UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM TEXCOCO

“GUÍA OPERATIVA PARA LA PROTECCIÓN DE DATOS INFORMÁTICOS EN EMPRESAS MEXICANAS”

T E S I N A

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN INFORMÁTICA ADMINISTRATIVA

PRESENTA
GRECIA VELASCO GONZÁLEZ

ASESORA
Lic. en I. A. Cinthya Teresita Islas Rodríguez

REVISORES
M. en C.C. Ma. Dolores Arévalo Zenteno
M. en C. Josué Vicente Cervantes Bazán

TEXCOCO, ESTADO DE MÉXICO, OCTUBRE DE 2017.

Texcoco, México a 21 de agosto de 2017

M. EN C. E. VIRIDIANA BANDA ARZATE
SUBDIRECTORA ACADEMICA DEL
CENTRO UNIVERSITARIO UAEM TEXCOCO.
PRESENTE:

AT´N L. EN D. MARCO RODRIGO LÓPEZ GONZÁLEZ
RESPONSABLE DEL DEPARTAMENTO DE TITULACIÓN.

Con base en las revisiones efectuadas al trabajo escrito titulado " GUIA OPERATIVA PARA LA PROTECCIÓN DE DATOS INFORMÁTICOS EN EMPRESAS MEXICANAS" que para obtener el título de Licenciado en Informática Administrativa presenta la sustentante Grecia Velasco González, con número de cuenta 1124730 respectivamente, se concluye que cumple con los requisitos teóricos-metodológicos por lo que se le otorga el voto aprobatorio para su sustentación, pudiendo **continuar con la etapa de digitalización** del trabajo escrito.

ATENTAMENTE

M. en C. Josué Vicente Cervantes Bazán.

M. en C.C. Ma. Dolores Arévalo Zanteno

L. en I. A. Cinthya Teresita Islas Rodríguez

c.c.p. INTERESADO GRECIA VELASCO GONZÁLEZ.
c.c.p. DIRECTOR L. EN L. A. CINTHYA TERESITA ISLAS RODRIGUEZ.
c.c.p TITULACIÓN L. EN D. MARCO RODRIGO LÓPEZ GONZÁLEZ.

TITULACION
RECIBIDO
Por González
Texcoco, Méx., 21 de Ago de 17

RESUMEN.

Para el presente trabajo, se planeó como objetivo general elaborar una guía para proteger la información informática de las empresas en México, en segundo momento de la investigación, se abordaron los objetivos específicos que consisten en recolectar datos en empresas en cuanto a seguridad informática, investigar y listar los posibles delitos informáticos, delimitar los principales delitos cibernéticos en México, analizar las tendencias de los principales ataques más usados en las empresas mexicanas, además determinar el impacto de los ciberdelitos en el entorno empresarial mexicano, por último se elaborará elaborar una guía de referencias que contenga información acerca de los delitos informáticos y como prevenirlos, enfocado al usuario. Todo esto con base a dicha investigación previa.

INTRODUCCIÓN

Con la creación de los sistemas de información, se genera la necesidad de tomar medidas preventivas en ellos, para proteger su integridad, pues, así como hay sistemas que garantizan la confidencialidad de los datos, también existe ciberdelitos cuyo propósito es variado va desde el sabotaje, hasta la destrucción de datos y alteraciones del funcionamiento de las computadoras.

Los ciberdelitos que tiene como objeto alterar el normal funcionamiento en las computadoras sin previo conocimiento de los usuarios; y para combatir este problema se hace indispensable contar con protección para combatir cualquier riesgo que pueda ocurrir.

Las causas por los ciberdelitos, riesgos que se pueden prevenir con una buena información. Que un manual sea bueno o malo es relativo, pues los usuarios son quienes finalmente deciden como poner en práctica lo de dicho manual para protección, decisión que deben tomar, para saber qué es lo que ajusta a las necesidades, además de tener conocimiento de cómo funciona y actúan los ciberdelitos, ya que de ellos también depende el tipo de protección que se debe dar al sistema para que no quede expuesto.

El capítulo 1 contiene el contexto de la investigación, la definición del problema, la justificación y los objetivos respectivamente. El capítulo 2 contiene el marco teórico, en él se tratan temas como Investigación de ciberdelitos y tendencias en México.

En el capítulo 3 se habla sobre el Respaldo Legal de delitos Informáticos en México, seguido del capítulo 4 donde se menciona sobre el Impacto de los delitos Informáticos en el área Empresarial.

El capítulo del 5 se mencionan los tipos de virus, la manera en que operan y la forma en que se puede prevenir. El capítulo 6 incluye un manual de prevención del delito informático para empresas en México, y por último el capítulo 7 y 8 comprenden del diseño metodológico, las conclusiones y la bibliografía respectiva.

Dedicatoria.

Dedico este trabajo con toda humildad principalmente a Dios, el que me ha dado fortaleza y sabiduría para continuar cuando a punto de caer he estado.

A mi madre Ma. Guadalupe González Montalvo, por ser el pilar más importante de mi vida, por demostrarme siempre su amor y su apoyo incondicional, a ella quien ha sabido formarme con buenos sentimientos, hábitos y valores, los cuales me han ayudado a salir adelante en todo momento.

A Mamá Adelita y Papá Rodrigo, por ser mi ejemplo de vida, por fomentar en mi la valentía, el amor, la madurez y la fortaleza ante cualquier situación, por ser mi hogar, mi familia.

A mi hermano Gerardo que siempre ha estado junto a mí y brindándome su apoyo, muchas veces poniéndose en el papel de padre.

A Joel S. G. por su tiempo, por su apoyo, por su cariño, por compartir momentos de alegría, tristeza y demostrarme que siempre puedo contar con él.

Los amos.

Agradecimientos.

A Dios.

Gracias por haberme acompañado y guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizaje, experiencias y sobre todo felicidad.

A mi madre Ma. Guadalupe.

Gracias por apoyarme en todo momento, por lo valores que me has inculcado, y por haberme dado la oportunidad y las herramientas de tener una educación en el transcurso de mi vida. Sobre todo, por ser mi guerrera, quien no se rinde que da todo de si por los suyos, por ser un excelente ejemplo de vida a seguir.

Mamá Adelita

Gracias por ser mi fortaleza, mi apoyo, mi amiga, mi confidente, gracias por tu amor, paciencia y esfuerzo de toda la vida, por ser una luchadora incansable, por ser una mujer extraordinaria.

Papá Rodrigo.

Gracias por ser mi papá, mi maestro, gracias por compartir tu sabiduría, gracias por tu apoyo, tus consejos, tu manera de educarme, por creer en mí y sobre todo por tu infinito amor.

A mi hermano Gerardo.

Gracias por ser mi sigiloso guardián y compañero, por cuidarme y estar ahí cuando te necesito, por tu cariño.

A mi tía Norma

Por tu apoyo, por tener una palabra de aliento cuando lo he necesitado.

A Joel Soriano G.

Gracias por tu infinita paciencia, por tu tierna compañía y tu inagotable apoyo. Gracias por compartir mi vida y mis logros, por ayudarme a crecer, a ser mejor persona, a confiar en mí, porque siempre das lo mejor, porque juntos somos un buen equipo.

A mis sobrinos Santiago y Marilú.

Gracias por cada sonrisa, por cada gesto de amor que emanan, por ser una luz en mi camino, por contagiarme su fascinación por la vida, y para que ellos sepan que en la vida se puede lograr lo que uno se proponga.

A mis primas Mishell y Monse.

Gracias por ser mis compañeras de muchas alegrías, por su cariño y apoyo, por ser como mis hermanas.

A todos mis tíos y primos.

Porque han formado parte de mi vida, de grandes enseñanzas, por el apoyo que entre todos nos brindamos en momentos duros, por cada palabra de aliento.

A mis Profesores.

En especial a, Cinthya Teresita Islas Rodríguez, Ma. Dolores Arévalo Zenteno y a Josué Vicente Cervantes Bazán quienes han trabajado a la par conmigo en la realización de este proyecto, por su paciencia, por su manera de motivarme. Gracias por ser mi guía, a quienes me dieron palabras de aliento para no bajar la guardia, quienes ahora hacen de mí una mejor persona.

A mis compañeros.

En especial a mi amiga Bety, por ser quien ha estado en los momentos que me han llevado hasta aquí, por tu fiel amistad, comprensión y apoyo.

A la U.A.E.M

Por ser mi casa durante el tiempo de estudio y darme las facilidades para crecer.

Con todo mi cariño Grecia.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

Capítulo 1. Contexto de la investigación.

En este capítulo se hablará sobre el contexto de la investigación, en términos de la problemática, la justificación, asimismo el objetivo general como los objetivos específicos de lo que va tratar el proyecto y así poder comprender de que va a tratar dicho proyecto.

1.1. Problemática

Definición de ciber delitos, es una actividad ilegal realizada a través del computador, existe un desacuerdo con respecto a un lugar en el que se ejecuta. (Chung, Chenb, & Changc, 2004). Otras definiciones pueden encontrarse en la literatura, Power asume como la intromisión sin autorización de un computador (Power, 2002).

En el argot informático el termino hacker se refiere a una persona que busca crear seguridad a partir de inseguridades informáticas. Por otra parte, un ciber delincuente usa herramientas informáticas para cometer delitos.

Algunos de los más importantes delitos en México son: Violaciones de datos en punto de venta (PoS), Ataque dirigido, entre otros según el artículo Tendencias de Seguridad Cibernética en América Latina y el Caribe (Symantec, 2014). Es por eso que este manual se enfocará en estos delitos.

Algunas empresas no cuentan con el departamento de seguridad informática, además de que no cuentan con un manual de seguridad. Por lo que este trabajo de investigación se desarrollará un Manual Genérico para el manejo de Seguridad en las empresas mexicanas incluyendo las tendencias de seguridad informática.

1.2. Justificación

Miembros de la Organización de los Estados Americanos (OEA) reconocieron formalmente que combatir los delitos cibernéticos y fortalecer la resiliencia cibernética era cuestión imperativa para el desarrollo económico y social, se debe contar con la capacidad de prevenir, mitigar responder, investigar y procesar de manera efectiva las conductas criminales, cuando sea pertinente, asimismo las autoridades deben promover la creación de una cultura de la seguridad cibernética y emprender acciones de concientización en esa materia para proteger a los

usuarios “quienes en el mundo actual están cada vez más expuestos”, con el fin de dotarlos del conocimiento que necesitan para proteger su información. (MICRO, 2013).

El ciber espionaje, las preocupaciones en materia de privacidad y el personal interno malintencionado fueron noticia y ocuparon un lugar destacado en las discusiones sobre seguridad cibernética en 2013. No obstante, varias violaciones de datos siguen proliferando y que las amenazas de los ciberdelincuentes siguen acechando a gobiernos, empresas y usuarios finales. Los delitos cibernéticos continuaron devengados grandes beneficios, mientras que la perspectiva de captura a los hackers y estafadores en línea demostraron ser limitada en todas las jurisdicciones. Estos factores fueron parte responsable de los altos costos por dichos motivos, se estima que ascendieron a por lo menos USD 113, 000 millones, suma suficiente para comprar un iPad a toda la población de México, Chile, Colombia y Perú, solamente en Brasil, los costos de los delitos cibernéticos alcanzaron los USD 8,000 millones, seguidos por México con USD 3,000 millones y Colombia con USD 464 millones. (Jason Kohn, 2013).

