Global 2014 de Riesgo Reputacional,* recuperado el 8 de febrero de 2017 de www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/riesgo-reputacional.html
- **El Economista** (19 noviembre, 2016). *14 datos sobre el comercio electrónico en México* recuperado el 8 de febrero de 2017, de eleconomista.com.mx/industrias/2016/11/19/14-datos-sobre-comercio-electronico-mexico
- **El Sol de México** (13 abril, 2016). *Empresas solo destinan 1% de su gasto a seguridad informática*, recuperado el 9 de febrero de 2017, de www.elsoldemexico.com.mx/finanzas/175299-empresas-solo-destinan-1-de-su-gasto-a-seguridad-informatica
- **Expansión** (27 julio, 2016). *Las estrategias de seguridad*, recuperado el 11 de febrero de 2017 de www.expansion.mx/empresas/2016/07/27/mas-mecanismos-de-seguridad-la-respuesta-empresarial-a-los-riesgos-en-mexico
- **Expansión** (16 septiembre, 2016). *México pierde 3,000 mdd al año en ciberataques*, recuperado el 11 de febrero de 2017, de www.expansion.mx/empresas/2016/09/14/israel-comparte-con-mexico-su-experiencia-contra-ciberataques
- **International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC). 2013.** *ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security management.* Suiza: ISO/IEC.

- **Legislación de Derecho Informático** (2016), recuperado el 07 de febrero de 2017 de www.informatica-juridica.com/legislacion/mexico/#toc-acceso-ilcito-a-sistemas-y-equipos-de-informtica
- **Mexican Business Web**, (5 marzo, 2016). *México registró más de 81 mil incidentes informáticos en 2015,* recuperado el 7 de febrero de 2017, de www.mexicanbusinessweb.mx/104369/mexico-registro-mas-de-81-mil-incidentes-informaticos-en-2015/
- **María del Consuelo Argüelles Arellano**, (2015), *Leyes vigentes en México para los programas de cómputo, las bases de datos y su documentación,* recuperado el 7 de febrero de 2017 de www.scielo.org.mx/pdf/cys/v18n2/v18n2a15.pdf.
- **Normateca Federal** (2017), *MAAGTICSI,* recuperado el 7 de febrero de 2017 de www.maagtic.gob.mx
- **Ponemon Institute LLC**, (2016). *2016 Cost of Data Breach Study: Global Analysis,* recuperado el 10 de febrero de 2017, de public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094wwen/SEL03094WWEN.PDF
- **Parraguez K., Luisa** (2017), *The State of Cybersecurity in Mexico: An Overview*, recuperado el 8 de febrero de 2017 de //www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf

Glosario

- **COBIT 5.0 for Information Security:** guía para ayudar a profesionales enfocados en el área de TICS a entender, utilizar, implementar y gestionar actividades relacionadas con la seguridad de la información, así como ayudar en la toma de mejores de decisiones manteniendo conciencia sobre tecnologías emergentes y las amenazas que las acompañan.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Integridad:** Propiedad de la información que se encuentra conformada por su exactitud y completitud.
- **ISO/IEC 27001:2013:** Estándares de seguridad que contienen las mejores prácticas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).
- **Proceso:** Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Seguridad de la Información**: Preservación de la confidencialidad, integridad y disponibilidad de la información.