Universidad Autónoma de Querétaro
Facultad de Informática
Especialidad En Maestría en Sistemas de Información

Metodología para la implementación de seguridad en TI de una organización en el Estado de Querétaro

Opción de titulación
Tesis o Publicación de artículos

Que como parte de los requisitos para obtener el Grado de
Maestría en Sistemas de Información

Presenta:
L.I. José Alejandro Vargas Díaz

Dirigido por:
MISD. Carlos Alberto Olmos Trejo

MISD.Carlos Alberto Olmos Trejo
Presidente — Firma

MISD.Juan Salvador Hernández Valerio
Secretario — Firma

MISD.Jesús Armando Rincones
Vocal — Firma

M.S.I.Gabriela Xicoténcatl Ramírez
Suplente — Firma

M.S.I. Sandra Patricia Arreguín Rico
Suplente — Firma

M.I.S.D. Juan Salvador Hernández Valerio
Director de la Facultad

Dr. Ma. Guadalupe Flavia Loarca Piña
Director de Investigación y Posgrado

Centro Universitario
Querétaro, Qro. Mayo 2016

RESUMEN

Las tecnologías de información han provocado cambios en nuestra sociedad por lo cual es indudable su influencia en el crecimiento tecnológico que vivimos. Las TICS facilitaron el desarrollo de internet, desde la generación y almacenamiento de grandes cantidades de información, hasta la capacidad de enlazar lugares alejados entre sí generando una comunicación casi en tiempo real. Los cambios sociales y culturales generados por rápida adaptación de las TICS en nuestra vida cotidiana han dificultado el entendimiento de las responsabilidades y riesgos de su uso inconsciente, y la regulación de las TICS en el ámbito jurídico ha sido lento en comparación al crecimiento tecnológico derivando en diversos agujeros en la legislación con los denominados delitos informáticos. A nivel mundial constituye un reto el actualizar la legislación referente a delitos informáticos y hacer frente a las amenazas internas y externas. La poca legislación referente a delitos informáticos y un casi nulo conocimiento de los riesgos de seguridad informática han convertido a México en un blanco fácil de ataques cibernéticos de los denominados hackers donde el sector más afectado son las pymes, estos ataques pueden dañar sus datos, sistemas, y sobre todo, sus actividades. En el presente trabajo se analizan diferentes estándares internacionales, metodologías, técnicas y herramientas para realizar la comprobación de la seguridad, en apego a la legislación vigente de los Estados Unidos Mexicanos. Esto con el objetivo de generar una metodología enfocada a la comprobación de la seguridad. La metodología propuesta se compone de dos ejes, el primero orientado a describir todos los elementos susceptibles dentro de una organización y el segundo a la herramienta que ayuda a auditar la seguridad de la organización.

(Palabras clave: Delitos Informáticos, Seguridad en Redes, Pentesting, Hacking, Seguridad Informática.)

ABSTRACT

Information Technologies have caused changes in our society, for which their influence in the technological growth we live is indubitable. ICTs enabled the development of the internet, from the generation and storage of great quantities of information, to the ability to link separate places generating communication in almost real-time. Social and cultural changes generated by a fast adaptation of ICTs on our daily lives have hindered the understanding of responsibilities and risks of their misuse, and ICTs regulation in the legal field has been slow compared to the technological growth causing diverse holes in the legislation with the so-called informatic crimes. On a world-wide level, it's a challenge to update the legislation regarding to informatic crimes and dealing with internal and external threats. Little legislation regarding to informatic crimes and an almost null knowledge of Information Security risks have turned México an easy target for informatic crimes from so-called hackers where the most affected sector are SMEs, this attacks can damage their data, systems, and above all, their activities. On the present assignment, different international standards, methodologies, techniques and tools to perform security checks are analyzed, according to the current legislation of Estados Unidos Mexicanos. This is with the purpose of generating a methodology focused on security check. The methodology proposal is composed of two axis, the first one focused on describing all the elements that are suceptible within an organization, and the second one to the tool that helps audit the security of the organization.

(**Keywords:** Informatic Crime, Network Security, Pentesting, Hacking, Information Security)

DEDICATORIA

A mis padres, por el apoyo incondicional brindado siempre, por motivarme a cumplir mis metas y por el cariño y comprensión mostrada en todo momento.

A mis hermanos, por ejemplo de esfuerzo que siempre he tenido de ellos, por su ayuda al debatir algunos temas y darme su punto de vista.

A mis Tíos, por los ánimos de seguir adelante y motivarme a continuar adelante.

A mi familia en general por estar al pendiente de mí y mi desarrollo profesional.

A mis amigos por el apoyo brindado a lo largo de estos años, por motivarme a terminar y por su apoyo moral e incondicional que siempre demuestran hacia mi persona.

AGRADECIMIENTOS

Al MISD. Carlos Alberto Olmos Trejo por el apoyo, paciencia y orientación en el desarrollo de este trabajo, por ser un soporte y encontrar un punto de vista distinto al mío que siempre ayudo a replantear ideas y mejorar la investigación, y sobre todo por ser un compañero de vida y de trabajo.

A la M. en C. Ruth Angélica Rico Hernández por darme la oportunidad de formar parte de su equipo de trabajo, por la confianza y el apoyo en mi desarrollo profesional.

Al MISD. Juan Salvador Hernández Valerio por su apoyo y fomentar constantemente mi crecimiento personal y académico.

A la M.S.I. Gabriela Xicoténcatl Ramírez por su apoyo incondicional en el desarrollo de este trabajo, por la orientación y consejos para mejorarlo.

A la M.S.I. Sandra Patricia Arreguín Rico por la actitud positiva y los ánimos a continuar con este trabajo.

Al M.S.I. Eduardo Aguirre Caracheo y al I.S. Diego Octavio Ibarra Corona por su apoyo condicional siempre, por su colaboración en el desarrollo de esta investigación.

A mis maestros por compartir sus puntos de vista y conocimientos conmigo.

A mis hijos académicos por su apoyo constante e incondicional, por su motivación a seguir creciendo profesionalmente y por permitirme presentar mis ideas con ustedes y ser críticos con mi trabajo.

TABLA DE CONTENIDOS

INDICE DE FIGURAS

1. INTRODUCCIÓN

El uso de las tecnologías de información y comunicaciones TICS ha llevado a la sociedad a una serie de cambios importantes en su quehacer y su comportamiento. La velocidad con que se ha ido implementando en cada aspecto de la vida cotidiana conlleva que el proceso de adaptación de las personas sea rápido y desmesurado lo que implica la dificultad de entender o estudiar los efectos de estos que modifican el comportamiento del ser humano. Es decir la sociedad se desarrolla dentro de un contexto de cambios constantes y rápidos acorde a tendencias globales, que llevan a una evolución que no siempre impacta de forma positiva ya que al ser tan corto el tiempo de implementación el proceso de conciencia y entendimiento de dicha tecnología no se lleva adecuadamente.

Es importante no solo pensar en el uso de las TICS en términos de innovación y bienestar social, sino que también se debe considerar las consecuencias negativas que pueden derivarse de su uso y, por ende, detectar en donde se necesitan tomar acciones específicas para la regulación del comportamiento o las conductas sociales, esto con la finalidad de buscar la orientación a hacia el respeto de los derechos y libertades de los terceros.

Un efecto negativo relacionado a este ritmo constante de cambios y adaptación a las TICS son los denominados delitos informáticos los cuales presentan el reto de su prevención, detección y legislación. La rapidez con la que crecen los medios informáticos y la globalización de estos genera preocupación e incertidumbre sobre el actuar para la prevención de ellos.

En la actualidad el uso de las Tecnologías información respaldan la forma en que vivimos, dependemos de ellas a tal grado que en todo momento son requeridas en nuestra vida cotidiana. El uso de estas tecnologías nos permiten crear un activo muy valioso en nuestra sociedad llamado información, una gran cantidad de conocimientos y usos pueden obtenerse y es por eso que es relevante tener un control sobre los mismos. El uso que puedan dar a información robada terceras personas, implica un riesgo para los propietarios de ella.

Por ello, el proteger la información es proteger la organización, y para ello es necesario tener una guía de implementación de seguridad tal como cualquier otro proceso productivo de la organización.

Existe una variedad de delitos que pueden cometerse, en este caso se contempla el uso de las tecnologías de información para cometerlos y donde casi cualquier individuo podría cometer un delito al obtener, modificar o eliminar información sin la autorización de su propietario o infringir la privacidad de personas tanto físicas como morales.

Hoy en día la crisis económica ha tenido graves consecuencias en el sector empresarial de México, en épocas de crisis las empresas intentan reducir gastos y esta medida que en un principio parece correcta, puede acarrear graves consecuencias. Si la reducción de gastos no se realiza de manera planeada, se corre el riesgo que parte de esta reducción de gasto se realice en detrimento de los mecanismos de control interno, en consecuencia, se reduce la capacidad de las empresas de prevenir y detectar irregularidades que eventualmente se conviertan en fraudes o pérdida de información vital (KPMG, 2010).

Es común ver titulares en medios electrónicos haciendo referencia a los delitos electrónicos en América latina y en México pero que contrastan con los datos oficiales del gobierno Mexicano.

Figura 1-1 Titulares de medios de noticias sobre delitos informáticos.

SEGURIDAD | NOTICIAS | 14 JUL 2014

Una de cada cinco empresas en el mundo ha sufrido un ataque APT

Tags: Seguridad Tendencias

También te puede interesar:

- El mercado europeo de appliances de seguridad se estanca en 2014

El 21 por ciento de las empresas de todo el mundo ha sufrido una amenaza persistente avanzada (APT). Esta ciberamenaza avanzada se describe como un ataque sigiloso, incesante, enfocado a objetivos determinados y con un propósito fundamental: extraer información de las empresas.

REFORMA

Se olvidan empresas de ciberseguridad

CNN EXPANSIÓN

México, 'en pañales' en ciberseguridad

Sólo 19% de las empresas tienen programas de seguridad informática, contra 40% a nivel global; una firma afectada paga hasta 20,000 dólares para corregir daños informáticos, dice Ernst & Young.

Aumentan 300% incidentes de seguridad cibernética en México

Domingo, 31 de agosto de 2014 - 2:06 pm

MÉXICO, D.F. (Notimex).- Datos preliminares para este año señalan un aumento de 300 por ciento en incidentes de seguridad cibernética en México, informó Symantec en su reporte de Tendencias de Seguridad Cibernética en América Latina y el Caribe.

Figura 1-2 Datos oficiales sobre delitos informáticos en México. Fuente: Consulta delitos informáticos Sistema Infomex.

PGR

Subprocuraduría Jurídica y de Asuntos Internacionales
Dirección General de Asuntos Jurídicos

Oficio: SJAI/DGAJ/09226/2014
Asunto: *Entrega de información por medio electrónico*
"2014. Año de Octavio Paz"

Anexo I

CANTIDAD DE AVERIGUACIONES PREVIAS INICIADAS EN EL FUERO FEDERAL POR DELITOS DE ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA*
DEL 1° DE ENERO DE 2012 AL 31 DE JULIO DE 2014

Entidad	Cantidad	Entidad	Cantidad
Aguascalientes	0	Nayarit	0
Baja California	6	Nuevo León	1
Baja California Sur	0	Oaxaca	3
Campeche	0	Puebla	1
Chiapas	1	Querétaro	0
Chihuahua	1	Quintana Roo	1
Coahuila	1	San Luis Potosí	1
Colima	0	Sinaloa	1
Distrito Federal	94	Sonora	5
Durango	0	Tabasco	0
Guanajuato	5	Tamaulipas	8
Guerrero	2	Tlaxcala	1
Hidalgo	2	Veracruz	3
Jalisco	3	Yucatán	0
México	5	Zacatecas	0
Michoacán	4	Áreas Centrales	8
Morelos	0	Total	157

*Previsto en el Título Noveno, Capítulo II, artículos 211 bis 1 al 211 bis 7, del Código Penal Federal.
El sistema estadístico no puede hacer una desagregación geográfica del trabajo de las Áreas Centrales.
Cifras preliminares.
Fuente: Sistema Institucional de Información Estadística (SIIE).

Río Guadiana 31, Planta Baja, Col. Cuauhtémoc, Del. Cuauhtémoc, México, DF, 06500
t. +52 (55) 5346 0000 | Exts. 5716 y 5717 www.pgr.gob.mx

En México el 75 por ciento de las Pymes, aproximadamente dos millones 500 mil de esas empresas, no cuenta con algún servicio de seguridad informática (El financiero, 2011).

Según los datos de la policía federal en su coordinación para la prevención de delitos electrónicos, desde mayo del 2010 al año 2013 se han atendido 3971 casos de investigación referente a delitos informáticos, de los cuales 258 fueron del 2010, 723 del 2011, 1331 del 2012 y 1479 del 2013, es evidente que el número de casos ha ido incrementando cada año sin contemplar el número de casos que no son denunciados.