El problema de la seguridad Informática se hace más grave con la evolución del internet y de las empresas por el manejo de datos, cada vez es más generalizado.

Los costos de las herramientas de protección son más accesibles, esto hace que la implementación de mecanismos de seguridad se dé en todos los niveles. Pero no es cuestión de costos, los constantes cambios de la tecnología hacen que, para mantener un nivel de seguridad, se deben actualizar permanentemente las herramientas con las que cuentan las empresas. Por lo que los hackers mejoran sus metodologías de penetración de manera rápida, pues la revisión constante en los mecanismos de seguridad es imprescindible.

La necesidad de conocer las características, riesgos y alcances de los ciberdelitos son de suma importancia para las empresas, así se podrá evitar que las organizaciones puedan estar en peligro de alguna violación a sus datos.

Estas son razones suficientes para desarrollar esta investigación y presentar un manual que posiblemente mitigue las inseguridades informáticas de una empresa en México. (Jason Kohn, 2013).

1.3 Objetivos

1.3.1. General

Elaborar una guía para proteger la información informática de una empresa y/u organización, en cuanto a ataques cibernéticos, su procedimiento de acción y prevención del delito.

1.3.2. Particulares

- Recolectar de datos en empresas en cuanto a seguridad informática.
- Investigar y listar los posibles delitos informáticos.
- Delimitar los principales delitos cibernéticos en México.
- Analizar las tendencias de los principales ataques más usados en las empresas mexicanas.
- Determinar el impacto de los ciberdelitos en el entorno empresarial mexicano.
- Elaborar una guía de referencias que contenga información acerca de los delitos informáticos y como prevenirlos, enfocado al usuario.

Capítulo 2. Tendencias de ciberdelitos en México.

Resumen.

En el siguiente capítulo, se presenta los conceptos básicos necesarios para la comprensión de este trabajo, así como una descripción de delito y ciberdelito, poniendo énfasis en el contexto de los tipos de ciberdelito que estos presentan y sobre los ataques dirigidos que estos presentan. Además de mencionar las diferentes maneras que son más utilizados para realizar su detección.

Objetivos del Capítulo.

- Definir los conceptos básicos necesarios para la compresión del ciberdelito.
- Presentar un panorama general sobre la tipología del ciberdelito.

2.1. ¿Qué es un delito?

Es una conducta humana que se opone a lo que la ley manda o prohíbe bajo la amenaza de una pena; Es la ley la que establece que hechos son delitos, es la ley que denomina que hecho se va a considerar como delito, es la ley la que designa y fija delictuales a un hecho. (Machicado, 2010).

2.1.1. Ciberdelitos

Una definición bastante común de ciberdelito es cualquier actividad delictiva en la que se utilizan como herramientas computadores o redes, o en la que estos son las víctimas de la misma o el medio desde donde se efectúa dicha actividad. (Gordon/Ford, 2006).

Según (KPMG, 2014), ciberdelito se define, como un conjunto de actividades ilícitas que se llevan a cabo para, robar, alterar, manipular, enajenar o destruir información o activos (como dinero, valores, bienes desmaterializados) de las compañías afectadas, utilizando para dicho fin algún medio informático o componentes electrónicos. La lucha contra el ciberdelito exige un enfoque global. Teniendo en cuenta que las medidas técnicas únicamente no pueden evitar ningún delito, es fundamental que se permita a las autoridades competentes investigar y perseguir el delito de manera efectiva. (Gercke, 2014).

2.1.2. Tipos de Delitos.

Delitos	Ejemplo
Delito contra la vida y la integridad corporal y contra la familia.	Homicidio. Lesiones. Ayuda o inducción al suicidio. Aborto. Abandono de personas. Violencia familiar.
Delitos relacionados con el manejo de información humana.	Procreación asistida e inseminación artificial. Manipulación genética.
Delitos contra la libertad personal y el normal desarrollo psicosexual.	Privación ilegal de la libertad y otras garantías. Secuestro. Tráfico de menores. Violación Hostigamiento sexual. Estupro Incesto
Delitos patrimoniales	Robo. Abuso de confianza. Fraude. Administración Fraudulenta. Extorsión Despojo Daño a la propiedad.
Delitos contra la salud	Producción, tenencia, transporte y comercio de narcóticos. Posesión de narcóticos. Siembra, cultivo, cosecha, acondicionamiento de narcóticos. Narcomenudeo y otras modalidades.
Corrupción de menores e incapaces	Pornografía infantil, incapaces que no tienen capacidad para comprender el significado del hecho o que no tienen capacidad para resistirlos. prostitución de menores. Turismo sexual. Lenocinio y trata de personas.
Delitos cometidos por servidores públicos	Ejercicio indebido del servicio público. Abuso de autoridad. Desaparición forzada de personas. Coalición de servidores públicos. Concusión. Ejercicio abusivo de funciones.

	Tráfico de influencias. Cohecho Cohecho a servidores públicos extranjeros. Peculado Enriquecimiento ilícito.
Delito contra la fe pública.	Falsificación de documentación. Falsificación de moneda. Falsedad ante la autoridad.
Encubrimiento y operaciones con recursos de procedencia ilícita.	Encubrimiento. Operaciones con recursos de procedencia ilícita.
Delitos contra la biodiversidad y el medio ambiente.	Delitos contra la biodiversidad. Delitos contra el medio ambiente.

Ilustración 1 Tipos de Delito.

2.1.3 Tipología del ciberdelito

El término “ciberdelito” abarca muy diversos tipos de delitos. Los delitos reconocidos comprenden una gran variedad de infracciones, lo que dificulta su tipología o clasificación. Un sistema de clasificación interesante es, el definido por el Convenio sobre la Ciberdelincuencia, en el que se distingue cuatro tipos diferentes. (Pulse, 2012).

- Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos.
- Delitos informáticos.
- Delitos relacionados con el contenido.
- Delito relacionado con el derecho del autor. (Gercke, 2014).

Esta clasificación no es totalmente coherente ya que se basa en un solo criterio para diferenciar las categorías. Tres de las categorías se refieren al objeto de la protección jurídica. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, delitos informáticos, no se refiere al objeto de la protección jurídica sino al método. Esa incoherente genera cierta coincidencia entre las categorías. (Gercke, 2014).

Capítulo 3. Respaldo Jurídico en contra de delitos Informáticos en México.

Resumen.

En el presente capítulo trata sobre la Legislación Informática la cual es definida, a su vez se analiza los tipos más importantes de ciberdelitos que necesitan ser regulados, por otra parte, se menciona de que manera se pueden proteger los datos y la sanción que se da de acuerdo a cada delito conforme a los artículos del código penal, y así poder proteger los datos

Objetivos del capítulo.

- Definir Legislación Informática.
- Analizar los principales delitos en México, de acuerdo al código penal.
- Comprender las sanciones que se dan los artículos que están postulados en el código penal, y así poder comprender el contexto del capítulo.

3.1. Legislación Informática.

El derecho surge como un medio efectivo para regular la conducta del hombre en sociedad. Pero la sociedad no es la misma en cada uno de los lugares del planeta ni es la misma en cada momento dela historia. La sociedad evoluciona, cambia a través del avance de la ciencia de la tecnología. (Rio, 2012).

El derecho regula la conducta y los fenómenos sociales a través de leyes. El proceso de creación e inserción de estas leyes a la vida de una comunidad jurídica determinada (en el caso México; municipio, estado, país) es largo y lento, sobre todo en sistema Jurídico. (Rio, 2012).

En los últimos años, las Tecnología de la Información y la Comunicación (TIC) han revolucionado la vida social en numerosos aspectos; científicos, comerciales, laborales, profesionales, escolares, e incluso cambiado los hábitos de entretenimiento y de interrelación de las personas al interior de las organizaciones.

Sin duda alguna, la informática ha tenido una gran evolución, hoy en día es común encontrar en cualquier tipo de organización computadoras que controlan inventarios, caja, etc., y esto nos permite llevar a cabo las actividades más

fácilmente, pero no debemos olvidar aquellos tiempos donde las computadoras y cualquier tipo de sistema informático eran realmente desconocidos. (Leal J. c., 2013).

Los primeros procesos que se intentó llevar acabo con ayuda de sistemas computacionales eran los que se podían presentar de forma matemática; la informática permitió realizar trabajos regularmente monótonos y repetitivos en departamentos dirigidos a puestos administrativos. Realizar estas tareas de forma automática trajo consigo grandes ventajas como la disminución de costo y aumentó en la productividad, siendo estas muy importante para las organizaciones. (Rio, 2012).

La tecnología avanza a una velocidad vertiginosa y el derecho, en especial el derecho mexicano, se ha quedado rezagado en la regulación de una materia que lo ha rebasado. (V. Batíz- Álvarez, 2011).

Con todo esto, se ha llevado a cabo esfuerzos por legislar en la materia y algunos de estos han fructificado, enunciemos los tópicos más importantes que ameritan regulación:

- Delitos Informáticos.
- Firma digital/ electrónica y contratos electrónicos.
- Correo electrónico (privacidad, spam).
- Protección a Base de Datos.
- Computo forense (evidencias electrónicas).
- Protección de propiedad intelectual.
- Regulación de contenidos en Internet.

De acuerdo con el artículo 40 de la Constitución Política de los Estado Unidos Mexicanos, somos una República democrática, representativa y federal, compuesta de Estados Libres y soberanos por lo que se refiere a su régimen interior, pero unidos en un pacto federal.

El poder legislativo, se deposita en un Congreso Federal, el cual tiene facultades exclusivas para legislar sobre: hidrocarburos, minería, industria cinematográfica, comercio, juegos con apuestas y sorteos, intermediación y servicios financieros,

energía eléctrica y nuclear, derecho marítimo ciudadanía, migración, vías generales de comunicación, correo, aguas, moneda, delitos federales, coordinación en materia de seguridad pública, fiscalización superior de la federación, leyes del trabajo reglamentarias del artículo 123 Constitucional. (Rio, 2012).

Los Estados pueden regular, en el ámbito de su competencia, las materias que no están expresamente reservadas a la Federación.

Delitos informáticos en términos jurídicos, para que exista delito es necesario un acto u omisión que sancionen las leyes penales, porque una de las características indispensables del delito es la tipicidad, es decir, que la conducta este descrita en un tipo penal, en una ley penal, además de ser antijuridica, culpable y punible. (Rio, 2012).

Principales delitos informáticos son:

- Fraude mediante el uso de la computadora y la manipulación de la información que estas contienen (técnica del salami u otras).
- Acceso no autorizado a sistemas o servicios (caballo de Troya, back, doors, etc.).
- Destrucción de programas o datos de reproducción no autorizado de programas informáticos.
- Uso no autorizado de programas y de datos.
- Intervención de correo electrónicos.
- Obtención de información que pasa por el medio (sniffer). (Rio, 2012).

ANÁLISIS DE LOS DELITOS.

Fraude mediante el uso de la computadora y la manipulación de la información que estas contienen:

El artículo 230 del Código Penal para el Distrito Federal, regula el delito de fraude: “Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero se le impondrá adelante, el artículo 231 dispone: “se impondrá las penas

previstas en el artículo anterior. Para obtenerte algún beneficio para si o para un tercero por cualquier medio acceso, entre se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valore, independientemente de que los recursos no salgan de la institución.

Aquí habría que valorar si es suficiente la descripción del tipo penal de fraude para ser aplicado o conductas realizadas mediante sistemas o programas de informática cuando no sean estos del sistema financiero sino de cualquier otra empresa, institución o persona.

Por otro lado, también podría considerarse regulado el fraude realizado mediante sistemas o equipos informáticos del sistema financiero en el Código Penal Federal. (V. Batíz- Álvarez, 2011).

ACCESO NO AUTORIZADO A SISTEMAS O SERVICIOS Y DESTRUCCION DE PROGRAMAS O DATOS:

Esta conducta se encuentra regulada en el Código Penal Federal, artículo 211 bis 1 a 211 bis 7, que determina en resumen lo siguiente: (V. Batíz- Álvarez, 2011).

CONDUCTA	PENA
Modificar, destruir provocar pérdida de información contenida en sistemas o equipos informáticos protegidos sin autorización. ▪ Si se trata de sistemas o equipos del Estado. ▪ Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.	6 meses a 2 años de prisión y 100 a 300 días de multa. 1 a 4 años y 200 a 600 días de multa. 6meses a 4 años de prisión y 100 a 600 días de multa.
Conocer o copias información contenida en sistemas o equipos informáticos protegidos sin autorización. ▪ Si se trata de sistemas o equipos del Estado.	3 meses a 1 año de prisión y 50 a 150 días de multa.

▪ Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.	6 meses a 2 años de prisión y 100 a 300 días de multa. 3 meses a 2 años de prisión y 50 a 300 días de multa.
Modificar, destruir o provocar pérdidas de información contenida en sistemas o equipos informáticos cuando se tenga autorización para el acceso. ▪ Si se trata de sistemas o equipos del Estado. ▪ Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.	2 a 8 años de prisión y 300 a 900 días de multa. 6 meses a 4 años de prisión y 100 a 600 días de multa.
Conocer o copiar información contenida en sistemas o equipos informáticos cundo se tenga autorización. ▪ Si se trata de sistemas o equipos del Estado. ▪ Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.	1 a 4 años de prisión y 150 a 450 días de multa. 3 meses a 2 años de prisión y 50 a 300 días de multa

Ilustración 2 Pena de Acuerdo a la conducta.

Las penas se encontrarán en una mitad cuando las conductas se realicen por empleados del sistema financiero y se incrementarán hasta en una mitad cuando la información obtenida se realice en provecho. (V. Batíz- Álvarez, 2011).

- REPRODUCCION NO AUTORIZADA DE PROGRAMAS INFORMATICOS:

Regula la ley Federal del Derecho de Autor, articulo 11 que establece el reconocimiento del Estado al creador de obras literarias o artísticas, entre las que, conforme al artículo 113 fracción XI, están los programas de cómputo los cuales a igual que las bases de datos quedan protegidos por las disposiciones de la Ley de la misma forma que las obras literarios, en el sentido de que los autores tienen los derechos patrimoniales y morales sobre sus obras (explotación, reproducción, publicación, exhibición, acceso, distribución, divulgación, reconocimiento de la calidad de autor, modificación y respeto a la obra) así como la facultad de transmitir esos derechos. (Rio, 2012).

El Titulo Cuarto de la Ley, que habla de la Protección al Derecho de Autor, regula en su Capítulo IV, (artículo 101al 114) los programas computación y las bases de datos, establecidos “se entiende por programas de computación la expresión original en cualquier forma lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea y función específica”.

La ley aplica la protección a los programas tanto operativos como aplicativos y deja afuera a los que tienen por objeto causar efectos nocivos. Autoriza al usuario legitimo a hacer las copias que le permitan la licencia, o bien, una sola que sea indispensable para la utilización del programa o sea destinada exclusivamente como resguardo. El autor tiene el derecho de autorizar o prohibir además de la reproducción, la traducción, adaptación arreglo o cualquier modificación al programa o reproducciones del resultante, la distribución, la recopilación (Proceso para revertir la ingeniería del programa) y el desembalaje. (V. Batíz- Álvarez, 2011).

Las violaciones a las anteriores disposiciones constituyen una infracción en materia de comercio, que son sancionadas por el Instituto Mexicano de Propiedad Intelectual con multa, que va desde 500 hasta 5000 días de salario dependiendo del tipo de infracción, además de poder efectuar visitas, pedir información y aplicar las medidas precautorias que estimen convenientes (aseguramiento de bienes).

Asimismo el Código Penal Federal, en sus artículos 424 al 429, tipifica como delitos y sanciona, entre otras, las conductas descritas en este inciso mencionado que impondrá de 6 meses a seis años de prisión y de 300 a 3000 días de multa al que use firma dolosa y con fines de lucro las ogras protegidas por la Ley Federal del Derecho de Autor, o bien, 2 a 10 años de prisión y dos mil a 20 000 días de multa al que produzca o reproduzca (entre otros actos) sin autorización y con fin de lucro obras protegidas por la Ley Federal de Derecho de Autor, así como aquel que fabrique con fines de lucro, dispositivos o sistemas diseñados para desactivar los dispositivos electrónicos de protección de un programa de computo. Se impondrá de 6 a 4 años de prisión y de 300 a 3000 días de multa al que fabrique, importe, venda o arriende algún sistema o dispositivo destinado a descifrar señales cifradas

de satélite que contengan programas o realice con fin de lucro cualquier acto destinado al mismo efecto, sin autorización del distribuidor de la señal.

- USO NO AUTORIZADO DE PROGRAMS DE DATOS:

La Ley Federal del Derecho de Autor, en sus artículos 107 al 110, protege como compilaciones a las bases de datos legibles por medio de máquinas que por razones de disposición de su contenido constituyan obras intelectuales, otorgándole a sus organizador el uso exclusivo por cinco años, asimismo, exceptuando las investigaciones de autoridades la información privada de las personas contenidas en bases de datos no podrán ser divulgadas, trasmitida ni reproducida salvo con el consentimiento de la persona de que se trate.

La ley determina los principios bajo los cuales deberá manejarse los datos personales, entre los que destacan los siguientes:

- Solo podrán obtenerse y ser ejecutados de tratamiento cuando sea adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades expresas y legitimas para las que se hayan obtenido.
- Deben ser correctos y actualizados, de modo que reflejen fielmente la situación del afectado.
- Deberán obtenerse por medios lícitos que garanticen el derecho a la intimidad de la persona, informando previamente al interesado de la existencia del archivo y sus derechos a acceder a este, así como a oponerse o cancelarlo.
- Será necesario el consentimiento del interesado para cualquier tratamiento de sus datos, excepto cuando se trate del ejercicio de las funciones propias de la administración pública la información conste en necesarios para tratamiento médico del interesado.
- Quienes por razones de su oficio o labor maneje de otros están obligados a hacerlo confidencialmente.
- El responsable del archivo garantizara el establecimiento de medidas de seguridad.

También regula la ley la manera en que se crearan, modificaran o eliminaran los archivos de datos de carácter personal de los organismos públicos y por los particulares, sanciona las infracciones con multa que va de las 50 a las 10 000 unidades de salario y en su caso, con la suspensión o cancelación de la operación del archivo cuando afecte a un grupo importante de interesados.

- INTERVENCION DE CORREO ELECTRÓNICO:

Este delito, que atenta contra la privacidad como derecho fundamental de las personas, se equipara desde mi punto de vista con el de violación de correspondencia que sanciona tanto en el Código Penal Federal, (ARTICULO. 173) como en el local del D.F. (artículo 333) al que abra o intercepte una comunicación escrita que no esté dirigida a él. Sin embargo, en estricto sentido esto aplica parala correspondencia postal solamente, por lo que en la Iniciativa de reformas y adiciones sobre diversas disposiciones del Código PENAL PARA EL Distrito Federal en mataría del fuero común y para toda la Republica en materia del fuero federal del 22 de marzo del 2000, se proponía una redacción que incluyera el acceso de las comunicaciones a través de medios electrónicos, electromagnéticos u ópticos. (V. Batíz- Álvarez, 2011).

Además, el artículo 167 fracción VI del Código Penal Federal sanciona con 1 a 5 años de prisión y 100 a 1000 días de multa al que dolosamente o con fines de lucro, interrumpa o interfiera con las comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos. En esta fracción podría encuadrar entonces la acción de intercepción correos electrónicos antes de que lleguen a su destinatario, pero no el leer la correspondencia electrónica de otra persona. (V. Batíz- Álvarez, 2011).

- OBTENCIÓN DE INFORMACION QUE PASA POR EL MEDIO (SNIFFER):

Este tipo de conductas, que se refiere a interpretar datos que las personas envían a través de la red (cuando hacen una compra por internet, por ejemplo, enviando datos personales y de crédito) se tipifican en el artículo 137 fracción VI Código Penal Federal a que hice referencia en el inciso anterior.

3.1.2. Protección de Datos

El estudio de la protección de datos no es nuevo. Se ha venido a desarrollar con mayor intensidad con el surgimiento de la informática por el gran volumen de información que pueden almacenar las computadoras, lo que puede crear un perfil personal que puede dañar nuestra imagen, como personal, así como de una organización, para perjudicarnos en las actividades habituales.

Se ha dado por llamar poder informático a la capacidad de un ente de influir sobre las organizaciones a través del uso de las computadoras y precisamente la protección de datos va encaminada a limitar este poder informático. (Murillo, 2010)

Es con base a esta idea que (Murillo, 2010) comparo se han elaborado ciertos principios básicos los cuales consideran los mínimos para legislación sobre el particular a saber:

A. PRINCIPIO DE LA JUSTIFICACÍON SOCIAL: La recolección de la información debe tener una finalidad y uso específico dentro de la sociedad. Es a lo que se refiere francesa en su artículo 1 que dice: la informática deberá estar al servicio de cada ciudadano. Su desarrollo deberá tener un lugar dentro del marco de cooperación internacional. No deberá intentar a la dignidad humana ni la vida privada ni las libertades individuales o públicas.

Resulta clara la disposición, sin embargo, consideramos que presenta tautologías si consideramos que la dignidad humana y la vida privada son precisamente libertades individuales y publicas a la vez.

B. PRINCIPIO DE LIMITACION DE LA RECOLECCIÓN: Se trata precisamente de la información respecto de la cual, de tenerse especial cuidado, es decir, la llamada información sensible que normalmente es la que se refiere a raza, religión, salud, costumbres, opiniones políticas. Con base en este principio debe prohibirse el manejo de esta información, salvo casos autorizados.

C. PRINCIPIO DE LA CALIDAD O FIDELIDAD DE LA INFORMACIÓN: S e refiere a la veracidad de los datos recolectados a efecto de que no produzca una imagen distinta de una persona, de donde se deriva otro principio que es el dirigido a la posibilidad de rectificar, actualizar o anular determinada información.

D. PRINCIPIO DE LA ESPECIFICACIÓN DEL PROPÓSITO O LA FINALIDAD: Este principio obliga al recolector de información a una doble obligación: por un lado, debe indicar al interesado cuál es el fin de la recolección y por otro, efectivamente usar los datos para tal fin, sancionándose el hecho de darles otro destino.

E. PRINCIPIO DE LA CONFIDENCIALIDAD: Este quizás es el principio más importante; podría decirse que se trata de la columna vertebral de la recolección de información personal, claro está aunado a los demás principios, pero es precisamente el que protege al individuo de posibles violaciones a su vida privada, salvo que el propio sujeto consienta la invasión a su intimidad, cuando exista orden de autoridad competente y cuando se trate de información indeterminada con fines estadísticos.