Figura 1-3 Denuncias ciudadanas delitos informáticos 2013. Fuente: Elaboración propia

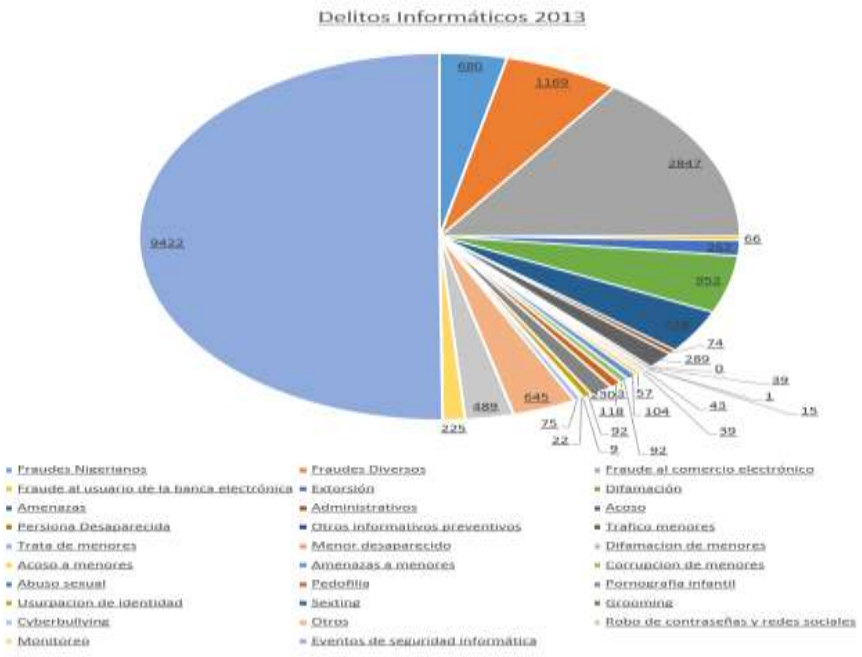

Figura 1.4 Denuncias ciudadanas delitos informáticos 2012. Fuente: Elaboración propia

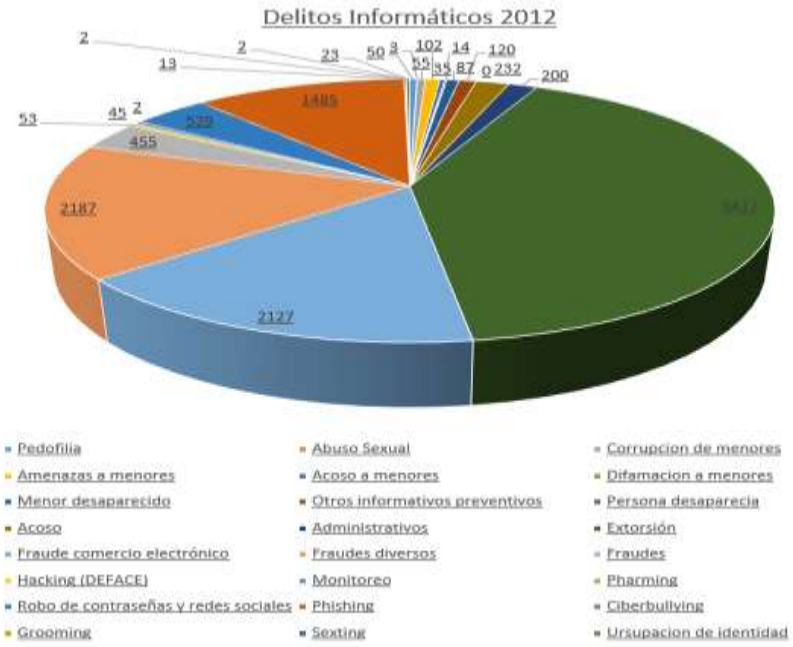

Figura 1.5 Denuncias ciudadanas delitos informáticos 2011. Fuente: Elaboración propia.

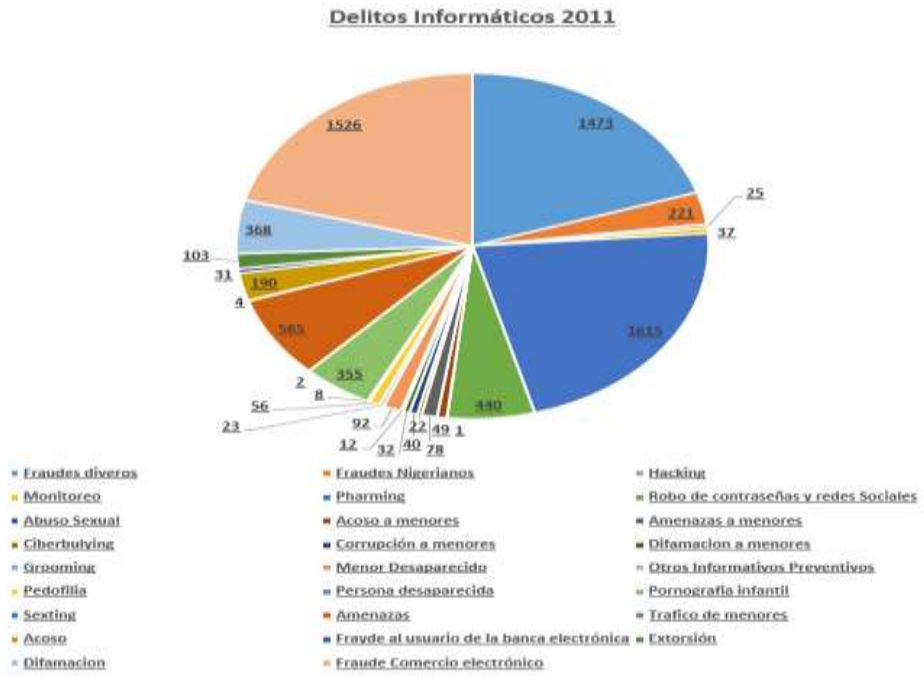

Figura 1.6 Investigaciones atendidas sobre delitos informáticos. Fuente: Elaboración propia

Año	Investigaciones Atendidas
2010	258
2011	723
2012	1331
2013	1479
Total	3791

Dada la importancia de la seguridad en los sistemas de información, algunas organizaciones han creado metodologías buscando encontrar una solución a la identificación de vulnerabilidades y la de brindar los mecanismos óptimos para facilitar su corrección. El problema con estas metodologías es la dificultad de adaptación en diferentes sectores, requerimientos para su implementación y legislaciones de diversas áreas geográficas que no se adaptan a la legislación de donde fueron creadas.

En el presente trabajo se realizó la investigación bibliográfica, tendencias de seguridad informática a nivel mundial, marco legal existente a nivel global y local así como el uso de información estadística sobre Delitos informáticos proporcionada por **SISTEMA INFOMEX** de Gobierno Federal Mexicano (quien actualmente recibe y contesta solicitudes referentes al acceso a la información pública) en la búsqueda de la creación de una metodología que permita ser guía en la implementación de seguridad en una pyme y como consecuencia en la verificación de la seguridad para tomar acción con medidas para su mejora.

Dentro del presente trabajo de investigación se busca comprobar la siguiente hipótesis: “Actualmente las empresas Queretanas no saben qué tan segura esta su información y como hacer uso de la tecnología para protegerla, o en su defecto conocen los riesgos pero desconocen cómo prevenirlos debido a la falta de metodologías de seguridad que se adapten a su entorno”, siguiendo el objetivo general de desarrollar una metodología que apoye al administrador de TI en la implementación de la seguridad informática, utilizando una serie de procesos y

pruebas propuestas para facilitar la detección de sectores de oportunidad, mejorar y equilibrar la seguridad en todas las áreas de la organización, todo esto en relación con las siguientes actividades:

- Realizar un análisis de tendencias de necesidades específicas respecto a seguridad de sistemas de información del entorno (Querétaro, México).
- Realizar un análisis de las metodologías existentes de seguridad informática.
- Recopilar la información de la actual legislación con referencia a seguridad y delitos informáticos en México.
- Realizar un análisis de bases de datos de vulnerabilidades conocidas.
- Generar un esquema de procesos divididos por áreas de acción y facilitar la medición del nivel de seguridad actual.
- Elaboración de métodos que ayuden a prevenir y evitar posibles fallas de seguridad.

2. SEGURIDAD INFORMATICA

Según la Real Academia de la Lengua la seguridad es la cualidad de seguro, es decir de estar libre y exento de cualquier daño, peligro o riesgo. En informática, como en otros aspectos de la vida, la seguridad entendida según la definición anterior, es prácticamente imposible de conseguir, por lo que se ha relajado y se tiende más al concepto de fiabilidad; se entiende un sistema seguro como aquel que se comporta como se espera de él.

2.1 ¿Qué es seguridad?

La seguridad se define como un conjunto de medidas de prevención, detección y corrección orientadas a proteger la confidencialidad, integridad y disponibilidad de los recursos informáticos (Pacheco, 2009).

Para la aplicación de la seguridad se puede usar un modelo definido donde se contemplen varios niveles tales como (Pacheco, 2009):

- Políticas, procedimientos y concientización.
- Seguridad física.
- Seguridad del perímetro.
- Seguridad de la red.
- Seguridad del equipo.
- Seguridad de las aplicaciones.
- Seguridad de los datos.

2.2 ¿Qué es un sistema de información?

Un sistema de información puede definirse como un conjunto de componentes que permiten capturar, procesar, almacenar, y distribuir la información para apoyar la toma de decisiones y el control en una institución. Además, para apoyar a la toma de decisiones, los sistemas de información pueden ayudar a los administradores y al personal, a analizar problemas, visualizar cosas complejas y crear nuevos productos (C. Laudon Kenneth, 1997).

- Un sistema de información está compuesto por 3 elementos básicos:
- La alimentación o entradas.
- El procesamiento.
- El producto o salida.

La alimentación consiste en la captura o recolección de datos primarios dentro de la institución o de su entorno para procesarlos en un sistema de información (C. Laudon Kenneth, 1997)

El procesamiento es la conversión del insumo en forma que sea más comprensible para los seres humanos (C. Laudon Kenneth, 1997)

Producto o salida es la distribución de información procesada a las personas o en las actividades en donde será usada (C. Laudon Kenneth, 1997).

2.3 Análisis de seguridad

Los conceptos y variables importantes y presentes en cualquier tipo de análisis de seguridad son (Sallis E., 2010):

- Posicionamiento.
- Visibilidad.
- Perfil Adoptado.

2.3.1 Posicionamiento

El primer punto para tener en cuenta es definir el posicionamiento desde donde se llevará a cabo el análisis de seguridad. Los posicionamientos pueden variar según lo que se desee obtenerse como resultado (Sallis E., 2010).

Generalmente pueden ser los siguientes:

- Posicionamiento externo.
- Posicionamiento interno.

El riesgo más importante es que el hecho de seleccionar un posicionamiento erróneo para el test hará que los resultados no sean los esperados, independientemente de que el análisis de seguridad haya sido llevado a cabo de manera perfecta (Sallis E., 2010).

Es importante tomar en consideración que la superficie del ataque nos indica cuán grande o pequeña es la porción de un sistema de información que, desde la posición y con la visibilidad que tenemos, tiene la probabilidad de ser explotada; por lo que mientras más superficie, mayor probabilidad de asestar un golpe exitoso, pero también podría suceder que en una pequeña superficie y en las

peores condiciones de visibilidad se logre concretar una intrusión exitosa (Sallis E., 2010).

2.3.2 Visibilidad

En este concepto se contempla cual será la información que se nos brindará previo al inicio del análisis sobre los sistemas de información que serán objetivos. Esta información definirá, entre otras cosas, qué etapas estarán presentes en un análisis de seguridad, en cuales de las etapas presentes se deberá poner mayor esfuerzo y otros aspectos relacionados (Sallis E., 2010).

Al igual que el posicionamiento, la visibilidad también define los resultados del análisis. Entonces antes de tomar la decisión sobre la visibilidad debemos preguntarnos ¿me interesa saber qué puede ver o hacer sobre mis sistemas de información alguien externo a la empresa que no tenga conocimientos alguno sobre de estos? o ¿me interesa saber qué puede ver o hacer alguien desde el interior, con un conocimiento avanzado sobre mis sistemas de información?, este tipo de preguntas son algunas de las variables que definen la visibilidad (Sallis E., 2010).

2.3.3 Perfil Adoptado

Podemos identificar la posición de los atacantes ubicándolos en el exterior de la organización o bien en el interior. Podemos también categorizar aquellos incidentes de seguridad que surgen sobre la base de firme convicción del atacante, o bien aquellos que surgen sobre la base de un error u omisión por parte de un usuario no intencionado, pero lamentablemente no se pueden definir categorías estáticas debido a que el comportamiento o los perfiles son sutilmente diferentes según la combinación de múltiples variables (Sallis E., 2010).

Durante el análisis de seguridad, se combinara además del conocimiento relacionado al objetivo y la posición, algunas variables emulando diferentes tipos de perfiles, como por ejemplo:

- Usuario sin privilegios.
- Usuario con privilegios.
- Tercero ajeno a la organización con acceso físico a la misma.
- Tercero ajeno a la organización sin acceso físico a la misma.
- Usuario con conocimiento técnico avanzado.
- Usuario con conocimiento técnico medio.
- Usuario con conocimiento técnico básico.
- Otros.

2.4 ¿Qué son las pruebas de penetración?

También conocidos como test de intrusión, son el tipo de análisis que da lugar a la realización de tareas asociadas a la explotación y pos-explotación de vulnerabilidades. Este tipo de análisis de seguridad se caracteriza por tener un objetivo definido, que finaliza cuando el mismo es alcanzado o el tiempo pautado para el desarrollo del análisis se agota (Sallis E., 2010).

Es un tipo de análisis de seguridad que no solo trata de identificar e informar las debilidades, sino que también intenta explotarlas, a fin de verificar eficientemente los niveles de intrusión a los que se expone el sistema de información analizado (Sallis E., 2010).

Una prueba de penetración ayuda a detectar y luego a tomar medidas para salvaguardar a la organización contra posibles fallas, intencionales o no, y obtener resultados benéficos (Pacheco, 2009).

Desde una perspectiva operativa, ayuda a darle forma a una estrategia de seguridad informática identificando vulnerabilidades y cuantificando el impacto de ellas. Esto nos brinda una serie de indicadores que nos permiten gestionarla de manera proactiva, así podremos calcular un presupuesto destinado a las medidas que requieren algún tipo de corrección, y prever o plantear futuras inversiones en seguridad (Pacheco, 2009).

Revisar las técnicas y habilidades de los intrusos es mirar hacia nuestra infraestructura de cómputo y comunicaciones para revisar si ha visto lo mismo que los intrusos han visto y de esta manera corregirlo (Cano, 2009).

3. LEGISLACION REFERENTE A DELITOS INFORMATICOS

Un código penal es un conjunto unitario, ordenado y sistematizado de las normas jurídicas punitivas de un Estado (Téllez, 2009). A nivel internacional la Organización de las Naciones Unidas, reconoce como delitos informáticos las siguientes conductas:

1. Fraudes cometidos mediante manipulación de computadoras:

- Manipulación de los datos de entrada.
- Manipulación de programas.
- Manipulación de datos de salida.
- Fraude efectuado por manipulación informática.

2. Falsificaciones informáticas:

- Utilizando sistemas informáticos como objetos.
- Utilizando sistemas informáticos como instrumentos.

3. Daños o modificaciones de programas o datos computarizados:

- Sabotaje informático.
- Virus.
- Gusanos.
- Bomba lógica o cronológica.
- Acceso no autorizado a sistemas o servicios.
- Piratas informáticos o hackers.

- Reproducción no autorizada de programas informáticos con protección legal.

En México se cuenta con un Código Penal Federal que aplica todos los delitos del orden federal y de un Código Penal individual para los delitos cometidos en cada uno de los estados que conforman la República Mexicana. A continuación se describen todos los artículos relacionados únicamente con delitos informáticos tipificados en el Código Penal de la República Mexicana y los Códigos Penales de los Estados que la conforman.

Código Penal Federal:

Artículo 211 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 impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 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 impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 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 impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 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 el sistema financiero, protegidos por algún mecanismo de

seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa (…).

Código Penal para el Estado de Aguascalientes.

En relación a delitos de querella.

Artículo 23.- Los delitos que se perseguirán por querella o a petición de parte legítimamente ofendida, son los siguientes:

XXVI.- Acceso sin autorización y daño informático, previstos en los artículos 223, 224, 225 y 226.

Artículo 223.- El Acceso sin autorización consiste en interceptar, interferir, recibir, usar o ingresar por cualquier medio sin la autorización debida o excediendo la que se tenga a un sistema de red de computadoras, un soporte lógico de programas de software o base de datos.

Artículo 224.- El Daño Informático consiste en la indebida destrucción o deterioro parcial o total de programas, archivos, bases de datos o cualquier otro elemento intangible contenido en sistemas o redes de computadoras, soportes lógicos o cualquier medio magnético.

Artículo 225.- Cuando el Acceso sin Autorización o el Daño Informático se cometan culposamente se sancionarán con penas de 1 mes a 3 años de prisión y de 50 a 250 días multa.

Artículo 226.- La Falsificación Informática consiste en la indebida modificación, alteración o imitación de los originales de cualquier dato, archivo o elemento intangible contenido en sistema de redes de computadoras, base de datos, soporte lógico o programas.

Artículos referentes a la conducta culposa se tienen:

Artículo 8º.- La conducta puede ser de acción u omisión.

La conducta de acción u omisión puede ser:

II.- Culposa: si el que la ejecuta, causa un resultado típico, incumpliendo un deber de cuidado que debía y podía observar según las circunstancias del hecho y sus condiciones personales.

Código Penal para el Estado de Baja California:

Artículo 175.- Tipo y punibilidad.- Al que sin consentimiento de quien tenga derecho a otorgarlo revele un secreto, de carácter científico, industrial o comercial, o lo obtenga a través de medios electrónicos o computacionales, se le haya confiado, conoce o ha recibido con motivo de su empleo o profesión y obtenga provecho propio o ajeno se le impondrá prisión de uno a tres años y hasta cincuenta días multa, y en su caso, suspensión de dos meses a un año en el ejercicio de su

profesión; si de la revelación del secreto resulta algún perjuicio para alguien, la pena aumentará hasta una mitad más.

Al receptor que se beneficie con la revelación del secreto se le impondrá de uno a tres años de prisión y hasta cien días multa.

Revelación del secreto: Se entiende por revelación de secreto cualquier información propia de una fuente científica, industrial o comercial donde se generó, que sea transmitida a otra persona física o moral ajena a la fuente.

Querella: El delito de revelación de secreto se perseguirá por querella de la persona afectada o de su representante legal.

Artículo 175 bis.- A quien sin autorización o indebidamente, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán (…).

Artículo 175 ter.- A quien sin autorización o indebidamente, copie o accese a información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán (…).

Artículo 175 quater.- Agravación de la pena.- Las penas previstas en los artículos anteriores se duplicarán cuando las conductas delictivas se ejecuten en contra de sistemas o equipos de informática del Estado o Municipios. (…).

Código Penal para el Estado de Baja California Sur

Artículo 195.-

III.- Acceda ilegalmente a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.

IV.- Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como información sustraída, de esta forma.

En el dos mil diez se aprobó esta reforma al código penal del Estado mencionado, es necesario hacer notar, que antes de esto, dicho Estado no consideraba en su legislación nada con respecto a los delitos informáticos (ni como medio ni como fin), a pesar de que se hace mención exclusivamente a cuestiones de tarjetas, no debe de dejarse a un lado la importancia de que haya mención ya al respecto.

Código Penal de Coahuila

Artículo 281 BIS. SANCIONES Y FIGURAS TÍPICAS DE LOS DELITOS CONTRA LA SEGURIDAD EN LOS MEDIOS INFORMÁTICOS COMETIDOS EN PERJUICIO DE PARTICULARES. Se aplicará prisión de tres meses a tres años y multa a quien:

I. Sin autorización para acceder a un sistema informático y con perjuicio de otro, conozca, copie, imprima, use, revele, transmita, o se apodere de datos o información reservados, contenidos en el mismo.

II. Con autorización para acceder a un sistema informático y con perjuicio de otro, obtenga, sustraiga, divulgue o se apropie de datos o información reservados en él contenidos.

Si la conducta que en uno u otro caso se realiza es con el ánimo de alterar, dañar, borrar, destruir o de cualquier otra manera provocar la pérdida de datos o información contenidos en el sistema, la sanción será de cuatro meses a cuatro años de prisión y multa.

Artículo 281 BIS 2. SANCIONES Y FIGURAS TÍPICAS DE LOS DELITOS CONTRA LA SEGURIDAD EN LOS MEDIOS INFORMÁTICOS COMETIDOS

EN PERJUICIO DE UNA ENTIDAD PÚBLICA. Se aplicará prisión de seis meses a seis años y multa a quien:

I. Sin autorización, acceda, por cualquier medio a un sistema informático, de una entidad pública de las mencionadas en el párrafo segundo del artículo 194, para conocer, copiar, imprimir, usar, revelar, transmitir o apropiarse de sus datos o información propios o relacionados con la institución.

II. Con autorización para acceder al sistema informático de una entidad pública de las mencionadas en el párrafo segundo del artículo 194, indebidamente copie, transmita, imprima, obtenga sustraiga, utilice divulgue o se apropie de datos o información propios o relacionados con la institución.

Si la conducta que en uno u otro caso se realiza, tiene la intención dolosa de alterar, dañar, borrar, destruir, o de cualquier otra forma provocar la pérdida de los datos o información contenidos en el sistema informático de la entidad pública, la sanción será de uno a ocho años de prisión y multa.

Si el sujeto activo del delito es servidor público, se le sancionará, además, con la destitución del empleo, cargo o comisión e inhabilitación para ejercer otro hasta por seis años.

Artículo 281 BIS 4. NORMA COMPLEMENTARIA EN ORDEN A LA TERMINOLOGIA PROPIA DE LOS DELITOS CONTRA LA SEGURIDAD DE LOS MEDIOS INFORMATICOS. A los fines del presente capítulo, se entiende por:

I. Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos

para generar, enviar, recibir, recuperar, procesar o almacenar información de cualquier forma o por cualquier medio.

II. Dato informático o información: toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático.

Código Penal para el Estado Libre y Soberano de Chiapas

Delito fraude contemplado en el Capítulo V:

Artículo 304:

XXIV.- Al que para obtener algún beneficio para sí o para un tercero, por cualquier medio acceda, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución.

Artículo 439.- Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema de seguridad o al que no tenga derecho a accesar, se le impondrá una sanción de uno a cuatro años de prisión y de cuarenta a doscientos días multa.

Al que, estando autorizado o tenga derecho de acceso a los sistemas o equipo de informática protegido por algún mecanismo o sistema de seguridad, innecesariamente o en perjuicio de otro destruya, modifique, o provoque pérdida de información que contengan los mismos, la pena prevista en el párrafo anterior, se aumentará en una mitad.

Artículo 440.- Al que, sin autorización accese, modifique, copie, destruya o provoque pérdida de información contenida en sistema o equipo de informática de

alguna dependencia pública protegida por algún sistema o mecanismo de seguridad se le impondrá una sanción de dos a seis años de prisión y de doscientos a seiscientos días de multa.

Artículo 441.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, innecesariamente o en perjuicio de otro o del servicio público modifique, destruya o provoque pérdida de información que contengan se impondrá prisión de tres a ocho años y de trescientos a ochocientos días multa.

Artículo 442.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, sin autorización copie, transmita o imprima información que contengan se le impondrá (…).

Código Penal para el Estado de Chihuahua

Artículo 185:

I. Quien produzca, fije, grabe, videograbe, fotografié o filme de cualquier forma imágenes o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explicitas o no, reales o simuladas.

II. Quien reproduzca, publique, publicite, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explicitas o no, reales o simuladas.

III. Quien ofrezca, posea o almacene intencionalmente para cualquier fin, imágenes o la voz de personas menores de edad o de personas que no tengan la

capacidad de comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explicitas o no, reales o simuladas.

Artículo 238. Se aplicará prisión de seis meses a seis años al que deteriore o destruya expediente o documento, de oficina o archivos públicos. Las mismas penas se aplicaran al que destruya, altere o provoque perdida de información contenida en sistema o equipo de informática de oficina o archivos públicos, protegidos por algún mecanismo de seguridad.

Artículo 326. A quien abra o intercepte una comunicación escrita que no esté dirigida a él, se le impondrá (…).

Los delitos previstos en este artículo se perseguirán por querella.

La misma sanción se impondrá en los casos en que la comunicación se encuentre registrada o archivada en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

Código Penal para el Estado de Colima

Artículo 10.- Se califican como delitos graves, para todos los efectos legales, por afectar de manera importante valores fundamentales de la sociedad, los siguientes delitos previstos por este Código:

Corrupción de menores en su modalidad de procurar o facilitar de cualquier forma el consumo de algún tipo de estupefaciente, psicotrópico o vegetales que determine la Ley General de Salud, como ilegales, a un menor o de quien no tenga capacidad para comprender el significado del hecho, tipificado por el segundo párrafo del artículo 155; así como en su modalidad de explotación pornográfica, prevista por el artículo 157 Bis, segundo párrafo, tratándose de la realización de acto de exhibicionismo corporal lascivo o sexual, con el objeto de videograbarlo, fotografiarlo o exhibirlo mediante anuncio impreso o electrónico.

Artículo 157 bis.- Al que explote a un menor o a quien no tenga capacidad para comprender el significado del hecho, con fines de lucro o para conseguir una satisfacción de cualquier naturaleza, se le impondrá (…).

Para los efectos de este artículo se tipifica como explotación de menor o de quien no tenga capacidad para comprender el significado del hecho, el permitir, inducir u obligar al sujeto pasivo, a la práctica de la mendicidad, o a realizar acto de exhibicionismo corporal, libidinoso o de naturaleza sexual, con el objeto de videograbarlo o fotografiarlo o exhibirlo mediante cualquier tipo de impreso o medio electrónico.

Artículo 234.- Se considera fraude y se impondrá pena de uno a nueve años de prisión y multa hasta por 100 unidades, para el caso de las fracciones I y II, y de tres a nueva años de prisión y multa hasta por la misma cantidad en el caso de las fracciones III, IV, V y VI, en los siguientes casos:

III.- Uso indebido de Tarjetas y documentos de pago electrónico.

IV.- Uso de tarjetas, títulos, documentos o instrumentos para el pago electrónico, falsos.

V.- Acceso indebido a los equipos y sistemas de cómputo o electromagnéticos. Al que con el ánimo de lucro y en perjuicio del titular de una tarjeta, documento o instrumentos para el pago de bienes y servicios o para disposición en efectivo, acceda independientemente a los equipos y servicios de computo o electromagnéticos de las instituciones emisoras de los mismos.

Artículo 244.- Se impondrá de tres meses a seis años de prisión y multa de 100 a 15 mil unidades, a quien ilícitamente:

III.- Altere equipo o programas de cómputo utilizados para la verificación de automotores (…).

Código Penal para el Distrito Federal

Artículo 187. Al que procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta, a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, audio grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, electrónicos o sucedáneos; se le impondrá de siete a catorce años de prisión y de dos mil quinientos a cinco mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales mencionados.

Al que fije, imprima, video grabe, audio grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participe una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta, se le impondrá la pena de siete a doce años de prisión y de mil a dos mil días multa, así como el decomiso y destrucción de los objetos, instrumentos y productos del delito.

Se impondrán las mismas sanciones a quien financie, elabore, reproduzca, almacene, distribuya, comercialice, arriende, exponga, publicite, difunda, adquiera, intercambie o comparta por cualquier medio el material a que se refieren las conductas anteriores.

Artículo 188. Al que almacene, adquiera o arriende para sí o para un tercero, el material a que se refiere el artículo anterior, sin fines de comercialización o distribución, se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa.

Delitos contra el patrimonio, artículo 231:

Artículo 231:

XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución (…).

Artículo 336. Se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien esté facultado para ello:

I. Produzca, imprima, enajene, distribuya, altere o falsifique tarjetas, títulos o documentos utilizados para el pago de bienes y servicios o para disposición de efectivo.

II. Adquiera, utilice, posea o detente tarjetas, títulos o documentos para el pago de bienes y servicios, a sabiendas de que son alterados o falsificados.

III. Adquiera, utilice, posea o detente, tarjetas, títulos o documentos auténticos para el pago de bienes y servicios, sin consentimiento de quien esté facultado para ello.

IV. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios.

V. Acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.

VI. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos

o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma.

VII. A quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos.

VIII. Produzca, imprima, enajene, distribuya, altere, o falsifique vales utilizados para canjear bienes y servicios. Si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán en una mitad.

Como se ha venido observando, en las diversas legislaciones vistas, los medios delictivos son los castigados, el delito es fraude, pornografía, etcétera. Efectivamente el legislador no puede dejar de considerar medios computarizados para obtener el resultado deseado por el sujeto que culmine con la acción delictiva.

Delitos ambientales, artículo 347 Bis:

Artículo 347 Bis:

Altere, permita la alteración u opere en forma indebida cualquier equipo o programa utilizado para la verificación vehicular prevista en las disposiciones jurídicas aplicables en el Distrito Federal.

Código Penal para el Estado Libre y Soberano de Durango

Artículo 156. Comete el delito de secuestro exprés el que prive de su libertad personal a otra persona, con el objeto de obtener un lucro mediante el uso de cualquiera de los siguientes medios: tarjetas de crédito, tarjetas de débito, título de crédito, medios electrónicos, informáticos, mecánicos, en especie o efectivo.

Artículo 211:

XXIII. Quien para obtener algún lucro para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores en perjuicio de persona alguna, independientemente de que los recursos no salgan de la institución.

DELITOS CONTRA LA SEGURIDAD EN LOS MEDIOS INFORMÁTICOS

Artículo 256. Se aplicará prisión de tres meses a tres años y multa de dieciocho a doscientos dieciséis días de salario, a quien:

I. Sin autorización para acceder a un sistema informático y con perjuicio de otro, conozca, copie, imprima, use, revele, transmita o se apodere de datos o información reservados, contenidos en el mismo.

II. Con autorización para acceder a un sistema informático y con perjuicio de otro, obtenga, sustraiga, divulgue o se apropie de datos o información reservados en él contenidos.

Si la conducta que en uno u otro caso se realice es con el ánimo de alterar, dañar, borrar, destruir o de cualquier otra manera provocar la pérdida de datos o información contenidos en el sistema, la sanción será de dos a seis años de prisión y multa de ciento cuarenta y cuatro a cuatrocientos treinta y dos días de salario.

Artículo 258. Se aplicará prisión de seis meses a seis años y multa de treinta y seis a cuatrocientos treinta y dos días de salario, al que:

I. Sin autorización, acceda, por cualquier medio a un sistema informático, de una entidad pública, para conocer, copiar, imprimir, usar, revelar, transmitir o apropiarse de sus datos o información propios o relacionados con la institución.