F. PRINCIPIO DE SALVAGUARDAR DE SEGURIDAD: Este principio se refiere al deber de seguridad sobre la información que se maneja por parte de los responsables de los ficheros que contienen datos, protegiéndolos de la perdidas, destrucciones o acceso no autorizado, o bien en circunstancias especiales destruir información (casos de guerra).

G. PRINCIPIO DE LA POLÍTICA DE APERTURA: Representa un deber hacer transparentes los procedimientos relativos al tratamiento de la información, con el fin de que dar a conocer a los ciudadanos la existencia, los fines, usos y métodos de operación de los ficheros automáticos.

H. PRINCIPIO DE LA LIMITACION EN EL TIEMPO: La información personal almacenada en archivos informáticos debe estar sujeta a determinada temporalidad, es decir, será conservada mientras se cumple la finalidad para la que fue solicitada; una vez cumplida tal finalidad debe ser borrada, salvo algunas excepciones.

I. PRINCIPIO DE CONTROL: Se refiere al establecimiento de un organismo con facultades de hacer valer los principios mencionados. Consideramos que este tipo de control debe ser realizado por todas las dependencias y unidades de la administración pública y con el fin de que efectivamente se lleve a cabo, deberá crearse la institución y con el fin de que efectivamente se lleve a cabo, deberá crearse la institución del HABEAS DATA. Nos referimos a esto posteriormente cuando traemos el tema relativo a los instrumentos jurídicos para la protección de la información. (Murillo, 2010).

3.1.2.1 Protección Jurídica en México de la información personal.

Los datos personales forman parte de la propia personalidad que caracteriza a todo individuo, empresa u organización. El nombre, apellidos, edad, domicilio, estado civil, religión, las propiedades, son parte de nuestra imagen como personas. Tienen tal importancia que en ocasiones sentimos necesitarlos para adaptarlos para al grupo social. (Amercianos, 2014).

Sin embargo, no es oculto que en nuestro país actualmente tales datos personales ya se encuentran en innumerable registros informatizados; como ejemplos podríamos citar desde la tienda de pizzas, pasando por el centro comercial, la farmacia, el laboratorio de análisis clínicos, los hospitales, hasta llegar a la tarjeta de crédito, el registro federal electoral, el registro de vehículos, el registro público de la propiedad, el registro federal de contribuyentes y que decir del registro nacional de población.

En síntesis, el proyecto de ley:

- Establece las bases para regular los archivos, bases, bancos de datos de personas físicas.
- Determinada las obligaciones de los titulares de los bancos, los derechos de los interesados para acceder a la información que les corresponde, el derecho de pedir la inclusión, modificación, bloqueo, suspensión o cancelación de datos.
- Reconoce la importancia de la regulación de un derecho fundamental como lo es el derecho a la intimidad personal. (Goddard, 2010).

3.1.3. Sanciones a los Delitos.

Dentro del primer proceso encontramos las siguientes disposiciones aplicables tanto del derecho mercantil como del derecho común (civil) que tratan de regular la relación entre particulares (gobernados) tales como son:

Códigos de Comercio

Art, 30 BIS. -La secretaria certificará los medios de identificación que utilicen las personas autorizadas para firmar electrónicamente la información relacionada en el registro público de comercio, así como de los demás usuarios del mismo y ejercerá el control de estos medios a fin de salvaguardar la confidencialidad de la información que se remitirá por esta vía.

Art. 80.- Los convenios y contratos mercantiles que se celebren por correspondencia telégrafo o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedaran perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que esta fuere modificada.

Art. 89.- en los actos de comercio podrán emplearse los medios electrónicos, ópticos, o de cualquier otra tecnología para efectos del presente código, a la información generada enviada, recibida o comunicada a través de dichos medios se le denominara mensaje de datos.

Ley de la Institución de Crédito.

Art. 52.- Las instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público, mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procedimiento de datos y redes de telecomunicaciones, ya sean privados o públicos, estableciendo en los contratos respectivos las bases para determinar lo siguiente:

- Las operaciones y servicios cuya prestación se pacte;
- Los medios de identificación del usuario y las responsabilidades correspondientes a su uso y;
- Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que trate.

El uso de los medios de identificación que se establezca conforme a los previsto por este artículo, en sustitución de la firma autógrafa, producirá los mismos efectos que las a leyes otorgan a los documentos correspondientes y, en consecuencia, tendrá el mismo valor probatorio.

Ley Federal de Protección al Consumidor.

Art. 1 Frac. VIII, Son principios básicos en las relaciones de consumo, la efectiva protección al consumidor en las transacciones efectuadas, a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados.

Art 25.- La Procuraduría tiene las siguientes atribuciones:

IX, BIS. - Promover en coordinación con la secretaria la formulación difusión y sus de códigos de ética por parte de proveedores, que incorporen los principios de esta ley de las transacciones que celebren con consumidores a través del uso de los medios electrónicos, ópticos, o de cualquier otra tecnología.

Código penal.

Art. 1803. – El consentimiento puede ser expreso o táctico, para ello se estará a lo siguiente: Frac. I; será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología o por signos inequívocos.

Art. 1811.- Párrafo segundo. Tratándose de la propuesta y aceptación hecha a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulaciones previas entre los contratantes para que produzca efectos. (Leal J. C., 2010).

Disposición que impulsan el desarrollo del proceso informático a través de la protección de derechos de propiedad intelectual y los derechos de autor de los sistemas informáticos.

Como parte de este proceso de seguridad en la propiedad intelectual de los sistemas encontramos tanto en la Ley de Propiedad Industrial, como en la Ley Federal DEL Derecho de Autor, disposiciones que garantizan jurídicamente el desarrollo del Sistema Informático:

Ley de la Propiedad Industrial.

Art. 178 BIS. - Los esquemas de trazado de circuitos integrados serán registrados y estarán protegidos en términos del presente título, al efecto, el instituto tendrá las facultades siguientes: (Murillo, 2010)

Art. 178 BIS 1. – Para los efectos de este título, se considerará como:

- Circuito integrado: un producto, en sus formas finales o en una forma intermedia, en el que los elementos, de los cuales uno por lo menos sea un elemento activo, y alguna o tas las interconexiones, formen parte integrante del cuerpo o dela superficie de una pieza de material semiconductor, y que este destinado a realizar una función electrónica.
- Art. 178 BIS 2.-Sera registrable el esquema de trazado original, incorporado o no a un circuito integrado que no haya sido comercialmente explotado en cualquier parte del mundo. También será registrable aun cuando haya sido comercialmente explotado de manera ordinaria, en México o en el extranjero,

siempre que la solicitud de registro se presente ante el instituto, dentro de los dos años siguientes a la fecha en que el solicitante lo explote comercialmente en forma ordinaria por primera vez en cualquier parte del mundo. (Murillo, 2010).

Ley Federal del Derecho del Autor.

Art. 101.- Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Art. 102. – Los programas de computación se protege en los mismos términos que las obras literarias, dicha protección se extiende tano a los programas operativos como a los programas aplicativos ya sea en forma de código fuente o de código objeto, se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Art. 103. - Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponde a este.

Como excepción a lo previsto por artículo 33 de la presente ley, el plazo de la cesión de derecho en materia de programas de computación no está sujeto a limitación alguna.

Art. 104. -Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre programa de computación o sobre una base de datos conservara, aun después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares, este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en si mismo un objeto esencial de la licencia de uso.

Art. 105. – El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

- Sea indispensable para la utilización del programa, o,
- Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando esta no pueda utilizarse por daño o perdida. La copia de respaldo deberá ser destruida cese el derecho del usuario para utilizar el programa de computación.

Art. 106. – El derecho patrimonial sobre un programa de computación comprende la facultad de autorización o prohibir:

- La reproducción permanente o provisional del programa en todo o en parte por cualquier medio y forma;
- La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa;
- Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler;
- La des compilación, los procesos para revertir la ingeniería de un programa de computación y el desembalaje.

Art. 107. – Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituya creaciones intelectuales, quedaran protegidas como compilaciones, dicha protección no se extenderá a los datos y materiales en si mismo.

Art. 110. – El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorización o prohibir:

- Su reproducción permanente o temporal, total o parcial, por cualquier medio y, de cualquier forma;
- La traducción, adaptación, reordenación y cualquier otra modificación;
- La distribución del original de las bases de datos;

- La comunicación al público y;
- La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Art. 111. – Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta ley en los elementos primigenios que contengan. (dr)ij.

Art. 112. – Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la presentación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnéticos y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior. (Leal J. c., 2013).

Art. 113. – Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta ley. (Leal J. c., 2013).

Art, 114. – Las transmisiones de obras protegidas por esta ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberá adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia. (Leal J. c., 2013).

Código Penal Federal.

Art. 426. – se impondrá prisión de 6 meses a 4 años, y de 300 a 1000 mil días de multa, en los casos siguientes:

- A quien fabrique, importe venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal y;
- A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal. (Leal J. c., 2013).

En cuanto a este proceso de seguridad observamos el como del Estado encuadro del desarrollo de los sistemas informáticos, en figuras jurídicas ya existentes tanto en materia de propiedad industrial como de derecho de autor, tales como el secreto industrial, patentes etc., en cuanto a la primera legislación y en cuanto a la ley materia de derechos de autor, el legislador de la protección de obras literarias a los programas de cómputo y sus manuales, pariendo así a particularidades al desarrollo del sistema informático, y como garante de la consecución de sus sistemas, certeza en el desarrollo informático el código Penal los delitos especiales aplicables en la materia, que intentan terminar con el plagio y el mal uso de sistemas para efectuar información tanto de los particulares. (Union., 1917).

3.1.4. Disposiciones que regulan el acceso a la información.

La consolidación de los sistemas Informáticos como fuente de acceso a la información gubernamental en su ámbito, como ente registral solamente o como su actuar en el desarrollo gubernamental.

- Seguridad jurídica frente a las TIC.

La garantía dada a individuos de que su persona, sus bienes y sus derechos no serán objeto de ataques violentos o que, si estos llegan a producirse, le serán aseguradas por la sociedad para su protección y reparación.

El diccionario Jurídico de México define la seguridad jurídica como la certeza que tiene el individuo de que su situación jurídica no será modificada más que por procedimientos regulares establecidos previamente. (Union., 1917).

- Derecho de la Informática

La seguridad frente al impacto tecnológico considera que el derecho de abrir su campo de aplicación frente al impacto tecnológico, y concebir al derecho de la informática, como una disciplina autónoma, que es nuestra posición, entendiéndolo como el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aprovechamiento y aplicación de las nuevas tecnologías de la información y de la comunicación en cualquier área, y relaciona los efectos jurídicos que de ella se desprende de su aplicación. (Union., 1917).

(Sueñe Llinás, 1986), define al Derecho de la Informática, como el conjunto de normas reguladoras del objeto informático o de problemas directamente relacionados con la misma.

- Delitos Informáticos.

Como derivación de las diversas áreas de estudio que impone el Derecho de la Informática, ubicamos los delitos informáticos y por ello debemos entender la conducta típica y atípica, antijuridica, punible e inpunible, en la que se ven insertos los conocimientos especializados del sujeto activo en tecnologías de la información y la comunicación y cuya condición sine qua non existe la utilización de un medio tecnológico y vulnera derechos inherentes a la persona.

En algunas sociedades altamente desarrolladas, denominan estas conductas como delitos cibernéticos. (Gaytán, 2009).

Seguridad de las TIC y jurídica frente a las TIC.