II. Con autorización para acceder al sistema informático de una entidad pública indebidamente copie, transmita, imprima, obtenga, sustraiga, utilice divulgue o se apropie de datos o información propios o relacionados con la institución.

Si la conducta que en uno u otro caso se realiza, tiene la intención dolosa de alterar, dañar, borrar, destruir, o de cualquier otra forma provocar la pérdida de los datos o información contenidos en el sistema informático de la entidad pública, la sanción será de uno a ocho años de prisión y multa.

Artículo 260. Para los fines del presente capítulo, se entiende por:

I. Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos para generar, enviar, recibir, recuperar, procesar o almacenar información de cualquier forma o por cualquier medio.

II. Dato informático o información: toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático.

Código Penal para el Estado de México

Artículo 17. Se impondrán de cuatro a diez años de prisión y de ciento cincuenta a quinientos días de salario mínimo de multa al que:

IV.- Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios.

V.- Acceda indebidamente a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.

Código Penal para el Estado de Guanajuato

Se aplicará de diez días a dos años de prisión y de diez a cuarenta días multa, a quien indebidamente:

I.- Abra, intercepte o retenga una comunicación que no le esté dirigida.

II.- Accese, destruya o altere la comunicación o información contenida en equipos de cómputo o sus accesorios u otros análogos.

No se impondrá pena alguna a quienes ejerciendo la patria potestad o la tutela, ejecuten cualquiera de las conductas antes descritas, tratándose de sus hijos menores de edad o de quienes se hallen bajo su guarda.

Código Penal para el Estado de Guerrero

Artículo 165.- Se impondrán las mismas penas previstas en el artículo 163, a quien:

I.- Se apodere de una cosa propia, si ésta se halla por cualquier título legítimo en poder de otro.

II.- Aprovechando energía eléctrica, algún fluido, programas computarizados, señales televisivas o de Internet, sin consentimiento de la persona que legalmente pueda disponer y autorizar aquéllas.

Código Penal para el Estado de Hidalgo

Artículo 221.- Al que por cualquier medio destruya o deteriore una cosa ajena o propia, con perjuicio de otro, se le impondrá la punibilidad prevista en el artículo 203 de este Código conforme al monto de lo dañado.

Artículo 352.- Se impondrá prisión de tres meses a cinco años y multa de treinta a cien días de salario mínimo general vigente en el estado, a quien:

XXVII.- Dentro de los ocho días previos a la elección y hasta la hora oficial del cierre de las casillas, publique o difunda por cualquier medio los resultados de encuestas o sondeos de opinión que den a conocer las preferencias de los ciudadanos.

Código Penal para el Estado Libre y Soberano de Jalisco

Artículo 194. Comete el delito de secuestro quien prive ilegalmente de la libertad a otro con la finalidad de obtener rescate o de causar daño o perjuicio.

I. Al responsable de secuestro se le sancionará con una pena de veinticinco a cuarenta años de prisión y multa por el importe de mil a tres mil días de salario mínimo, y en su caso destitución, e inhabilitación del servidor público para desempeñar otro empleo, comisión o cargo público, cuando:

Para lograr sus propósitos, se valga de redes o sistemas informáticos internacionales o de otros medios de alta tecnología, que impliquen marcada ventaja en el logro de su fin.

Código Penal para el Estado de Michoacán

Artículo 164.- Comete el delito de pornografía de personas menores de edad o de personas que no tienen capacidad para comprender el significado del hecho:

I. Quien induzca, procure, facilite o permita por cualquier medio a persona menor de edad o a persona que no tiene capacidad para comprender el significado del hecho, a realizar actos sexuales o de exhibicionismo corporal, reales o simulados, de índole sexual, con el fin de grabarlos, videograbarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, medios electrónicos o de cualquier otra naturaleza, independientemente de que se logre la finalidad.

II. Quien fije, grabe, videograbe, fotografíe, filme o describa actos de exhibicionismo corporal, reales o simulados, de carácter sexual, en los que participe persona menor de edad o persona que no tiene capacidad para comprender el significado del hecho.

III. Quien reproduzca, ofrezca, almacene, distribuya, venda, compre, rente, exponga, publique, publicite, transmita, importe o exporte por cualquier medio las grabaciones, videograbaciones, fotografías o filmes a que se refieren las conductas descritas en la fracción II de este artículo.

Artículo 203 bis:

V. Adquiera o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes y servicios o disposición de efectivo, así como a quien posea o utilice la información sustraída de esta forma.

Código Penal para el Estado de Morelos

Artículo 213.- Se aplicará prisión de seis meses a tres años y de trescientos a quinientos días multa:

I.- Al que ilegalmente fabrique, reproduzca o publique libros, escritos, imágenes u objetos obscenos y al que los exponga, distribuya o haga circular.

II.- Al que realice exhibiciones públicas obscenas por cualquier medio electrónico, incluyendo Internet, así como las ejecute o haga ejecutar por otro.

Artículo 213 quater.- Al que procure, facilite o induzca por cualquier medio a un menor, o a un incapaz, a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlo, fotografiarlo o exhibirlo mediante anuncios impresos o electrónicos, incluyendo la Internet.

Código Penal para el Estado de Nuevo León

Artículo 365.- Se equipara al robo, y se castigará como tal:

IV. El apoderamiento material o mediante vía electrónica de los documentos que contengan datos en computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

Código Penal para el Estado Libre y Soberano de Oaxaca

Capítulo I:

Artículo 241.- Comete el delito de abuso sexual, quien sin consentimiento de una persona ejecute en ella o la haga ejecutar un acto sexual, que no sea la cópula, o la obligue a observar cualquier acto sexual aun a través de medios electrónicos. Al responsable de tal hecho, se le impondrá de dos a cinco años de prisión y multa de cincuenta a doscientos días de salario mínimo.

Capítulo II:

195 Bis.- Comete el delito de pornografía infantil, el que procure, facilite, obligue o induzca por cualquier medio a uno o a más menores de dieciocho años, con o sin su consentimiento, a realizar actos de exhibicionismo corporal, lascivos o sexuales, con la finalidad de video grabarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrá de cinco a diez años de prisión y multa de seiscientos a setecientos treinta días de salario mínimo.

Código de Defensa Social para el Estado Libre y Soberano de Puebla

Artículo 245 bis. Se impondrá prisión de uno a ocho años y multa de diez a cien días de salario:

IV. Al que adquiere, copie o falsifique los medios de identificación electrónica, cintas o dispositivos magnéticos de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

V. Al que acceda indebidamente a los equipos y sistemas de cómputo o electromagnéticos de las Instituciones emisoras de tarjetas, títulos, documentos o instrumentos, para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán, a quien utilice indebidamente información confidencial o reservada de la Institución o persona que legalmente esté facultada para emitir tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

En caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo, se aplicarán las reglas del concurso.

Código Penal para el Estado de Querétaro:

Capítulo II:

Artículo 232 Bis:

Se impondrán de tres a nueve años de prisión y multa por el equivalente de doscientos a cuatrocientos días de salario mínimo general vigente en la época en que se cometa el delito, al que, sin consentimiento de quien esté facultado para ello:

I.- Produzca, imprima, enajene, distribuya, altere o falsifique, aun gratuitamente, adquiera, utilice, posea o detente, sin tener derecho a ello, boletos, contraseñas, fichas, tarjetas de crédito o débito y otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consignan u obtener cualquier beneficio.

II.- Altere, copie o reproduzca, indebidamente, los medios de identificación electrónica de boletos, contraseñas, fichas u otros documentos a que se refiere la fracción I de este artículo.

III.- Acceda, obtenga, posea, utilice o detente indebidamente información de los equipos electromagnéticos o sistemas de cómputo de las organizaciones emisoras de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo o de módem o cualquier medio de comunicación remota y los destine a alguno de los supuestos que contempla el presente artículo.

IV.- Adquiera, utilice o detente equipos electromagnéticos, electrónicos o de comunicación remota para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas, tarjetas de crédito, tarjetas de débito u otros documentos a los que se refiere este artículo o de archivos de datos de las emisoras de los documentos.

Código Penal para el Estado Libre y Soberano de Quintana Roo

Artículo 189 bis. Se impondrá hasta una mitad más de las penas previstas en el artículo anterior, al que:

Copie o reproduzca, altere los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos para el pago de bienes o servicios o para disposición en efectivo.

IV. Accese indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Código Penal para el Estado de San Luis Potosí

Artículo 136. La pena a imponer será de treinta a cincuenta años de prisión y sanción pecuniaria de dos mil a seis mil días de salario mínimo, cuando concurra

en la comisión del delito de secuestro previsto en el artículo 135 de este Código, cualquiera de las siguientes agravantes:

XIII. Se utilicen instalaciones dependientes de cualquier autoridad o instrumentos de trabajos oficiales, tales como frecuencias electrónicas, sistemas de cómputo, claves o códigos oficiales, o cualquier sistema de comunicación de uso exclusivo de la autoridad.

Artículo 182. Al que por cualquier medio procure, obligue facilite, o induzca a una persona menor de dieciocho años de edad, o de persona que no tiene la capacidad para comprender el significado del hecho, o de persona que no tiene capacidad para resistirlo, a realizar actos de exhibicionismo corporal o sexuales, con el objeto de video grabarla, fotografiarla, exhibirla o describirla mediante cualquier tipo de material visual, de audio, electrónico, sistemas de cómputo, transmisión de archivos de datos de red pública o privada de telecomunicaciones, o cualquier medio, se le impondrán de diez a catorce años de prisión, y de quinientos a cinco mil días de multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales gráficos.

Al que modifique por cualquier medio electrónico, mecánico, de programa de cómputo, la imagen de una o varias personas menores de dieciocho años de edad, o de personas que no tienen capacidad para comprender el significado del hecho, haciéndolas aparecer en actos de exhibicionismo corporal o sexual, se le impondrá la pena de diez a catorce años de prisión y multa de quinientos a tres mil días de multa.

Artículo 195. Se equiparan al robo y se sancionarán como tal:

IV. El apoderamiento material de documentos, datos o información contenidos en computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin el consentimiento de la persona que legalmente pueda disponer de los mismos.

Código penal para el Estado de Sinaloa

Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:

I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información.

II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Código Penal para el Estado de Sonora

Artículo 319.- Se considerará como Fraude para los efectos de la sanción:

XI. Al que, por sorteos, rifas, loterías, promesas de venta o por cualquier otro medio se quede en todo o en parte con las cantidades recibidas, sin entregar la mercancía u objeto ofrecido.

Código Penal para el Estado de Tabasco

Artículo 316. Al que intervenga la comunicación privada de terceras personas, a través de medios eléctricos o electrónicos, se le aplicará prisión de uno a cinco años.

Artículo 326 bis. Al que intercepte, interfiera, reciba, use o ingrese por cualquier medio sin la autorización debida o, excediendo la que tenga, a una computadora personal, o a un sistema de red de computadoras, un soporte lógico de programas de cómputo o base de datos, se le impondrá de seis meses a dos años de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 326 bis 1.- A quien sin autorización modifique, destruya o deteriore en forma parcial o total, archivos, bases de datos o cualquier otro elemento intangible contenido en computadoras personales, sistemas o redes de cómputo, soportes lógicos, o cualquier otro medio magnético, se le sancionará con penas de dos a ocho años de prisión y de cuatrocientos a mil doscientos días multa. Cuando el activo tenga el carácter de encargado del manejo, administración o mantenimiento de los bienes informáticos dañados, las penas se incrementarán en una mitad más.

Artículo 326 bis 2.- Se impondrán penas de dos a seis años de prisión y de cuatrocientos a mil días multa, al que copie o imite los originales de cualquier dato, archivo o elemento intangible contenido en una computadora personal o en un sistema de redes de computadoras, base de datos, soporte lógico, siempre que para ello se requiera autorización y no la obtenga.

Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma, los bienes informáticos falsificados, previstos en este Título.

Artículo 326 bis 3- Cuando los ilícitos previstos en este Título se cometan utilizando el equipo de cómputo de terceras personas, las penas se incrementarán en una mitad.

Como es de apreciarse en el artículo 316, la conducta es con respecto a la intervención en las comunicaciones privadas, dicha acción debe de realizarse a través de medios electrónicos o eléctricos, dejando a un lado una de las cuestiones que son de vital importancia, es decir, la información, que es uno de los objetos en cuestión dentro de los delitos informáticos.

Código Penal para el Estado de Tamaulipas

Artículo 194-Bis.- Comete el delito de pornografía de menores de edad e incapaces:

I.- El que obligue o induzca a uno o más menores de dieciocho años o incapaces a realizar actos de exhibicionismo corporal, lascivos, sexuales o pornográficos con la finalidad de grabarlos, videograbarlos, filmarlos, fotografiarlos o exhibirlos mediante anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicación, sistemas de cómputo, medios electrónicos o de cualquier otra naturaleza.

Como puede percibirse, el "delito informático" como tal no existe dentro de este artículo, lo que se castiga son los medios por los cuales se puede llegar a cometer el delito que se castiga "pornografía de menores"; por tanto queda en segundo término la forma en que se llegue a cometer dicho delito.

Artículo 207-Bis.- Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo de seguridad o que no tenga derecho de acceso a él, se le impondrá una sanción de uno a cuatro años de prisión y multa de cuarenta a ochenta días salario.

Artículo 207-Ter.- Al que sin autorización modifique, destruya o provoque pérdida e información contenida en sistema o equipo de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a seis años de prisión y multa de doscientos a seiscientos días salario.

Artículo 207-Quater.- Al que sin autorización conozca o copié información contenida en sistemas o equipos de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a cinco años de prisión y multa de cien a trescientos días salario.

Artículo 207-Quinquies.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente modifique, destruye o provoque pérdida de información que contengan se impondrá una

sanción de tres a ocho años de prisión y multa de trescientos a ochocientos días salario.

Artículo 207-Sexies.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y multa de cien a trescientos días salario.

Código Penal para el Estado de Yucatán:

Artículo 211.- Al que procure o facilite por cualquier medio que uno o más menores de dieciocho años, con o sin su consentimiento, los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de cuatrocientos a quinientos días-multa.

Código Penal para el Estado de Zacatecas

Artículo 183 Bis. También cometen el delito de corrupción de menores y se harán acreedores a las sanciones previstas:

II Quienes propicien o permitan que menores de dieciocho años presencien, por medio de aparatos electrónicos la exhibición de las cintas de vídeo a que se refiere la fracción anterior.

Conclusión o Análisis

Los anteriores artículos extraídos de los diferentes códigos penales pertenecientes a los estados que integran la República Mexicana fueron el resultado de un análisis extenso de cada uno de ellos, buscando siempre la relación con los denominados delitos informáticos con la finalidad de poder listar un compendio de

artículos que ayudan al marco legal el cual sirve para regular estas actividades a nivel nacional.

- La clasificación de los delitos informáticos en México se da en 3 categorías:
- Delitos Patrimoniales por ejemplo el fraude electrónico
- Delitos de Pornografía como por ejemplo la distribución de material pornográfico de menores de edad
- Delincuencia Organizada como por ejemplo la piratería de software

Al realizar este análisis se pude identificar en la mayoría de estos que los delitos se persiguen por querella, no específicamente como un delito informático. En su mayoría, la redacción de estos artículos llevan a la omisión de otros elementos importantes, que derivado de la poca actualización de algunos de ellos, impactan finalmente en que los elementos descritos en ciertos casos no son los más actuales y por consiguiente no incorporan los nuevos elementos tecnológicos, lo que deja en desprotección a estos. En relación a lo anterior se describe en algunos códigos penales como un delito "… el que acceda a equipos protegidos por un mecanismo de seguridad…" especificando únicamente a equipos con un mecanismo de seguridad lo cual dejaría desprotegidos a todos aquellos equipos que no cuenten con alguno. Relacionado con la corrupción de menores existe la descripción que menciona únicamente a las cintas de video donde de igual forma no contempla nuevas tecnologías que podrían ser utilizadas como medios de almacenamiento.

Algunos artículos tipifican actividades referentes a una conducta o acción culposa describiendo que estas se realizan cuando el infractor tenía la intención de realizar dicha actividad ilícita o en el incumplimiento de un deber, lo cual genera que, un resultado sin intención de producirlo no cumpla las características que este articulo tipifica o adicional a esto, argumentando un desconocimiento de los alcances que tiene la tecnología podría justificar esta conducta culposa.

4. METODOLOGIAS DE SEGURIDAD INFORMATICA

4.1 Definición

Acorde a la Real Academia de la Lengua Española la palabra metodología significa “Conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal”, lo cual ayuda a definir que una metodología es la estrategia que se utilizará para cumplir con los objetivos de una investigación o tarea específica (Briones, 2002).

Podemos entonces decir que una metodología en términos prácticos está compuesta por una serie de decisiones, procedimientos detallados y técnicas que cumplen funciones particulares. Para el análisis de estas metodologías se tomó a consideración únicamente las metodologías que se han ido actualizando en los últimos 5 años, todo esto debido a que se considerarían actuales en relación a la velocidad con que los sistemas informáticos cambian y se adaptan al entorno.

4.2 Metodología OSSTMM

Open Source Security Testing Methodology Manual (OSSTMM) es un manual de metodología para pruebas de seguridad desarrollada por el Institute for Security and Open Methodologies (ISECOM), esta metodología presenta una referencia de cómo llevar a cabo un test de seguridad de forma ordenada. Comprende gran parte de los aspectos que se deben tomar en cuenta al momento de realizar pruebas de seguridad, se encuentra dividida en varias secciones, como parte importante de esta metodología se contempla el uso de los denominados puntos de revisión con tareas específicas en cada uno de las actividades a realizar para cada sección. Las secciones están conformadas por:

A) Seguridad de la Información: La describe con 3 puntos, revisión de la inteligencia competitiva, revisión de la privacidad y recolección de documentos.

B) Seguridad de los Procesos: Define la seguridad de los procesos con 3 elementos que son el testeo de solicitud, el testeo de sugerencia dirigida y el testeo de las personas confiables.

C) Seguridad en las tecnologías de internet: Describe la importancia de la seguridad con 16 puntos que son la logística y controles, la exploración de la red, la identificación de los servicios del sistema, la búsqueda de información competitiva, la revisión de privacidad, obtención de documentos, la búsqueda y verificación de vulnerabilidades, testeo de aplicaciones de internet, enrutamiento, testeo de sistemas confiados, testeo de control de accesos, testeo de sistema de detección de intrusos, testeo de mediadas de contingencia, descifrado de contraseñas, testeo de denegación de servicios y la evaluación de políticas de seguridad.

D) Seguridad en las comunicaciones: Está centrada en la verificación de testeo de PBX, testeo del correo de voz, revisión del fax, testeo del modem.

E) Seguridad Inalámbrica: Está conformada por 11 puntos orientados a la verificación de radiación electromagnética, verificación de redes inalámbricas, verificación de redes bluetooth, verificación de dispositivos de entrada inalámbricos, verificación de dispositivos de mano inalámbricos, verificación de comunicaciones sin cable, verificación de dispositivos de vigilancia inalámbricos, verificación de dispositivos de transacción inalámbricos, verificación de RFID, verificación de sistemas infrarrojos y revisión de privacidad.

F) Seguridad Física: Este punto se orienta a la revisión del perímetro, revisión de monitoreo, evaluación de control de acceso, revisión de propuesta de alarmas, revisión de ubicación y revisión de entorno.

Se enfoca a 7 disciplinas:

1) Búsqueda de vulnerabilidades: Se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.

2) Escaneo de la seguridad: consiste en general en las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de puntos débiles de la red y de una análisis individualizado.

3) Test de Intrusión: trata en general sobre los proyectos orientados a objetivos en los cuales existe una meta, que incluye ganar acceso privilegiado con medios pre-condicionales.

4) Evaluación de riesgo: abarca los análisis de seguridad a través de entrevistas e investigación, que incluye la justificación de negocios, las justificaciones legales y las justificaciones específicas de la industria.

5) Auditoria de seguridad: se centra en la inspección manual de los privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.

6) Hacking Ético: se refiere a los test de intrusión en los cuales el objetivo es obtener accesos en la red dentro de un periodo de tiempo predeterminado en la duración del proyecto.

7) Test de seguridad: es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de un análisis mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del periodo de tiempo que dure el proyecto de análisis.

4.3 ISSAF

Information System Security Assessment Framework (ISSAF) es un proyecto de la Open Information System Security Group (OISSG). Constituye un marco de trabajo detallado respecto a las prácticas y conceptos relacionados con las tareas a realizar al conducir un test de seguridad. La información contenida en ISSAF se encuentra organizada alrededor de lo que se denomina criterios de

evaluación, estos criterios de evaluación se componen de los siguientes elementos: 1) Descripción del criterio de evaluación, 2) Puntos y objetivos para cubrir, 3) Prerrequisitos para conducir la evaluación, 4) El proceso mismo de evaluación, 5) El informe de los resultados esperados, 5) Las contramedidas y recomendaciones, 6) Referencias y documentación externa.

Dichos criterios se encuentran contenidos dentro de diferentes dominios entro los que es posible encontrar desde los aspectos más generales, como los conceptos básicos de la administración de proyectos de seguridad, hasta las técnicas más específicas como la ejecución de pruebas. Incluye elementos como plantillas para facilitar su implementación, estas plantillas son los acuerdos de confidencialidad, seguimiento de proyecto, listas de verificación, verificación de estado de antivirus, características para el armado de un laboratorio de pruebas.

4.4 OWASP

Open Web Application Security Proyect (OWASP) es un proyecto centrado en la seguridad sobre aplicaciones web, que está conformado por una comunidad abierta y libre cuya misión es hacer visible y consciente a la seguridad en aplicaciones. Todo el material está disponible bajo una licencia de software libre y abierto. La fundación OWASP es una asociación sin fines de lucro. Los proyectos OWASP se dividen en dos categorías principales, de desarrollo y de documentación. Los proyectos de documentación actual son:

1) Guía de desarrollo: es un documento que proporciona una guía detallada para la construcción de aplicaciones web seguras.

2) Guía de Pruebas: una guía centrada en las pruebas y listas de comprobación de seguridad sobre aplicaciones web.

3) Top 10: un documento de conciencia sobre vulnerabilidades más críticas sobre aplicaciones web.

4) Legal: un proyecto basado en la contratación de servicios de software y sus aspectos de seguridad.

5) AppSec FAQ: respuestas a las preguntas más frecuentes sobre seguridad de aplicaciones web.

En cuanto a desarrollo se incluyen los proyectos WebScarab, un software para realizar pruebas de seguridad en aplicaciones y servicios web, y WebGoat, un entorno de entrenamiento para que los usuarios aprendan sobre seguridad de aplicaciones web de forma segura y legal. OWASP contempla dentro de su metodología 8 fases de pruebas para la comprobación de seguridad:

1) Obtención de información.

2) Pruebas de reglas de negocio.

3) Pruebas de autenticación.

4) Pruebas de manejo de sesión.

5) Pruebas de validación de datos.

6) Pruebas de denegación de servicio.

7) Pruebas en servicios web.

8) Pruebas en AJAX.

4.5 ISO/IEC 127000

La serie de normas ISO/IEC 127000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la comisión electrotécnica internacional (IEC). Esta serie de normas describe las

mejores prácticas para el diseño, implementación y mantenimiento de un sistema de gestión de la seguridad de la información (SGSI), cuenta con 23 estándares publicados. Esta serie de normas está compuesta por:

1) ISO/IEC 27000 overview & vocabulary: Describe el vocabulario estándar para la implementación de un SGSI (sistema de gestión de la seguridad de la información). Se considera en desarrollo debido a que no todos los puntos de esta serie de normas están terminadas.

2) ISO/IEC 27001 formal ISMS (Information security management systems) specification: Esta norma específica los requisitos para la implementación de un SGSI, se le considera la norma más importante y es la que más actualizaciones ha sufrido desde su publicación en el año 2005, la última actualización de esta norma fue a finales del 2013.

3) ISO/IEC 27002 infosec controls: Es el código de buenas prácticas para la gestión de seguridad de la información, su última actualización fue en el 2013.

4) ISO/IEC 27003 ISMS implementation guide: Esta norma marca las directrices para la implementación de un SGSI, describe el proceso de implementación y diseño. Su última actualización fue en el 2010.

5) ISO/IEC 27004 infosec metrics: Describe las métricas para la gestión de la seguridad de la información, proporciona las recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Su última actualización se realizó en el 2009.

6) ISO/IEC 27005 infosec risk management: Trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de seguridad de la información. Su última actualización fue en el 2011.

7) ISO/IEC 27006 ISMS certification guide: Son los requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma muestra los requisitos específicos para la certificación de SGSI. Su última actualización fue en el 2011.

8) ISO/IEC 27007 management system auditing: Es una guía para auditar al SGSI. Toma en específico la norma 127001 para considerar los puntos de la auditoria. Su última actualización fue en el 2011.

9) ISO/IEC 27008 technical auditing: Está norma es complementaria a la norma 127007, se centrada en los puntos técnicos de la auditoria. Su última actualización fue en el 2011.

10) ISO/IEC 27010 for inter-org comms: consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones. Contempla actividades como el suministro, mantenimiento y protección de una organización o de la infraestructura crítica. Su última actualización fue en el 2012.

11) ISO/IEC 27013 for ISMS + IT service management: Es una guía de implementación integrada. Está relacionada con la gestión de servicios de TI. Su última actualización fue en el 2012.

12) ISO/IEC 27014 infosec governance: Consiste en una guía de gobierno corporativo dela seguridad de la información. Su última actualización fue en el 2013.

13) ISO/IEC 27015 for financial services: Es una guía de SGSI orientada a las organizaciones del sector financiero y seguros. Su última actualización fue en el 2012.

14) ISO/IEC 27016 infosec economics: Es una guía de valoración de los aspectos financieros de la seguridad. Su última actualización fue en el 2014.

15) ISO/IEC 27018 cloud privacy: Es una guía de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

16) ISO/IEC 27019 process control energy: Es una guía para sistemas de control específicos relacionados con el sector de la industria de la energía. Su última actualización fue en el 2013.

17) ISO/IEC 27031 information and communications technology business continuilty: Es una guía de apoyo para la adecuación de las tecnologías de información y comunicaciones de una organización para la continuidad del negocio. Su última actualización fue en el 2011.

18) ISO/IEC 27032 cybersecurity: Esta norma proporciona una guía para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esta actividad y de sus dependencias en otros dominios de seguridad. Establece una descripción general de la seguridad cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de sus papel en la seguridad cibernética, una orientación para abordar problemas comunes y un marco que permite a las partes interesadas a que colaboren en la solución de problemas. Su última actualización fue en el 2012.

19) ISO/IEC 27033-1 to 5 network security: Es una norma dedicada a la seguridad en redes, está conformada de 5 partes que son: conceptos generales, directrices de diseño e implementación de seguridad en redes, escenarios de referencia en redes, el aseguramiento de las comunicaciones entre redes mediante gateways de seguridad y el aseguramiento de comunicaciones mediante VPN´s. Existen dos partes más que son la convergencia IP y las redes inalámbricas aunque no han sido publicadas oficialmente. Su última actualización fue en el 2009.

20) ISO/IEC 27034-1 application security: Norma dedicada a la seguridad en aplicaciones informáticas. Consiste en 6 partes que son: conceptos generales,

marco normativo de la organización, proceso de gestión de seguridad en aplicaciones, validación de la seguridad en aplicaciones, estructura de datos y protocolos y controles de seguridad de aplicaciones, guía de seguridad para aplicaciones de uso específico. Su última actualización fue en el 2011.

21) ISO/IEC 27035 incident management: Este estándar está enfocado a la gestión de incidentes de seguridad, hace énfasis en las actividades de detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

22) ISO/IEC 27036-1-2 & 3 information and communications technology supply management: Ofrece la guía para la evaluación y forma de tratar los riesgos de seguridad de la información que involucra la adquisición de servicios de otros proveedores. Su última actualización fue en el 2013.

23) ISO/IEC 27037 digital evidence: Proporciona una guía para la identificación, obtención, recolección, manejo y protección digital de la evidencia forense. Su última actualización fue en el 2012.

4.6 MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología orientada a organizaciones públicas y privadas, está enfocada en la protección de la información y los sistemas que la tratan. Cabe destacar que esta metodología está desarrollada en conjunto con el gobierno de España con la colaboración del ministerio de hacienda y administración pública y con la dirección general de modernización administrativa, procedimientos e impulso de la administración electrónica. La finalidad de MAGERIT es permitir conocer el valor de la información y ayudar a protegerlo, la metodología está conformada por 5 puntos que son:

1) Método de análisis de riesgos: Muestra una aproximación metódica para determinar el riesgo siguiendo una serie de pasos pautados.

2) Proceso de gestión de riesgos: Describe los impactos y riesgos a que está expuesto el sistema, y plantea la toma de decisiones que estará condicionada según los factores de gravedad de impacto o riesgo, las obligaciones a las que la organización está sometida por la ley, las obligaciones a las que por contrato está sometida la organización.