El bien inmaterial que no se agota y se genera día a día es la información, valor imprescindible la cultura en una sociedad moderna.

Un conjunto de datos organizados y estructurados genera información y representa el elemento fundamental para la toma de decisiones en forma eficaz y eficiente, su característica maleable al caso concreto le da el valor de relevancia para el fin, que se utilice, su grado de importancia impone han atractivo para aquellos que identifican su potencial inserto.

Este concepto general frente al Derecho una sustantiva atención ya que la salvaguarda de la información se constituye en uno de los derechos fundamentales del hombre, y frente al impacto tecnológico, se ha conformado en una institución jurídica denominada la intimidad, que se desprende del concepto de privacidad, depositando en aquellos datos personales de un individuo que lo define como identificado o identificable. Este derecho no deja ajeno a una persona oral, a un gobierno o un país, es justamente el mayor atractivo para aquellos que conocen las bondades del desarrollo.

3.1.4.1 Código de Comercio.

Art- 30 BIS. – La Secretaria podrá autorizar el acceso a la base daros del registro público del Comercio a personas que así lo soliciten y cumplan con los requisitos para ello, el Reglamento Respectivo y los Lineamientos que emita la secretaria sin que dicha autorización implique en ningún caso inscribir o modificar los asientos registrales. (Union., 1917).

La Secretaría certificara los medios de identificación que utilicen las personas autorizadas para firmar electrónicamente la información relacionada en el registro público de comercio, así como de los demás usuarios del mismo y ejercerá el control de estos medios a fin de salvaguardar la confidencialidad de la información que se remita por esta vía.

En este sentido la legislación federal establece ya las bases para el control de los actos de comercio a través de bases de datos electrónicos, sin embargo, este desarrollo homogéneo de los sistemas registrales de las diversas entidades federativas, que permita lograr un sistema de registro a nivel nacional para fácil acceso a la información en la materia. (Rio, 2012).

3.1.4.2 Del acceso a la información pública gubernamental.

Con los avances en el desarrollo Informático, el público en general puede acceder a la información pública gubernamental, a tal nivel que solamente lo que está protegido por las leyes no será difundido, pero no por causas de falta de capacidad en el sistema Informático; ahora como siguiente tarea del gobierno es ir al fondo de la protección de lo que no debe ser difundido o existen reservas para ello, como son los datos personales, información que pone en peligro la seguridad nacional, los procesos judiciales, etc. Y de lo que aún no se ha difundido y que se debe hacer. (Rio, 2012).

Para lo anterior, el 11 de junio del 2002 fue publicada la Ley de Transparencia y Acceso a la Información Pública Gubernamental, y a partir de esa fecha se han publicado 13 disposiciones más que regulan ese sistema de información.

Esa ley tiene como finalidad, proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.

Asimismo, se creó el Instituto Federal de Acceso a la Información pública con el objeto de difundir el ejercicio del derecho de acceso a la información, resolver sobre la negatividad a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades.

Gracias al desarrollo del sistema Informático, las dependencias y entidades exigen el flujo de información a través de medios electrónicos y vía satelital, tanto entre ellas como a particulares e inclusive los particulares también la aprovechan de cierta manera y más allá, se instrumenta gracias a este sistema político de protección y preservación y preservación ambiental para mejorar la calidad de vida de las personas, como medidas anticipadas para evitar el deterioro ambiental, jugando el sistema informático un papel muy importante en la educación ambiental, existiendo programas gubernamentales con indicadores concretos en materia de medio ambiente; dentro de las planeación ambiental el sistema informático es uno de sus principales recursos para el logro de sus objetivos; el Reglamento de la Ley General del Equilibrio Ecológico y de la Protección al Ambiente en materia de ordenamiento ecológico, ese sistema tiene como finalidad registrar, organizar, actualizar y difundir la información disponible en materia ambiental y de recursos naturales. (Union., 1917).

3.1.5 Cuadro de conclusión.

Delito	Características	Ejemplo
Delito contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.	Acceso ilícito a sistemas informáticos. Interpretación ilícita de datos informáticos. Interferencia en el funcionamiento de un sistema informático. Abusos a dispositivos que faciliten la comisión de delitos.	Robo de identidad. La conexión a redes no autorizadas. Utilización de spyware y de kelogger.
Delitos Informáticos	Falsificación informática mediante la introducción, borrado o supresión de datos informáticos. Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.	Borrado fraudulento de datos. La corrupción de ficheros.
Delitos relacionados con el contenido.	Producción, oferta, difusión, adquisición de contenido ilícito, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.	Contenido de Pornografía infantil, etc.
Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.	Copia y distribución de programas informáticos.	piratería informática.
Sabotajes informáticos.	Delito de daños mediante la destrucción o alteración de datos.	Programas o documentos electrónicos contenidos en redes o sistemas informáticos.
Fraudes informáticos.	Manipulación de datos o programas para la obtención de un lucro ilícito.	Delitos de estafas.

Ilustración 3 Cuadro de conclusiones del Delito.

Capítulo 4. Impacto de los delitos informáticos en el contexto empresarial.

Resumen.

En este capítulo se dará una reseña de México, sobre cómo ha sufrido ciberdelitos el cual forma parte de la Organización de los Estados Americanos(OEA), por otra parte, se menciona las empresas mexicanas que trabajan con sistemas informáticos, a su vez las empresas que han sido atacadas por malware y por último la manera en que las empresas les han dado solución a esos ataques.

Objetivos del Capítulo.

- Informar sobre la situación en la que se encuentra México por los ataques cibernéticos en las empresas.
- Listar las diferentes empresas en México que trabajan con sistemas informáticos.
- Mencionar empresas que hayan sido atacadas por malware y la solución que le dieron a dichos ataques.

4.1. Informe de México de la OEA

En esta sección se presentan información de las empresas en México.

4.1.1. México

México tiene una población de 118,419,000 de habitantes, una cobertura de internet del 38.4%, y suscriptores de banda ancha fija: 10.5%. Además, La Policía federal de México es la principal autoridad operacional en lo que respecta a iniciativas relativas a la seguridad y el delito cibernético en México, pero muchas otras instituciones gubernamentales también desempeñan un rol activo. Dentro de la Policía Federal, las divisiones científicas mantienen una unidad responsable de coordinar actividades para investigar, prevenir y procesar toda conducta considerada delicita que utiliza medios electrónicos y cibernéticos. Además de desarrollar una amplia gama de actividades relacionadas con la seguridad de la tecnología cibernéticas, la información y las comunicaciones a nivel nacional, esta unidad también utiliza técnicas de investigación especiales como el monitoreo de la

actividad pública de internet, el uso de la figura de usuario simulado y operaciones encubierta. La División Científica también es la sede del principal equipo de respuesta a incidentes de seguridad cibernética (CSRT) con responsabilidad a nivel mundial, el CERT-MX. Si bien el CERT-MX no tiene un sitio web propio, sus datos de contacto pueden encontrarse en el sitio web del Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST). (Amercianos, 2014).

Además, para que las partes interesadas más relevantes participen en la promoción de la agenda nacional de seguridad cibernética, se creó le Comité Especializado en Seguridad de la Información (CESI) con la misión de desarrollar una Estrategia Nacional de Seguridad de la Información (ENSI), que seguirá todas las acciones concretas, claramente articuladas y coordinadas para fortalecer las capacidades del Estado en materia de seguridad de la información, seguridad cibernética, delito cibernético, ciber defensa y protección de infraestructura. A través del CESI, las autoridades también desarrollaron un Protocolo de Colaboración entre el CERT-MX y las diversas dependencias del gobierno central mexicano, para abordar y responder ante los incidentes cibernéticos que podrían hacer peligrar las infraestructuras críticas del país. (Amercianos, 2014).

El personal de la División Científica recibió y continúa recibiendo capacitación brindada por el Sistema de Desarrollo Policial (SIDEPO) de México, y por muchas otras organizaciones de seguridad y policiales en países que incluyen Colombia, Estados Unidos, Holanda Y Japón. Se hace hincapié en que las actividades de formación recibidas por el personal garanticen su capacitación de acuerdo con las responsabilidades específicas que les corresponden, y que sus conocimientos y habilidades estén lo más actualizadas posible. La capacitación relativa a las investigaciones y análisis forenses digitales se centra en la cadena de custodio, la identificación y confiscación de evidencia digital, los sistemas analíticos telefónicos, los análisis forenses digitales y los análisis forenses de dispositivos celulares. Asimismo, algunos miembros del personal recibieron capacitación de organizaciones no gubernamentales tales como Centro Nacional y Centro

Internacional para Niños Desaparecidos y Explotados (NCMEC e ICMEC, respectivamente). (Amenazas., 2014)

Para garantizar la continuidad de las operaciones y la garantía de los datos a nivel institución, se hace un respaldo de la información y se aplican técnicas de recuperación de datos en dispositivos individuales según las necesidades. Además, todas las instituciones gubernamentales principalmente deben cumplir con los requisitos de la norma ISO 207001 relativos al sistema de gestión de seguridad de la información.

Las autoridades mexicanas han desarrollado relaciones de colaboración activas con otros gobiernos y organizaciones internacionales, trabajando con entidades policiales nacionales y con CSIRT, y a través de organizaciones internacionales como FIRTS y la Organización de Estados Americanos (OEA/CICTE).

Los esfuerzos del gobierno por generar conciencia sobre seguridad cibernética incluyeron la organización de varias conferencias para instituciones gubernamentales y educativas (de nivel primario a universitario), y tareas de divulgación entre ciudadanos y otras entidades públicas y privadas.

Las autoridades gubernamentales mencionaron un gran número de impedimentos para reducir el delito cibernético y aumentar la seguridad cibernética en México. Uno de ellos es la constante falta de legislación que permita a las entidades policiales actuar en forma inmediata para enfrentar las amenazas a la seguridad y los delitos cibernéticos. Las capacidades limitadas de las entidades policiales para actuar en muchas instancias debilitan las investigaciones, perpetua la sensación de impunidad entre los grupos criminales organizados les permite implementar las últimas tecnologías y técnicas para cometer delitos, el otro gran impedimento es la constante falta de conciencia entre la población general sobre seguridad cibernética, incluidos riesgos y practicas recomendadas. (Amercianos, 2014).

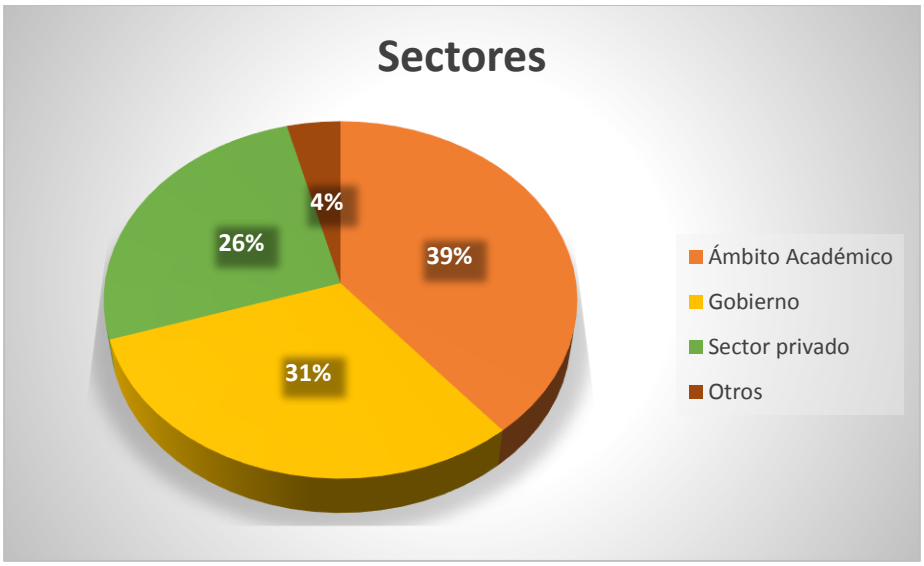


Ilustración 4Entidades Afectadas por los delitos Informáticos.