3) Proyectos de análisis de riesgos: Marca las actividades recurrentes que existen dentro del proceso de gestión de riesgos. Considera 3 puntos que son las actividades preliminares, la elaboración del análisis de riesgos y la comunicación de los resultados. A su vez permite generar los roles y funciones en específico de los actores que se encuentran involucrados con el manejo de la información y de los sistemas informáticos.

4) Plan de seguridad: Esta sección trata de cómo llevar a cabo planes de seguridad, entendiendo por tales proyectos para materializar las decisiones adoptadas para el tratamiento de los riesgos, estos planes reciben diferentes nombres en diferentes contextos y circunstancias tales como: planes de mejora de seguridad, plan director de seguridad, plan estratégico de seguridad y plan de adecuación.

5) Desarrollo de sistemas de información: Presenta los puntos necesarios a contemplar para que los sistemas de información no se conviertan en una fuente de riesgo en el sentido de que no permita que se materialicen las amenazas. Constituye una guía para el diseño y desarrollo de sistemas de información seguros, identifica dos actividades que son las actividades relacionadas con la propia seguridad del sistema de información que se está desarrollando y las actividades que velan por la seguridad del proceso de desarrollo del sistema de información.

4.7 The Security Risk Management Guide

Esta metodología está desarrollada por Microsoft, está diseñada con la finalidad de ayudar en el desarrollo de una estrategia para proteger la disponibilidad,

integridad y confidencialidad de los datos de los sistemas informáticos de las organizaciones. Esta metodología está orientada a proteger 3 aspectos:

1) Confidencialidad: Se enfoca a la información que requiere protección contra la divulgación no autorizada. Por ejemplo, datos que se van a difundir en un momento determinado, información personal e información comercial patentada.

2) Integridad: Se refiere a la información que debe protegerse de modificaciones no autorizadas, imprevistas o accidentales. Por ejemplo información de censos, indicadores económicos o sistemas de transacciones financieras.

3) Disponibilidad: Se refiere a la información o los servicios que deben estar disponibles puntualmente para satisfacer requisitos o evitar pérdidas importantes. Por ejemplo, sistemas esenciales de seguridad, protección de la vida y predicciones de huracanes.

Adicional a estos aspectos muestra cómo establecer un plan de contingencia en caso de desastre.

5. PROPUESTA DE METODOLOGIA

La siguiente metodología se desarrolló con el propósito de ofrecer una guía de referencia que permita la implementación de seguridad en una pyme en el Estado de Querétaro, México. Esta metodología permitirá implementar, comprobar y ayudar en la toma de decisiones en cómo definir una estrategia que planifique tanto recursos económicos como humanos. Cabe destacar que esta propuesta contiene información dirigida a todos los niveles de la organización, su diseño está basado en el análisis de las metodologías mencionadas previamente y en las mejores prácticas recomendadas por el estándar ISO 127001-2013 el cual marca como agrupar los controles de revisión de seguridad y sus líneas de actuación las cuales están incluidas en los 34 puntos principales contenidos en esta metodología, todo

esto en cumplimiento del Código Penal Federal y Código Penal Estatal del Estado de Querétaro.

5.1 Introducción

Para dar una mejor comprensión de la gestión de seguridad los tres elementos esenciales de una organización deben trabajar de manera conjunta y coordinada, estos tres elementos son la tecnología, los procesos y las personas.

En base a estos tres elementos se buscará implementar un sistema de gestión de la seguridad de la información (SGSI) que permita mitigar las vulnerabilidades que pudieran ocasionar una perdida y minimizar los daños en los activos si alguno de los riesgos llegara a materializarse. Hay que resaltar que la seguridad no es un producto sino un proceso continuo que debe ser controlado, monitorizado y actualizado constantemente. Está conformada de treinta y cuatro puntos, los cuales se pueden usar a manera de pregunta para obtener un diagnóstico rápido y conocer los puntos débiles de la organización o se puede implementar cada uno de ellos para establecer un ambiente seguro. Los puntos a considerar para la implementación de seguridad se basan en los siguientes principios:

-Disponibilidad: Asegurar que los usuarios autorizados tengan el acceso cuando lo requieran en un tiempo adecuado.

-Integridad: Garantía de la exactitud, de que la información sea completa y de los mecanismos que la procesan.

-Confidencialidad: Asegurar que la información es sólo accesible para aquellos autorizados y que se cumpla el marco legal vigente.

-Autenticidad de los usuarios del servicio: asegurar la identidad de los usuarios que manejan o acceden a la información o los equipos.

-Autenticidad del origen de los datos: asegurar la identidad u el origen de los datos.

-Seguimiento de los servicios (trazabilidad): asegurar que en todo momento se pueda determinar quién hizo que acción y en qué momento.

-Seguimiento de los datos: asegurar que en todo momento se podrá determinar quién ha accedido a los datos.

Con el fin de facilitar la lectura e implementación, la metodología se encuentra estructurada en los siguientes puntos:

1.- Seguridad relacionada con las reglas del negocio: estos elementos se consideran la base para la implementación de seguridad en la organización y serán los puntos de partida que marcan la directriz de lo que se busca asegurar e implementar, están directamente relacionados con las políticas de seguridad, las relaciones que existen con terceros (como pueden ser los diferentes tipos de proveedores) y acuerdos de confidencialidad tanto para elementos externos como internos de la organización.

2.- Seguridad relacionada con la capacitación del personal: incluye la formación, capacitación, funciones, confidencialidad y recomendaciones necesarias para que el personal pueda apoyar con la implementación de seguridad. En orden de importancia este es el segundo escalón en la implementación de seguridad, el personal es considerado el eslabón más débil de la organización pero se puede fortalecer con la capacitación y la implementación de controles adecuados que sean de fácil entendimiento para estos.

3.- Seguridad relacionada con el hardware: contempla la seguridad física del entorno, la seguridad física y lógica de las comunicaciones, los dispositivos utilizados en el que hacer de la organización.

4.- Seguridad relacionada con el software: contiene los puntos a considerar en la implementación, desarrollo, compra y actualización de software para la organización.

5.- Seguridad relacionada con la revisión del sistema: contiene las tareas necesarias para la auditoria del sistema.

6.- Resumen: Contiene una breve descripción de los puntos más importantes desarrollados a través de la metodología para facilitar la lectura e implementación.

7.- Anexo de Herramientas: Un apartado con la descripción en extenso de herramientas, ligas de descarga y requerimientos para su implementación en los controles descritos en esta metodología.

8.- Anexo de Marco Normativo: Un apartado que contiene en extenso el marco normativo, leyes y procedimientos a contemplar en materia de seguridad de la información.

9.- Anexo de Ataques y Vulnerabilidades en los Sistemas de Información: Un apartado para la conciencia y descripción de los principales ataques y técnicas conocidas a la fecha para vulnerar sistemas de información.

10.- Glosario de Términos: Contiene una explicación o descripción de los conceptos más importantes que aparecen en la metodología.

Para efectos de tener una herramienta que permita visualizar los resultados, se desarrolló un formulario en PHP con HTML que permite contestar preguntas relacionadas con los treinta y cuatro puntos y generar un gráfica que simplifica el detectar las áreas de oportunidad, permite generar un documento PDF para almacenar los resultados. Como parte del formulario se agregó un punto más denominado “No Aplica” en caso de que la pregunta en cuestión no vaya acorde a

la pregunta que se está evaluando, la cantidad de no aplica se puede visualizar en la gráfica y con esto conocer la cantidad de elementos que se podrían aprovechar para implementarlos en nuestra organización.

Figura 5-1 Formulario de diagnóstico de estado de la seguridad. Fuente: Elaboración Propia

Si lo que se desea es realizar un diagnóstico previo y centrarse únicamente en los puntos débiles de la organización se debe responder a las siguientes preguntas, en caso de que la respuesta sea no a alguna de ellas esto indicará que será un punto a considerar en la mejora o implementación de seguridad en ese aspecto. Existe la posibilidad de que alguno de los puntos descritos no aplique para la organización que se está evaluando, al finalizar deberá tomar los apartados que se respondieron con “NO” como los puntos a implementar y los que se respondieron como “NO APLICA” podrá considerarse como áreas de oportunidad para su implementación. Los puntos que evalúa esta metodología son:

- Seguridad orientada a las políticas y procedimientos (Preguntas: 1-7)
- Seguridad orientada al personal (Preguntas: 8-12)
- Seguridad orientada a los espacios y equipo físico (Preguntas: 13-24)

- Seguridad orientada al software (Preguntas: 25-30)
- Seguridad orientada a la verificación (Preguntas: 31-34)
- No Aplica (Contabiliza este tipo de respuesta)

Las preguntas son las siguientes:

1.- ¿Existe un comité de seguridad que coordine las actividades en relación a seguridad de la organización?

2.- ¿Existe una política de seguridad de la empresa?

3.- ¿Existe un documento guía para que permita la clasificación de la información?

4.- ¿Existe un documento que permita controlar el intercambio de información con terceros?

5.- ¿Existe un procedimiento para validar los contratos de prestación de servicios que involucran los procesos de la organización para garantizar y deslindar responsabilidades entre los involucrados?

6.- ¿Existe un mecanismo para regular los intercambios de información con terceros y los involucrados en dichos intercambios?

7.- ¿Se analizan que las medidas a implantar tengan una validez legal conforme al código penal vigente?

8.- ¿Están definidas las funciones y responsabilidades del personal, existe un mecanismo de validación de su entendimiento e implementación?

9.- ¿Existen un documento que se deba firmar por parte de los usuarios respecto a la confidencialidad de la información o los procedimientos de la organización?

10.- ¿Existe un plan de concientización para el personal sobre la importancia de medidas de seguridad definidas por la organización?

11.- ¿Se encuentran definidas las normas para el abandono de puesto de trabajo y la implementación de seguridad del espacio de trabajo?

12.- ¿Existe un procedimiento de asignación de contraseña y mecanismo de capacitación del personal sobre las buenas prácticas de sus usos?

13.- ¿Se tienen restringidos los accesos de sitios públicos de internet para los usuarios de la organización?

14.- ¿Se tiene restringido el uso de correo electrónico a usuarios no autorizados?

15.- ¿Existe un procedimiento para el control de las incidencias y se hace del conocimiento de los usuarios?

16.- ¿Se encuentra definido un perímetro de seguridad para proteger los sistemas de información y sus normas para el acceso?

17.- ¿Se encuentran definidos los espacios de acceso público?

18.- ¿Se tiene definido un plan de continuidad del negocio que garantice la recuperación de los sistemas de información en caso de un desastre?

19.- ¿Se tienen definidos los procedimientos para la creación de inventarios y clasificación de activos?

20.- ¿Se cuenta con un registro de entrada y salida de activos y el mecanismo para la autorización de salida de estos?

21.- ¿Se tiene definido un proceso para la eliminación y reutilización de medios de almacenamiento?

22.- ¿Se tiene definidas las normas para el uso de medios extraíbles?

23.- ¿Se tiene definido el procedimiento para los mantenimientos preventivos y correctivos?

24.- ¿Se tiene un diseño de suministro eléctrico que contemple medidas de respaldo en caso de pérdida de energía?

25.- ¿Se tienen definidos los requisitos de seguridad mínima para la adquisición de software?

26.- ¿Se tiene definido un procedimiento de instalación de actualizaciones o parches de seguridad?

27.- ¿Se tiene definido un procedimiento de instalación o implementación de antivirus?

28.- ¿Se tiene definida una política para la creación de copias de seguridad?

29.- ¿Se tiene definido un mecanismo de identificación de conexiones externas hacia la organización?

30.- ¿Se tiene definido un procedimiento que garantice la confidencialidad de los datos?

31.- ¿Se tiene definido un procedimiento para verificar la sincronización de los relojes de los servidores?

32.- ¿Se tiene configurado un registro de accesos a los sistemas de información?

33.- ¿Se tiene definido un procedimiento para la creación de un entorno de pruebas seguro?

34.- ¿Se tiene definido un procedimiento para el monitoreo de los sistemas?

Una vez resuelto este cuestionario podremos detectar los puntos faltantes en la organización, a continuación se describen los puntos para un mayor entendimiento e implementación.

5.2 Seguridad relacionada con las reglas del negocio

El establecer una política de seguridad, definir directrices claras para el tratamiento de la información generada o recibida por la organización, promover o adoptar una estructura para un mejor clasificación de la información, establecer procedimientos para regular las comunicaciones y relaciones con terceros (por ejemplo el envío de correos electrónicos o el uso de redes sociales), asegurar el cumplimiento de todos los aspectos legales que obliguen a la organización en materia de tratamiento de la información (tomando como base de cumplimento la LFPDPPP).

5.2.1 Definición de la política de Seguridad de la Empresa.

Para llevar un mayor control en la búsqueda de la implementación de seguridad en la organización, se debe crear un comité de seguridad o un encargado que cumpla la función de coordinar y calendarizar las actividades relacionadas con la verificación de estos controles. El comité será el encargado del establecimiento de medidas disciplinarias o sanciones que servirán para que en el caso de que algún miembro incumpla lo establecido en cuestión de seguridad, se imponga una sanción acorde a lo establecido por dicho comité. Dicho comité deberá establecer mecanismos de vigilancia y control los cuales deberán realizarse periódicamente. Para esto se deberá:

- **Definir un comité de seguridad que coordine las actividades de creación y actualización de las directrices en cuanto a la implementación de seguridad, su función también será el validar**

periódicamente el cumplimiento de la política de seguridad en la organización.

Establecer una política de seguridad tiene el propósito de informar y concientizar a los empleados sobre la estrategia de seguridad que tiene la organización y ayuda a definir los lineamientos generales de cómo actuar para evitar amenazas y reaccionar ante incidentes de seguridad. La política debe establecer directrices claras, normas para el tratamiento de la información y definir los responsables de su desarrollo, implantación y gestión.

La política deberá estar aprobada por la dirección de la organización para evitar dudas o confusiones al respecto. Se deberá dar difusión y capacitación para que todo el personal de la organización conozca de su existencia, la importancia de su implementación y los alcances.

La política de seguridad deberá contener:

- Alcance de la política
- Normas para el tratamiento de la información
- Responsables del desarrollo, implementación y gestión de la política (la recomendación es conformar un comité de seguridad de la información)

Adicionalmente las directrices que se sugiere deberán formar parte de la política son:

- Queda estrictamente prohibido el uso de los activos de la empresa, tanto recursos informáticos, como información, para finalidades definidas en la política de seguridad.

- Existe la obligación de parte de los usuarios el bloqueo y aseguramiento de su puesto de trabajo cuando este sea abandonado ya sea temporalmente o al finalizar su jornada laboral, por ejemplo el bloqueo de

inicio de sesión del equipo cuando se abandone su lugar de trabajo y el almacenar fuera de la vista de todos los documentos que puedan contener información.

El marco legal que soporta este punto puede consultarse en el Anexo de Marco Normativo en la sección Guía de Seguridad para la Protección de Datos Personales. Para esto se deberá:

- **Se debe definir la política de seguridad para la organización y sus respectivos mecanismos de difusión con el personal.**

5.2.2 Clasificación de la información

Para la clasificación de la información es importante establecer las diferencias, estas clasificaciones pueden ser: publica, restringida y confidencial. Estas diferencias permitirán conocer qué medidas de seguridad se deberán aplicar e irán en relación a los puntos previamente mencionados que son disponibilidad, integridad y confidencialidad de los datos. Esta guía podrá contener un catálogo de tipos de información, su manejo y clasificación. Puede utilizarse el catalogo contenido en la guía de seguridad incluida en el anexo de marco normativo. A su vez el Gobierno Mexicano a través del Instituto Nacional de Transparencia, Acceso a la Información (INAI), publican una guía con propuestas de clasificación de la información según el tipo y origen. Para esto se deberá:

- **Crear un documento guía para la clasificación de la información o determinar que se implementará la generada por el INAI.**

5.2.3 Contratos con terceros

Por la naturaleza de los sistemas de información, es común que exista un grado de subcontratación de servicios de terceros. Debido a que no es común que los terceros conozcan la política de seguridad de la organización, será necesario el

hacer de su conocimiento la política de seguridad de la organización ya que sin esta no podrán ser capaces de prestar el servicio contratado con las garantías exigidas, se recomienda regular formalmente los servicios que se estén subcontratando. Por esta razón el acceso a los datos e información propios de la organización deben estar reguladas mediante contrato. Consultar el apartado contrato de confidencialidad del anexo de marco normativo. Para esto se deberá:

- **Regular mediante un contrato el tratamiento de información y prestación de servicios con proveedores externos que impliquen el intercambio de información.**

Como todo contrato, los términos y condiciones podrán ser actualizados, para esto es necesario la revisión a fin de comprobar que las medidas de seguridad y confidencialidad siguen vigentes. La recomendación es que esta vigilancia se haga al menos una vez por año o en su defecto cada que exista un cambio en la ley que impacte sobre esta. Para esto se deberá:

- **Vigilar la vigencia y los alcances de todos los contratos de prestación de servicios para asegurar que se ajustan a la política de seguridad de la organización.**

También será importante establecer cómo serán los intercambios de información con terceros. Este proceso debe estar bien definido y se debe hacer del conocimiento de todos los implicados. Este tipo de intercambios puede generar amenazas a la integridad de los datos y también a la confidencialidad de los mismos. Evitar la pérdida, intercepción o alteración de la misma debe ser una prioridad de la organización. Por ejemplo se puede definir como un mecanismo de intercambio de información que todo archivo intercambiado de manera electrónica, solo sea por medio del correo electrónico institucional. Otro ejemplo puede ser el no permitir el uso de memorias USB para compartir archivos ya que la perdida de este medio implicaría vulnerar la información contenida, en su caso de permitir el uso de este

medio podría establecerse un mecanismo para el cifrado de los datos, consultar el anexo de herramientas en el punto de cifrado de información. Para esto se deberá:

- **Regular los intercambios de información que exista con terceros, se deberá comunicar los requisitos al personal de la organización y a los terceros que estén involucrados en dichos intercambios.**

Establecer en todas las medidas de seguridad adoptadas las respectivas validaciones en donde se puedan detectar los incumplimientos legales establecidos en la política de seguridad implementada en la organización. Algunas de estas validaciones podrán hacerse por medio de herramientas y otras tendrán que ser evaluadas por el comité de seguridad. Consultar el anexo normativo en su apartado de código de procedimientos civiles y el anexo de herramientas. Para esto se deberá:

- **Analizar la validez legal de las medidas a implantar en el sistema de seguridad de la información y validar constantemente su vigencia.**

5.3 Controles Relacionados con el Personal

El personal que maneja el sistema de información, es uno de los elementos principales en el análisis de medidas de seguridad de la información, de su colaboración depende en buena medida el éxito o fracaso de muchas de las medidas de seguridad a implantar. Como se mencionó previamente el personal será el punto débil en la implementación de seguridad, en caso de que este no esté bien capacitado.

5.3.1 Definición de funciones y responsabilidades

Una de las principales amenazas de toda organización es el acceso de usuarios no autorizados (internos o externos) que puedan consultar, modificar y borrar e incluso borrar información a la que no deberían acceder. Cada miembro del personal debe ser informado de sus funciones y obligaciones en el tratamiento de los datos con los cuales está involucrado. Se deben definir las funciones y responsabilidades de seguridad para cada uno de los usuarios del sistema de información; para ello se aplicará el principio de establecer los mínimos privilegios necesarios para el desarrollo de dichas labores. Para esto se deberá:

- **Definir cuáles serán las funciones y responsabilidades de cada miembro de la organización respecto a la seguridad de la información, definir los mecanismos de difusión y capacitación para asegurar que todos las reciban y entiendan.**

5.3.2 Definición de cláusulas de confidencialidad

Todo usuario debe recibir orientación sobre la obligación de mantener secreto profesional sobre los datos que conozca en el desarrollo de sus funciones, aún después de finalizar la relación laboral que le une con la organización. Estas cláusulas deben ser aplicadas tanto para el personal contratado como para el personal externo aun con una contratación temporal. Consultar el acuerdo de confidencialidad y no divulgación contenido en el anexo de normativo. Para esto se deberá:

- **Definir cláusulas sobre la confidencialidad y no divulgación de información, se deberá firmar por cada miembro que tenga acceso a la información un documento de aceptación de dichas cláusulas.**

5.3.3 Conciencia y educación sobre las normas de seguridad

Para que los usuarios puedan colaborar con la gestión de la seguridad, se les debe concientizar e informar con el fin de que cumplan con las medias establecidas. Es necesario capacitar al personal de forma adecuada sobre seguridad y sobre el uso correcto de los sistemas de información. Para esto se deberá:

- **Generar un calendario de concientización y capacitación de personal sobre la importancia de la implementación de seguridad en el que hacer de sus labores diarias.**

5.3.4 Escritorio de trabajo y seguridad de equipo desatendido

El uso inapropiado del escritorio de trabajo y el entorno pude generar amenazas sobre la confidencialidad de los datos, como accesos no autorizados a datos o sistemas de información. Se deben establecer normas para que el personal tenga el escritorio sin información visible que pueda comprometer la confidencialidad de los datos al igual como debe estar libre de tener físicamente documentos confidenciales a la mano de cualquiera.

Se debe adoptar una política de escritorio limpio de papeles y medios extraíbles así como normas para cuando el usuario abandona su estación de trabajo. Un ejemplo es el error al colocar claves de acceso en un post-it o direcciones ip de acceso a algún sistema de información. Otro error grave seria por ejemplo el tener documentos en el escritorio del equipo que puedan revelar nombres sobre documentos confidenciales o simplemente mostrar la ubicación de los mismos.

Se recomienda verificar el funcionamiento de bloqueo de equipo o en si defecto que el usuario conozca el procedimiento para realizarlo, la función de

bloqueo de acceso al equipo viene implementada en cualquier sistema operativo. Para esto se deberá:

- **Definir las reglas de abandono y gestión del espacio de trabajo.**

5.3.5 Responsabilidad en el uso de contraseñas

La autenticación de usuarios es un control común mente utilizado para limitar el acceso a un sistema y asignación de privilegios. La fortaleza de este control radica en la complejidad y en la longitud de esta contraseña y en la periodicidad en que esta sea cambiada, la debilidad se encuentra en que el usuario tenga la capacidad de recordar dicha contraseña sin necesidad de tenerla almacenada en algún espacio visible para otros usuarios. Se recomienda consultar el apartado de Anexo de Ataques y Vulnerabilidades en los Sistemas de Información y el anexo de herramientas para complementar este punto.

Se recomienda el uso de una herramienta para verificar la fortaleza de la contraseña o en su defecto considerar que tenga una longitud recomendada de 12 dígitos, mayúscula, minúscula, números y algún símbolo. Como medida para fortalecer la implementación de la seguridad se podrá implementar la doble autenticación ya sea con el uso de mensajes SMS, algún dispositivo de hardware o en su defecto el uso de algún patrón de validación biométrico como podría ser un lector de huella, de retina o biométricas de teclado. Para esto se deberá:

- **Definir una política de asignación de contraseñas, de su caducidad, así como de la capacitación y concientización a los usuarios sobre el correcto uso y la importancia de su confidencialidad.**

5.3.6 Normas de uso de servicios públicos

El uso de servicios de terceros (por ejemplo internet), puede dar lugar a amenazas de seguridad que pueden vulnerar los sistemas de información, las actividades que lo pueden causar serian el acceso a sitios no seguros, la descarga e instalación de software no seguro o no autorizado, la ejecución de códigos y herramientas maliciosas. Se deben establecer reglas para el uso de estos servicios, limitar el acceso y privilegios solo para los usuarios autorizados.

De igual forma se debe informar al personal sobre los riesgos que llevan el hacer mal uso de estos servicios y el riesgo al que exponen los datos y los sistemas de información como por ejemplo la perdida de información o la encriptación de los datos. Se recomienda revisar los anexos de Ataques y Vulnerabilidades en los Sistemas de Información y el de herramientas para complementar este punto. Para esto se deberá:

- **Restringir el uso de los servicios públicos para todos los usuarios de la organización, definiendo cuáles serán los servicios a los que podrán acceder. Los usuarios autorizados a servicios externos deberán recibir capacitación adicional sobre las consecuencias o amenazas que podrían resultar y de cómo podrán protegerse.**

5.3.7 Normas de seguridad en correo electrónico

El uso de correo electrónico genera importantes amenazas, desde la infección de equipos, la suplantación de identidad, hasta el envío de información sin las debidas medidas de seguridad. Deben de implementarse normas de seguridad para el uso correcto del correo electrónico. El envío de información confidencial deberá estar protegida para evitar el acceso no autorizado por terceros. Se podrá considerar la asignación de un límite de tamaño para archivos en su envío o recepción, el bloqueo de extensiones de tipos de archivos, etc. Se recomienda

revisar los anexos de Ataques y Vulnerabilidades en los Sistemas de Información y el de herramientas para complementar este punto. Para esto se deberá:

- **Restringir el uso de correo electrónico a los usuarios acorde a las necesidades de la organización. Los usuarios autorizados a servicios externos deberán recibir capacitación adicional sobre las consecuencias o amenazas que podrían resultar.**

5.3.8 Formación sobre el maneja de incidencias

Deben existir canales establecidos para informar, lo más rápidamente posible, de los incidentes relativos a la seguridad y al mal funcionamiento de los sistemas de información.

Todos los empleados de la organización, incluidos los externos, deben conocer los procedimientos de comunicación de incidencias, así como las infracciones en materia de seguridad que pueden tener un impacto en la seguridad de los activos de información.

La formación ayudará a la hora de localizar, resolver y analizar las incidencias que ocurren en el sistema de información de la empresa, antes de que el daño producido pueda extenderse o agravarse. Como medida se puede crear un directorio telefónico de emergencias para la notificación de incidentes que requieran una acción rápida. Para esto se deberá:

- **Definir un procedimiento de notificación, gestión y respuesta de incidencias de seguridad y entregar a por escrito a cada usuario sus obligaciones para el cumplimiento de las mismas.**

5.4 Controles Relacionados con los Sistemas de Información

Los controles a considerar en este punto se agrupan en físicos y lógicos, estos deberán definir normas para su funcionamiento y uso.

5.4.1 Seguridad Física Relacionada con el Entorno

Se debe definir un perímetro físico para controlar el acceso no autorizado a la información o los sistemas. De igual forma se debe regular el acceso a dicho perímetro, para ello se deben implementar controles físicos de seguridad de entrada como suelen ser puertas, cerraduras, alarmas, cámaras de vigilancia. El perímetro físico será la primera barrera de protección de los sistemas de información, se debe informar a todo el personal sobre la importancia de estos controles y sus funciones. Se recomienda revisar el anexo de normatividad en el punto de guía de seguridad donde se mencionan las sugerencias a implementar de controles físicos de acceso. Para esto se deberán:

- **Definir un perímetro de seguridad con el fin de prevenir los accesos no autorizados. Se deben definir las normas de acceso al interior de dicho perímetro que será únicamente para personal autorizado.**
- **Establecer un adecuado control de los espacios de acceso público, considerando en ellos el control del acceso de terceros si fuera necesario.**

5.4.2 Protección Contra Amenazas Externas y Ambientales

Se deben definir medidas de seguridad para evitar la pérdida de información total o parcial derivada de desastres naturales que no son controlables por la organización. Se debe analizar los posibles riesgos a los que la organización pudiera enfrentarse y en el caso de equipo crítico, buscar la ubicación más adecuada y segura para resguardar el valor del activo en ciertos casos fuera de la organización (almacenamiento en la nube). Para esto se deberá:

- **Establecer un plan de continuidad del negocio que garantice la recuperación de los sistemas en caso de desastre.**

5.4.3 Seguridad física relacionada con los medios

Se debe definir la forma de identificar el tipo de información que contiene cada uno de los medios utilizados en la organización. Esta identificación debe cubrir medios físicos y lógicos. Los etiquetados deberán llevar una nomenclatura que permita su distinción de forma fácil, es recomendable en su caso manejar códigos de colores para tener un elemento visual para su identificación. Estos códigos deberán permitir identificar el tipo de información que contienen, ser inventariados y estar en un lugar de acceso restringido. De igual forma todo activo debe ser identificado e inventariado. Para esto se deberá:

- **Crear un inventario de medios de almacenamiento, equipo de cómputo y etiquetarlos de acuerdo a las normas o códigos establecidos en la política de seguridad.**

5.4.4 Salidas de activos con datos de las instalaciones

Se deben definir los mecanismos para las salidas y entradas de activos, con la finalidad de controlar los movimientos de los mismos fuera del perímetro establecido en las instalaciones de la organización es especial con equipos que contengan datos o configuraciones . La entrada de activos es importante registrarla debido a que pudieran contener malware que al ser conectado dentro de la organización podría poner el peligro otros activos y los sistemas de información.

Se recomienda el uso de formatos de salida y entrada (o uso de sistema de control) de activo donde quede establecido quien es el responsable y la previa autorización del responsable del departamento, la fecha y hora de salida/entrada así como el motivo por el cual es necesaria su salida/entrada. Para esto se deberá:

- **Crear una bitácora de registro para la salida y entrada de activos, la finalidad de su salida o entrada, la fecha, hora y la**

respectiva autorización del responsable del departamento, todo esto como requisitos mínimos.