De los incidentes denunciados ante la Policía Federal Mexicana, y sin incluir incidentes que involucraron ciudadanos y particulares, aproximadamente 31% fueron contra instituciones gubernamentales, 26% contra entidades del sector privado, 39% contra organizaciones académicas y 4% contra otras entidades. Los incidentes del sector lógico no autorizado aumentaron aproximadamente 260%, las infecciones de malware aumentaron 323% y los incidentes de phising aumentaron (México, 2014).

También se observaron aumento considerable de los incidentes relativos a amenazas persistentes avanzadas (APT) contra medianas empresas y el uso de código malicioso a fin de Hackear información de usuarios para luego intentar extorsionarlos. Este último tipo de incidentes también provoco un aumento en el uso de malware que utiliza encriptaciones de seguridad complejas para atacar a los servidores de pequeñas y medianas empresas (PyME), lo que tiene un impacto cada vez mayor en el sector productivo. (México, 2014)

Los incidentes de seguridad cibernética más denunciados incluyeron el uso de malware, phising, hackeos y vandalismo y las intrusiones en sistemas. Los

incidentes de fraudes y extorsión más denunciados incluyeron los fraudes de comercio electrónico, las estafas nigerianas, los fraudes de banca electrónica y la extorsión. Además, las denuncias de quejas particulares incluyeron la difamación, as amenazas, el robo de contraseñas, la suplantación de identidad y el acoso.

En cada estado de la República Mexicana enjuicia a las personas en forma independiente por los delitos cometidos, no existen cifras disponibles respecto del total de enjuiciamientos por delitos cibernéticos a nivel nacional. (México, 2014).

4.1.2. Empresas Mexicanas que utilicen Sistemas Informáticos.

Estas son algunas empresas que utilizan sistemas informáticos en México.

Ilustración 5 Empresas Mexicanas que trabajan con Sistemas.

- Ganaderos Productores de Leche Pura (Alpura).
- CEMEX México.
- Galvak.
- Multipack.
- Cementos Apasco (Grupo Apasco).
- Controladora Comercial Mexicana (Comercial Mexicana).
- Vitro Corporativo.
- GRUMA (Grupo Maseca).

- Pfizer.
- Hylsamex.
- Promoción y Operación (PROSA).
- Cuprum.
- Acciones y Valores de México (ACCIVAL).
- Novartis Farmacéutica.
- Supremo Tribunal de Justicia del Estado de Chihuahua.
- Ekco.
- Quálitas, Compañía de Seguros.
- Janssen-Cilag de México.
- Finanzas Monterrey.
- Grupo Diagnostico Proa (Proa).
- Productos Kraft.
- General Motors de México.
- The American British Cowdray Medical Cnter IAP (Centro Medico ABC).
- Instituto Sonorense de Infraestructura Educativa (ISIE).
- Grupo Casa Saba (Casa Saba).
- Municipio de Naucalpan (Ayuntamiento de Naucalpan).
- Tecnológico de Monterrey, Campus Estado de México.
- TUM Transportistas Unidos Mexicanos Div. Nte.
- Brisol-Myers-Squibb.
- Federal Express Holding México (FedEx)
- Unilever de México.
- Tequila herradura (Casa herradura).
- Merck Sharp & Dohme de México.
- Mexicana de Aviación.
- Comercializadora Palacio de Hierro.
- Levi Strauss de México.
- Eli Lilly de México.
- Malta Texo.
- Celanese mexicana.

- Deportes Martí.
- Productos Internacionales Mabe.
- Electronica y Medicina.
- Grupo Copamex.
- Holding Protel.
- Alphabet de México.
- Tyco Electrónicos México.
- GCC Cementos.
- Dirección de pensiones de estado de Jalisco.
- Grupo Sedi.
- Grupo Pavisa.

4.1.3. Empresas Mexicanas atacadas por Malware.

Ciberataque golpea a empresas de México.

Empresas mexicanas de los sectores bancarios y telecomunicaciones si resulto afectadas por el ciberataque mundial perpetrado con un virus Rasomware llamado WannnaCry.

La plataforma Malware Tech y Karspersky Lab señalaron que México fue unos de los 100 países afectados por la falla divulgada en documentos pirateados de la Agencia DE Seguridad Nacional (NSA).

Ante el ciberataque, la Comisión Nacional de Seguridad (CNS) explico que México aplica el protocolo de gestión de incidentes para prevenir afectaciones a sus instituciones ante el ciberataque que ha afectado principalmente a compañías estatales y hospitales en otras partes del mundo.

Ante estos hechos, el Centro de Especializaciones en Respuesta Tecnológica (CERT) de la División Científica de la Policía Federal trabaja coordina mente con otros países a nivel internacional.

El virus, conocido como Ransomware, es un software malicioso que cifra y secuestra los archivos de las computadoras para exigir un pago de liberación de

esa información, la infección se da por algún error del usuario al acceder a sitios que contienen códigos maliciosos.

El modo de propagación de Rasomware es a través de vínculos falsos de bancos u organizaciones policiales, o pueden ser transmitidito por vía de redes de archivos de uso compartido para conseguir claves de acceso para descargar programas. El monto que solicitan es de 300 bitcoins, esta es una moneda virtual y su tipo de cambio al día de hoy es de 1.6 dólares por bitcoin.

De acuerdo con la firma de seguridad computacional Avast Software, más de 57 mil compañías, instituciones y organizaciones e todo el mundo han sido afectadas por el ataque.

Entre los países afectados se encuentran Reino Unido, Estados Unidos, Rusia, Italia, Vietnam, China y España. (NTMX, 2017).

4.1.4. Ejemplo de ataques y solución.

Al menos 500 usuarios corporativos en México fueron afectados, según Kaspersky; sin embargo, la policía cibernética mexicana indicó que no se había detectado ataques.

Ciudad de México (Expansión) – El ataque cibernético, que afecto este viernes a al menos 99 países del mundo, también dejo cientos de víctimas de México, de acuerdo con el director de Investigación y Análisis en América Latina de Kaspersky Lab, Dmitry Bestuzhev.

Por las menos 500 organizaciones en el país fueron afectadas por el programa informático maligno conocido como ransomware, dijo en entrevistas el ejecutivo de la compañía y advirtió que el número podría aumentar si no se toman las medidas pertinen33tes.

Aunque no es uno de los principales afectados, México es una de las víctimas, aunque muchas empresas deciden ocultar esta información por proteger lo que ellos llaman su prestigio, afirmo Bestuzhev.

Los comentarios del especialista difieren de los del Centro Especializado en Respuesta Tecnología de la Policía Federal, quien indico, en un comunicado, que “por el momento en México no se han detectado ataques de este virus”.

El ataque cibernético ¿Qué es y cómo Prevenirlo?

El embate funciona a través de un programa WannaCry y su principal objetivo es bloquear los archivos de un ordenador infectado para que, posteriormente, los hackers soliciten un rescate por la recuperación de los archivos, según Kaspersky, la firma que dio a conocer las afectaciones.

Los atacantes exigen a la victimas realizar el pago solo a través de la moneda virtual Bitcoin.

Los hackers para la recolección de los pagos, registros 18 transacciones, que redituaron en 3.42 Bitcoins, equivalentes a 6,003 dólares o alrededor de 114,357 pesos, al tipo de cambio de este día.

Para Dmitry, es complicado conocer el origen de este ataque debido a la dificultad de trabajar conjuntamente en las redes internacionales de internet.

Es difícil conocer al actor de estos ataques pues para lograrlo primero se debe identificar plenamente la dirección IP que los origino y después, están las complicaciones de una posible colaboración internacional que no es sencilla.

Sin embargo, no se pudo prever que surgirá otro brote a nivel internacional, el cual, ha afectado a 98 países entre ellos México, el problema de este tipo de software, insiste Bestuzhev, es que se apodera fácilmente de los permisos de un computador al grado de que puede llegar a ser “Dios” y dejar completamente vulnerable al sistema operativo ante la más mínima amenaza.

El Centro Criptológico Nacional de España dijo, más temprano, que el ataque afectada a sistemas Windows cifrados todos sus archivos y los de las unidades de

red a las que estén conectadas, e infectado al resto de sistema Windows que haya en esa misma red.

Por lo que, para el investigador de Kaspersky Lab, la amenaza no está cerca de llegar a su fin, pues esto depende de que Microsoft desarrolle los parches completamente funcionales para Windows el principal sistema operativo afectado -y que- además, las personas los instalen y pongan en funcionamiento.

Al principio no se tomó muy en serio al ransomware, pero este ataque demuestra que no estemos preparados y lo más preocupante es que afecto a organizaciones indispensables como instituciones de Salud en Reino Unido, por ejemplo, añadió Dmitry. Hasta ahora, el ataque ha dejado un total de 75,000 ciberataques a nivel mundial y se extiende rápidamente.

Capítulo 5. Tipos de ciberdelitos.

Resumen.

En este capítulo se dará a conocer la tipología sobre los ciberdelitos informáticos, donde se define cada uno de los diferentes tipos de ataque, a su vez se menciona paso a paso la manera en que es su ataque y la posible solución que se le puede dar a cada uno de ellos, así como su definición desu procedimiento.

Objetivos del Capítulo.

- Definir cada uno de los delitos Informáticos.
- Mencionar paso a paso la manera en que ataca cada delito Informático.
- Explicar las posibles soluciones a los ataques mencionados.

5. 1. Delitos informáticos

En esta sección se presentan los malware más importantes, así como su definición, su modo de ataque y la solución a ellos.

5.1.1. Definición del delito PoS (Puntos de venta).

Son software de gestión de ventas inteligentes y flexibles que permiten al usuario tener el máximo control sobre el movimiento de dinero en caja de manera automática, proporcionando la disminución de perdidas en punto de venta y proveyendo mayor control interno sobre las compras y ventas de las tiendas, pagos, así como también la calidad de atención que brinda a los clientes. Todo de manera rápida y sencilla. (Virtual., 2013)

5.1.1.2. Modo de Ataque.

Violaciones de Datos en Punto de Venta (PoS), sus etapas son las siguientes:

Fuente (Symantec, 2014).

1. INFILTRACIÓN

   El atacante logra ingresar a la red corporativa mediante spear-phishing, servidores vulnerables y otros métodos tradicionales.

Ilustración 6 Infiltración, fuente (Symantec,2014)

2. FUGA EN PUNTO DE VENTA.

   El ataque busca puntos de acceso a la red del punto de venta.

Ilustración 7 fuga de punto de venta, fuente (Symantec,2014)

3. HERRAMIENTA DE ROBO DE DATOS.

   El atacante instala malware e los sistemas de PoS para robar datos de las tarjetas de crédito.

Ilustración 8 herramienta de robo de datos (Symantec,2014)

4. PERSISTENCIA Y CAUTELA.

   El malware roba los datos luego de cada transacción con tarjeta de crédito y, con el tiempo, acumula una gran cantidad de datos robados.