5.4.5 Medidas de reutilización / eliminación de medios de almacenamiento

Se deben definir los procedimientos para los medios que se reutilizan y de cómo debe ser el proceso de eliminación y borrado para evitar posteriores accesos no autorizados a la información almacenada. Por ejemplo las empresas pertenecientes al sector financiero se someten a un estándar que indica la cantidad de veces que debe ser borrado un disco duro para así garantizar que la información no podrá ser recuperada. Para activos de tipo desechable también deben de establecerse políticas para su destrucción antes de ser tirados a la basura.

En el caso de la documentación digital se recomienda el uso de una herramienta para su eliminación segura y que se garantice que esta no se pueda recuperar. Para esto se deberá:

- **Establecer los procesos formales para la eliminación y reutilización de medios de almacenamiento para garantizar la confidencialidad de la información almacenada en ellos, estos deberán estar definidos en la política de seguridad.**

5.4.6 Norma de uso de dispositivos móviles y medios extraíbles

Los dispositivos móviles (portátiles, agendas electrónicas, tablets, pc, laptops etc.) así como los medios extraíbles (USB, discos duros portátiles, teléfonos, cámaras) generan vulnerabilidades en la seguridad del sistema de información, debido a su facilidad de uso, alta movilidad, capacidad de almacenamiento y políticas permisivas por parte de las organizaciones, que permiten el flujo de información albergada en los soportes sin control alguno.

La tendencia creciente BYOD (bring your own device) requiere controles necesarios para no vulnerar los datos, un ejemplo de estos tipos de controles es el

uso de servicios web, donde aunque se acceda desde un dispositivo personal, los datos generados y los accesos siguen siendo en los servidores de la organización.

Se recomienda el uso de herramientas para la encriptación o cifrado de datos contenidos en estos medios. Para esto se deberá:

- **Establecer normas de uso de dispositivos y medios extraíbles que garanticen la confidencialidad de la información almacenada en ellos y la seguridad de los equipos con los que interactúan.**

5.4.7 Mantenimiento de equipos

Se deben establecer calendarios de mantenimientos preventivos/correctivos y los controles necesarios para mantener limpio y bien configurado el equipo. El personal encargado de realizar los mantenimientos debe estar capacitado para esta tarea y conocer las políticas de privacidad de la organización. El periodo de mantenimiento se recomienda sea de al menos 2 veces por año. Para esto se deberá:

- **Establecer procedimientos de mantenimiento de equipo de cómputo y la forma de verificación de que son realizados en tiempo y forma.**

5.4.8 Protección contra fallos en el suministro energético

Se debe generar un plan de contingencia ante fallas del suministro eléctrico, deberá contener las características de los equipos que se usaran de respaldo y las acciones posteriores a los cambios. La recomendación es que los equipos estén protegidos contra picos de voltaje y batería que permita guardar cambios y apagar los equipos. Para esto se deberá:

- **Diseñar la arquitectura del sistema de suministro eléctrico incluyendo las acciones a realizar en caso de ser necesaria la implementación de un equipo de respaldo.**

5.5 Seguridad Lógica en los Sistemas

Se deberán estudiar las necesidades del negocio para la implementación de nuevos sistemas de información o mejoras a los existentes, especificando las exigencias de seguridad.

Se recomienda hacer uso de los servicios online que lista las vulnerabilidades respecto a sistemas operativos y su gravedad. Para esto se deberá:

- **Como paso previo a la adquisición de software, se deben definir los requisitos de seguridad mínimos que el software debe garantizar y probar que se cumplen.**

5.5.1 Actualizaciones de software

Implantación de medidas

Se debe definir un procedimiento de actualización del software instalado en la empresa, estableciendo el cauce de recepción de parches y actualizaciones.

- Empleo de procedimientos de control de cambios formales.
- Cuando se realizan cambios y/o actualizaciones en sistemas de información cruciales para la organización, éstos se deberán probar previamente para asegurar que no hay ningún impacto adverso sobre operaciones de organización o su seguridad.

Se recomienda verificar que este configurado el proceso de actualizaciones automáticas en los equipos, esta característica viene incluida en todos los sistemas operativos. Se recomienda la creación de un entorno de pruebas que permita

garantizar posteriormente que la actualización no generará fallas en un futuro. Para esto se deberá:

- **Definir un procedimiento de actualización de software, instalación de parches y de equipos, asegurando que dichas actualizaciones se han probado previamente a su puesta en producción.**

5.5.2 Protección contra código malicioso

Se deberán poner en marcha medidas para la detección, prevención y recuperación del sistema frente a código malicioso, así como procedimientos para crear conciencia en los usuarios.

Instalar en todos los equipos antivirus y mantenerlo actualizado, también establecer normas para solo el software legal y autorizado por la empresa sea instalado en los equipos del sistema de información. Para esto se deberá:

- **Definir un procedimiento de elección, instalación y actualización de antivirus en la organización, desarrollando actuaciones de formación y concienciación complementarias a usuarios para evitar la entrada de código malicioso.**

5.5.3 Copias de seguridad

Una estrategia de copias de seguridad adecuada, es la forma más efectiva contra posibles desastres que puedan afectar al sistema de información de la organización.

Establecer procedimientos para la gestión de copias de seguridad, que permitan recuperar en su totalidad los datos y configuración de los sistemas al instante anterior a la pérdida de datos. Las copias de seguridad tendrán que estar incluidas en el inventario de medios.

Se recomienda el uso de una herramienta para la administración de copias de seguridad. Este tipo de herramientas vienen incluidas con el sistema operativo aunque no vienen habilitadas por default. En el caso de las máquinas virtuales se puede hacer uso de los snapshots para la recuperación de las configuraciones y estatus de los equipos en el transcurso del tiempo o al modificar alguna configuración especifica. Para esto se deberá:

- **Establecer una política para la creación de copias de seguridad que garanticen la reconstrucción de los datos y configuración de los sistemas al instante anterior de la pérdida de información.**

5.5.4 Seguridad Lógica en las Comunicaciones

Establecer mecanismos para la identificación automática de los equipos al acceder al sistema de información, autenticando así las conexiones desde terminales determinados.

Se recomienda el tener una herramienta de monitoreo hacia las conexiones de los sistemas de información. Estas herramientas son conocidas como detectores de intrusos. Para esto se deberá:

- **Para aquellas organizaciones que permiten tener accesos externos a su sistema de información se debe establecer un sistema de identificación de los equipos externos para garantizar que el acceso está autorizado.**

5.5.5 Cifrado

Una política de empleo de controles criptográficos para la protección de información debería ser desarrollada y puesta en práctica.

Los controles criptográficos deberían ser usados desde el cumplimiento con todos los acuerdos relevantes, leyes y regulaciones.

Para este punto se recomienda el uso de una herramienta para el cifrado de datos y validación de documentos, usando firmas digitales o llaves públicas. Para esto se deberá:

- **Definir un procedimiento de cifrado de la información que garantice la confidencialidad de los datos.**

5.6 Controles relacionados con la Revisión del sistema

Las medidas de seguridad que se deben aplicar al sistema de información para permitir una adecuada revisión de los sistemas y medidas implantadas. Todo esto cumpliendo respetando el principio de trazabilidad o contabilidad.

5.6.1 Sincronización de relojes

La correcta sincronización de relojes de los procesadores es esencial para la exactitud de los datos reflejados en los archivos de registro (logs y registros de auditoria) y para la realización de auditorías, investigación de incidencias, o como prueba en casos legales o disciplinarios. La inexactitud de los registros de auditoría puede inutilizar las evidencias recogidas.

Los relojes de todos los sistemas de informática relevantes de tratamiento de información o de dominio de seguridad, deberán ser sincronizados con una fuente de tiempo reconocida y exacta.

Se recomienda verificar la configuración del sistema operativo, por default se tiene configurada la fecha y hora con los servidores de internet. Para esto se deberá:

- **Configurar y sincronizar los relojes de los servidores y equipos acorde a la zona horaria de la organización.**

5.6.2 Control de registros de acceso

- Los errores de acceso deberán ser registrados, analizados y servir como soporte para llevar a cabo acciones correctivas.
- Las actividades de auditoría y verificación de sistemas operacionales deberán ser planificadas para evitar interrupciones en los procesos de negocio.
- Los registros de las instalaciones y la información de los logs deberán estar protegidos contra el acceso no autorizado.

Se recomienda el uso de una herramienta que facilite el desglose de información sobre el registro de accesos donde se generen reportes y existan filtrados para mejorar su comprensión, generalmente el sistema operativo cuenta con una. Para esto se deberá:

- **Configurar registros de acceso que contengan la identificación de los accesos al sistema.**

Un ambiente de pruebas seguro permite generar casos de estudio donde se pueden practicar diferentes configuraciones sin el riesgo de afectar los equipos en producción. La recomendación es la creación de ambientes virtuales que permitan realizar estos cambios experimentales, documentar su comportamiento y posteriormente recomendar si se considera pertinente la actualización o implementación del caso de estudio probado en el entorno. En ciertos casos las herramientas virtuales permiten en migrar lo virtual a lo físico para facilitar su implementación. Para esto se deberá:

- **Definir un procedimiento para la creación de un entorno de pruebas seguro.**

El monitoreo de los sistemas de información y de los servidores debe ser una tarea a ejecutar continuamente, el éxito en la prevención de un problema estará marcado por la adecuada identificación de incidencias detectadas y por su debida notificación a los responsables de cada sistema o servidor. Para esto se deberá:

- **Definir un procedimiento para el monitoreo de los sistemas de información y los servidores.**

6. IMPLEMENTACIÓN

La implementación de la presente metodología se realizó en las instalaciones del Centro de Desarrollo de la Facultad de Informática de la UAQ, departamento dedicado al desarrollo de software que se implementa dentro de la Facultad, la Universidad y a externos. Sus principales desarrollos son aplicaciones Web y su personal está conformado principalmente por alumnos y 3 maestros, toda la infraestructura, software y personal es administrado por los tres maestros con la excepción de las comunicaciones de voz/datos las cuales son proporcionadas y gestionadas por el departamento de informatización de la Universidad Autónoma de Querétaro. El cuestionario se aplicó para evaluar el nivel de seguridad al interior del departamento. El cuestionario se aplicó para evaluar el nivel de seguridad al interior de dicho departamento.

En el resultado final del diagnóstico mostrado en la siguiente imagen, se puede observar que la categoría de mayor puntuación fue la seguridad orientada al software, mientras que las otras 4 categorías predomina el “No”.

Figura 6-1 Resultado implementación metodología. Fuente: Elaboración propia.

La recomendación en este diagnóstico fue la de implementar los controles necesarios para fortalecer las categorías restantes tales como seguridad física, la relacionada al personal y la orientada a la verificación.

7. CONCLUSIONES

Después de realizar la presente investigación se llegó a las siguientes conclusiones:

La seguridad es el resultado de un proceso cuyo éxito depende del compromiso de cada uno de los actores que componen una organización.

No es posible llegar a un punto de nulidad de riesgo pero se pueden identificar las posibles amenazas y oportunidades y tomar acciones sobre ellas.

El marco normativo que rige nuestro país necesita llevar un proceso de cambio para adaptarse a las nuevas tecnologías, en el periodo de esta investigación se pudo identificar como ha ido madurando e incluso se tiene aprobada la creación de un código penal único para corregir las deficiencias y brechas entre un código penal de un estado y otro, pero aunque se tiene aprobado no se tiene una fecha de implementación.

La metodología depende en su mayoría del compromiso de las personas, estas son la parte más vulnerable en la seguridad de los sistemas de información, es posible implementar lo último en tecnología para proteger los sistemas pero sin el compromiso del factor humano dicha tecnología no podrá cumplir su propósito.

El desarrollo de una metodología que abarque todo el proceso de seguridad y las herramientas para cada proceso es una tarea complicada, por lo cual se recomendaron características a cumplir y no cerrarse solo a una herramienta.

La adquisición de herramientas que ayuden en la tarea de verificación de vulnerabilidades es bastante costosa, el encontrar herramientas de uso libre es más complicado y por lo general no existe soporte en su implementación.

Es poca la difusión que existe en nuestro país sobre la importancia de implementar seguridad en una organización, de momento está más enfocado a la protección de datos personales.

8. REFERENCIAS

Alonso, C. (2013). Pentesting con FOCA. En C. Alonso, *Pentesting con FOCA* (pág. 240). España: OxWord.

Briones, G. (2002). *Metodología de la investgación cuantitativa en las ciencias.* Bogota Colombia: INSTITUTO COLOMBIANO PARA EL FOMENTO DE LA EDUCACION SUPERIOR.

C. Laudon Kenneth, P. L. (1997). *Administración de los sistemas de Información, organización y tecnología .* USA: Prentice Hall.

Cano, J. (2009). *Computación Forense. Descubriendo los rastros informáticos.* México: Alfa Omega.

Cassou, R. J. (09 de noviembre de 2015). *Revista del Instituto de la Judicatura Federal No. 28.* Obtenido de Instituto de la Judicatura Federal Escuela Judicial: http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

El financiero. (21 de Septiembre de 2011). *75% de las Pymes, sin seguridad Informática*. Obtenido de El financiero.com: http://www.elfinanciero.com.mx/index.php/economia/pymes/15735-75-de-las-pymes-sin-seguridad-informatica

Garrido, J. (2012). Análisis Forense Digital en Entornos Windows. En J. Garrido, *Análisis Forense Digital en Entornos Windows* (pág. 238). España: Informatica 64.

González, P. (2013). Metasploit para pentesters. En P. González, *Metasploit para pentesters* (pág. 284). España: 0xWord.

González, P. (2013). Pentesting con Kali. En P. González, *Pentesting con Kali* (pág. 250). España: 0xWord.

KPMG. (2010). *Encuesta de Fraude en México*. Obtenido de http://www.kpmg.com/MX/es/IssuesAndInsights/ArticlesPublications/Documents/Estudios/Encuesta_fraude_en_Mexico_2010.pdf

Pacheco, F. (2009). Ethical Hacking. En F. Pacheco, *Ethical Hacking* (pág. 320). Argentina: Manual Users.

Pacheco, F. J. (2009). *Hacking, Ethical.* Argentina: Manual Users.

Rando, E. (2012). Hacking con buscadores, Google, Bing & Shodan. En E. Rando, *Hacking con buscadores, Google, Bing & Shodan* (pág. 292). España: Informatica 64.

Sallis E., C. C. (2010). *Ethical Hacking.* Argentina: Alfa Omega.

Téllez, V. J. (2009). Derecho Informático. En V. J. Téllez, *Derecho Informático* (pág. 636). Mexico Df: Mc Graw Hill.