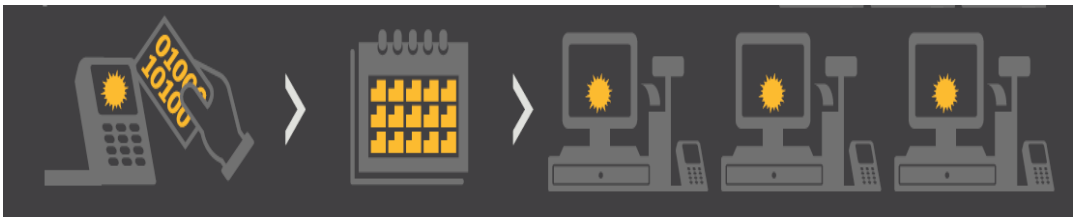


Ilustración 9 persistencia y cautela (Symantec,2014)

5. PRUEBAS.

   El atacante secuestra el sistema interno para su “servidor de pruebas”, y cumula datos de miles de sistemas PoS.

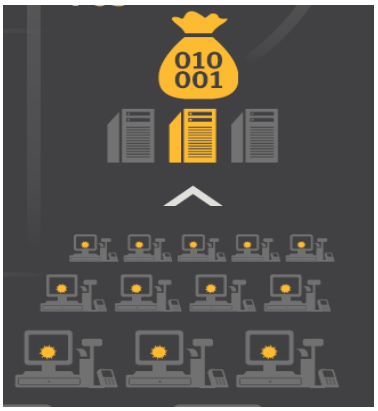


Ilustración 10 pruebas (Symantec,2014)

6. EXFILTRACIÓN.

   Se exfiltran los datos obtenidos a un servidor externo, como servidor de un tercero en la nube que ha sido comprometido.

Ilustración 11 exfiltración (Symantec,2014).

5.1.1.3. Acciones de prevención.

1. SENSIBILIZA EL USUARIO PARA LA SEGURIDAD DE LA RED.

   Entrenamiento de seguridad del usuario final es un gran beneficio para la empresa, desde que haya cambio de comportamiento y relación del usuario con la máquina. Entre los colaboradores para ayudar a eliminar errores que podría llevar una invasión, bien como ayudarlos a percibir un comportamiento extraño por maliciosos o los defraudadores.

2. ELABORE UNA POLÍTIA DE CRIPTOGRFÍA Y APLIQUE.

El robo de laptops es una de las mayores razones del número de violaciones de datos, por eso, es necesario tener una política de criptografía que debe ser impuesta para los laptops de los colaboradores.

3. IMPLANTE LA DETENCIÓN Y PREVENCIÓN DE INTRUSOS.

Detención y prevención de intrusos deben ser usados para todos los sistemas que son accesibles a través de la internet, como servidores web, sistemas de correo electrónico, servidores del Active Directory u otros sistemas que son considerados misión crítica.

4. PARE CON MOVIMIENTOS A TRAVÉS DE DOWNLOAD

Hay tantas violaciones que ocurren vía movimiento de download – sites maliciosos o comprometidos que pueden explorar una máquina simplemente al tener acceso a un sitie. Ser capaz de bloquear eso es la llave para una buena política de seguridad.

5. REALICE EVALUACIONES DE VULNERAVILIDAD REGULARES.

Muchas empresas aun solamente ejecutan scans de vulnerabilidad, una vez por trimestre. Esos deben ser hechos semanalmente. Hoy día, las organizaciones deben realizar comprobaciones de vulnerabilidad contra, todos los sistemas en su red, tanto interna como externa.

6. APLIQUE LA CORRECIÓN INTEGRAL

Cada persona que sabe acerca de la corrección integral, pero muchos aun no lo hacen de forma amplia. Muchas personas de la TI simplemente aceptan las actualizaciones de los Microsoft y creen que todo es bueno.

7. UTILICE DE UN MONITOREO DE COMPORTAMIENTO.

El empleo de un programa de monitoreo del sistema, donde la persona de RH o responsable por la conformidad puede reproducir el comportamiento de un proceso que es inestable.

8. HACER BACKUP

Muchas violaciones ocurren por la pérdida o robo de cintas de backup de datos. En servicio de backup remoto permite que la empresa use la internet para guardar información de forma segura y eficaz, sin nunca necesitar usar cinta que pueden ser pérdidas o robadas. (Cardenas., 2016).

5.1.2. Definición spear-phishing.

El spear-phishing es un correo electronico diseñado con ingenieria social con objeto de engañar a una persona o un pequeño grupo de personas y realizar un ataque dirigido. (Symantec, 2014).

Un ataque watering-hole, por su parte requiere que los atacantes infiltren u sitio web legitimo visitado por sus victimas, instalen un codigo malicioso y luego esperen que estas victimas cigan en la trampa. Los ataques dirigidos en America Latina no solo siguen crecendo sino evolucioando. (Corporation., Symantec Security Response, 28 de agosto de 2013.)

En el 2013, mas del 50% de los archivos adjutos usados en los ataques de spear-phishing a nivel mundial contenian archivos ejecutables. Estos archivos son potencialemte peligrosos ya que pueden contener malware o pequeños programas para infectar la maquina de un usuario.Tambien se utilizaron documentos con formato PDF o Microsoft Word de Forma regular. Estos documentos representaron

7.9% y 5.3% de los archivos adjuntos, respectivamente. (Corporation., Informe anual sobre amenazas., 2014).

5.1.2.1. Tipos de ataques ejecutables.

Tipo ejecutable	2013	2012
.exe	31.3%	39%
.scr	18.4%	2%
.doc	7.9%	34%
.pdf	5.3%	11%
.class	4.7%	<1%
.jpg	3.8%	<1%
.dmp	2.7%	1%
.dll	1.8%	1%
.au3	1.7%	<1%
.xls	1.2%	5%

Ilustración 12 tipos de ataques ejecutables (Symantec, 2014).

- Más del 50% de los archivos adjuntos a los correos electrónicos usados en ataques tipo spear-phishing en 2013 contenían archivos ejecutables. (Symantec, 2014)-
- Se utilizaron documentos con formato PDF o Microsoft Word de forma regular. Estos documentos representaron 7.9% y 5.3% de los archivos adjuntos respectivamente. Sin embargo, estos porcentajes han disminuido.
- Los archivos Java con extensión .class representaron 4.7% de los archivos adjuntos utilizados en ataques de tipo spear-phishing.

En total, más de 552 millones de identidades se expusieron durante 213 en todo el mundo, lo que permitió a distintos delincuentes acceder a información sobre tarjetas de crédito, fecha de nacimiento, numero de documentos de identidad domicilios particulares, historias clínicas, números de teléfono, información financiera, direcciones de correo electrónico, claves de acceso, contraseñas y otra clave de información personal. (Ibid). Para comprender la magnitud del delito, podemos señalar que las tarjetas de crédito robadas pueden venderse por un valor de hasta USD 100 en el mercado negro, lo que hace de las violaciones de datos una actividad

sencilla y de bajo riesgo para los ciberdelincuentes, pero sin duda rentable. (Corporation, Underground Economy Servers, 2010).

Si bien el spear-phishing fue alguna vez el método preferido para instalar malware, los ataques “watering-hole” lo están reemplazando poco a poco en la región, esto no significa que los ataques tipo spear-phishing estén en desuso. Si bien ha disminuido la cantidad total de correos electrónicos utilizados y victimas por campaña de spear- phishing, en 2013 hubo un aumento de 91% en la cantidad de campañas. (Amenazas., 2014). Esto indica que los cibercriminales están realizando mayores esfuerzos y diseñando estos ataques para dirigirlos a víctimas potenciales en América Latina. Las tres fuentes principales de ataques de phishing en América y el Caribe son Brasil, Colombia y Argentina. De hecho, estos tres países aportan 74% de todos los ataques de phishing en América Latina y 3.2% a nivel mundial. (Corporation., Informe anual sobre amenazas 19., April 2014).

5.1.2.2. Definición de ataques dirigidos.

Malware es un programa malicioso para robar informacion sensible o confidencial. Un ataque dirigido utiliza malware orientado a un ususario o grupo de usuarios especificodentro de una organización en especial. Este malware puede distribuirse mediante un correo electronico de tipo spear-phishing (ataques dirigidos) o una fora de infeccion a traves de sistios web conocide como ataque “watering-hole”.

Existen muchos tipos de malware,entrevirus,troyanos,gusanos. adware,keyloggers, dialers, rootkits, ransomware, rogueware, etc. (Quintero, 2011).

5.1.2.2.1. Clasificación

- Virus: auto. Réplica, infecta otros programas.
- Gusano: se replica mediante copias de si mismo, pero no infecta a otros programas.
- Troyano: no se replica ni infecta a otros programas de forma automática e indiscriminada.

- Aware: presenta publicidad no deseada.
- Keylogger: captura pulsiones en el teclado, espía lo que el usuario escribe.
- Rootkit: usa técnicas para permanecer oculto en el sistema ante el usuario y las aplicaciones de seguridad.
- Backdoor: función de puerta trasera, permite al atacante conectarse y controlar la maquina infectada.
- Dialer: realiza llamadas de tarificación especial incrementando la factura telefónica.
- Bot: los sistemas infectados son “zombies” que conforman una “botnet” o red de botd; esta red acepta órdenes de forma remota.
- Ransomware: cifra documentos y archivos, pide al usuario que pague un rescate si quiere la clave que permita acceder a los originales.
- Rogueware: falso antivirus, te hacen creer que el sistema está infectado y cobra para la supuesta desinfección.
- Crimeware: nueva denominación para el malware orientado al cibercrimen y fraude, con un claro interés de lucro. (Quintero, 2011).

5.1.2.3. Modo de Ataque.

1. INCURSIÓN.

El atacante logra el ingreso a la organización víctima. En general, se realizan actividades de reconocimiento previo que permitan encontrar la táctica de ingeniería social adecuada.

Ilustración 13 incursión (Symantec, 2014)

2. DESCUBRIMIENTO.

Una vez que el atacante ha logrado el ingreso; procurará mantenerlo y descubrir a que datos y otros recursos valiosos desea acceder.

Ilustración 14 descubrimiento (Symantec, 2014).

3. CAPTURA.

Luego de descubrir e identificar los datos valiosos, el atacante encontrará la forma de recopilación antes de intentar exfiltrarlos.

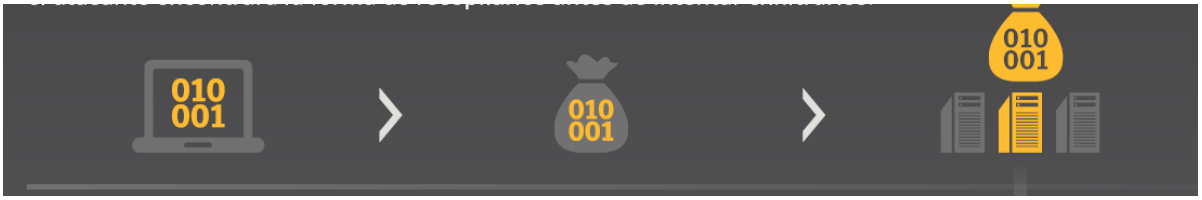


Ilustración 15 captura (Symantec, 2014).

4. EXFILTRACIÓN

El atacante encontrará un mecanismo para robar los datos de la organización víctima. Para lograr, puede subir los datos a un servidor o sitio o web remoto. Otros métodos más discretos pueden concluir la encriptación y estenografía, para hacer el proceso de exfiltración aún más difícil de detectar, como esconder datos dentro de paquetes de petición de DNS.

Ilustración 16 exfiltración (Symantec, 2014).

5.1.2.4. Acción de prevención

- Usar antivirus actualizado.
- Actualización del sistema operativo, navegador y resto de aplicaciones.
- Uso de usuario restringido vs administrador.
- Evitar abrir correos no deseados y enlaces llamativos en las redes sociales.
- Evitar abrir documentos e instalar software de fuentes no confiables. (Quintero, 2011).

5.1.2.5. Las industrias más afectadas por ataques tipo spear-phishing.

Ilustración 17 Industrias afectadas por ataques de tipo spear-phisisng. (Issue, 2014).

- La industria manufacturera fue la más afectada en 2013, y represento 30% de todos los ataques perpetrados en América Latina.
- La categoría de servicio profesionales incluye servicios contables, jurídicos, de ingeniería y de salud.
- La categoría de servicios no tradicionales incluye servicios comerciales, de entretenimiento y reparaciones.

5.1.3. Definición de Ransomware (Secuestro Informático).

Es un software malicioso que al infectar los equipos le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda información y datos almacenados. El virus lanza una ventana emergente en la que nos pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual. (Jaén, 2012).

5.1.3.1. Modo de Ataque.

Los estafadores continúan aprovechándose de ransomware; a menudo los atacantes se hacen pasar por agentes de las fuerzas de seguridad locales y así exigen el pago de una multa falsa, que suele oscilar entre USD 100 Y 500, como condición para desbloquear una computadora que estaba supuestamente bloqueada, y que había sido usada por las autoridades durante una investigación. (Corporation, Ibid. en 48, 2013)

En abril del 2014, una propagación de Ransomware llevo a la policía de México a publicar un aviso formal. (Issue, 2014).

Los ataques de Ransomware son sumamente rentables y con frecuencia se modifican para asegurar que sigan teniendo éxito. El paso siguiente de esta evolución fue el programa Ransomcrypt, conocido comúnmente como Cryptolocker. Este es el más prominente de los nuevos tipos de programas extorsivos. En lugar de hacerse pasar por un agente de la ley, el atacante solicita explícitamente una recompensa para descifrar archivos de usuarios que han sido atacados. Cryptolocker utiliza un cifrado RSA 2,048 de alto grado, que actualmente es imposible de descifrar. Salvo que un usuario haya hecho una copia de seguridad de sus datos antes del ataque de Cryptolocker, es probable que sus datos queden inaccesibles para siempre. Estas amenazas causan aún más daño a las empresas, pues también se afectan los archivos contenidos en unidades de redes compartidas o conectadas. Las investigaciones indican que, en promedio, 3% de los usuarios cuyas computadoras han sido infectadas pagan la recompensa, mientras que 97% restante pierde sus datos, o bien, debe contentarse con una copia de seguridad no actualizada. (Krebs., 2013)

Retener archivos cifrados para obtener una recompensa no es una práctica nueva, pero, en el pasado, los delincuentes tenían dificultades para lograr el pago de la recompensa. Con el surgimiento de los métodos de pago online. Ransomcrypt tiene todo lo necesario para seguir creciendo. Los que están más expuestos al riesgo de perder datos, archivos, o memorias son las pequeñas empresas y lo consumidores. La prevención y las copias de seguridad resultan cruciales para proteger a los usuarios contra este tipo de ataques. (Krebs., 2013)

Ilustración 18 Ejemplo de Ransomware dirigido a usuarios en Argentina (Krebs., 2013)

Ilustración 19 Ejemplo de Ransomware dirigido a usuarios en Argentina (Krebs., 2013)

5.1.3.2. Acción de Prevención

- Mantener todos los softwares del equipo actualizado.
- Asegurarse que las actualizaciones automáticas estén activas para poder de esta manera recibir los últimos parches de seguridad de Microsoft.
- Mantener activado el firewall.
- Usar un bloqueo de ventanas emergentes.
- Los archivos maliciosos ocultan su verdadera naturaleza. (Reducers, 2010).

5.1.4. Definición de DDoS (Denegación de servicios).

Según (ROMERO, 2016), es contra un sistema informático que da lugar a que el servicio ofrecido a los usuarios se vea seriamente comprometido. Como por ejemplo ellos tenemos los virus.

Por otro lado (Bermejo, 2007), dice que los ataques de Denegación de Servicio (DoS) tiene la finalidad de provocar que un servidor o recurso sea inaccesible para los usuarios legítimos. Un ataque de Denegación de Servicio Distribuido es un tipo especial de ataque DoS en el que se utilizan varios equipos para realizar un ataque coordinado contra una máquina. Este tipo de ataque se suelen utilizar maquinas denominadas zombies que el atacante consigue controlar gracias a algún tipo de malware, al conjunto de máquinas Zombies que controla un atacante se las suele denominar BotNets. (Bermejo, 2007)

Este tipo de ataques pueden provocar:

- Parada para todos los servicios de una máquina.
- La máquina solo puede dar determinados servicios.
- La máquina no puede dar servicio a determinados usuarios.

5.1.4.1. Modo de ataque.

Los ataques DoS se pueden llevar a cabo de diferentes formas y cubren una infinidad de servicios. Existen tres tipos básicos de ataques.

- Consumo de recursos limitados
- Destrucción o alteración e datos.
- Destrucción o alteración física de componentes de la red.

Atacantes

Algunos de los grupos que pueden llevar a cabo este tipo de ataques son:

- Script Kiddies
- Competencia
- Militares
- Empleados Incompetentes

Ejecución de los ataques DDoS

Una clasificación de los ataques de denegación de servicios atendiendo al tipo de objetivó elegido. Para cada uno de ellos se detallarían los mecanismos que pueden ser efectuados por el atacante para llevar a cabo el atacante.

Así, cuando se considera el objetivó al que va a atacar, los ataques se pueden categorizar dentro de los siguientes tipos. (Mirkovic J. D., 2004)

- Los ataques de denegación deservicio.

  Inestables cuando se les envía paquetes fragmentados con marcas de fragmentación incoherentes. Esta vulnerabilidad se puede explotar enviado dos paquetes UDP con marcas de fragmentación mal construidas a la víctima. Para este exploit existen numerosa variante, conocidas como bonk, boink, teardrop y newtear.

- Ataques de inundación pura:

  La forma más obvia de ejecutar un ataque DoS de inundación pura es enviar una gran cantidad de mensajes, divididos en paquetes, a un servicio que resida en una maquina objetivo. A menos que algún elemento de red entre la víctima y las maquinas atacantes realice el filtrado de dichos paquetes, la victima ocupara sus recursos en recibir y procesar los mensajes. Si se envían suficientes paquetes de ataque, todos los recursos de la maquina destino estarán ocupados en procesar peticiones que no poseen ningún valor.

- Ataques de vulnerabilidad:

  Como ya se ha mencionado, el ataque a una vulnerabilidad consiste en el envío de un paquete, construido de forma especial, hacia un destino, de modo que aprovecha una determinada vulnerabilidad en el recurso objetivo del ataque y consigue afectar al servicio que presenta.

5.1.4.2. Prevención de ataques DoS.

Las estrategias de prevención tratan de eliminar la posibilidad de que un ataque se efectué antes de que este se produzca. Estas aproximaciones introducen cambios en los protocolos, aplicaciones y sistemas para fortalecerlos contra los intentos de ataque. La prevención referida a los ataques DoS, tiene como objetivo aminorar el riesgo de sufrir algunos de los ataques de vulnerabilidad, dificultar el atacante la tarea de conseguir una cantidad de agente elevada y reducir las probabilidades de éxito del ataque. Sin embargo, aun jugando un papel fundamental para la seguridad, la prevención no elimina la amenaza que suponen los ataques de denegación de servicio.

En el campo de prevención de ataque DoS, se podría clasificar las posibles medidas en cuatro mecanismos. (Mirkovic J. a., 2014):

- ATAQUE DE PROTOCOLO

Esta tipología está constituida por los ataques de inundación que aprovechan la debilidad o asimétrica de un protocolo para conseguir su objetivo, evitando tener que enviar una cantidad muy elevado de mensajes para obtener ventajas, con respecto la víctima, en el consumo de recursos respecto a la liberación de los mismos. (Schuba, 1997)

- ATAQUES UN RECURSO FISICO

Se puede realizar un ataque contra un recurso físico especifico de una máquina, como por ejemplo su CPU, memoria, capacidad de conmutación de un encaminador, etc. los recursos que forman parte de la infraestructura de la red son particularmente atractivos para ser atacados, ya que estos ataques tienen impacto sobre gran parte de la población e internet. Como ejemplo, el servicio de encaminamiento es un recurso de infraestructura critico que puede ser atacado mediante DoS. (Jou, 2000).

Los ataques de denegación de servicio.

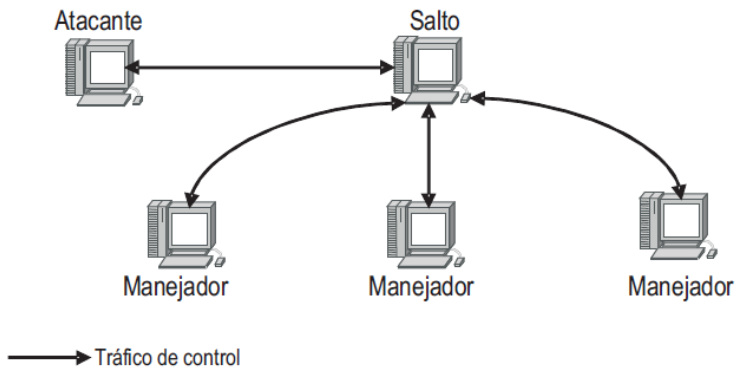


Ilustración 20 maquina actuando como asalto para un ataque DDoS. (State, 2013).

- Mecanismo de seguridad del sistema.

  Estos mecanismos tratan de incrementar la seguridad global el sistema, mediante la protección de acceso ilegítimos, eliminando fallos (bugs) en las aplicaciones actualizando las implementaciones de los protocolos para impedir intrusiones y la utilización del sistema con fines perversos, etc.

  La capacidad de los ataques de denegación proviene generalmente del gran número de máquinas comprometidas que generan flujos de ataque de forma coordinada. Si estas máquinas fueran seguras, los atacantes perderían su capacidad de reclutamiento y la amenaza que suponen los taques DDoS desaparecería. Por otro lado, los sistemas vulnerables a intrusiones pueden convertirse por sí mismo en víctima de ataques en los cuales el atacante, habiendo conseguido acceso ilimitado a la máquina, borra o altera sus contenidos. Por tanto, la implementación de mecanismos de seguridad del sistema evita la proliferación de máquina vulnerables. (Tripwire for servers., 2007).

  Siempre que se pueda encontrar una vulnerabilidad en un servidor concurrente consistente en la existencia de un patrón temporal fijo en su comportamiento que permita predecir los instantes en que se producen las salidas, se puede ejecutar un ataque DoS a baja tasa contra él.

Se han propuesto algunos ejemplos de sistemas servidores concurrentes a los que es factible atacar mediante el procedimiento aquí expuesto. Entre ellos, por su importancia actual, destaca el servidor HTTP.

La eficiencia obtenida por los ataques DoS a baja tasa contra servidores concurrentes es muy elevada.

Este tipo de ataques es muy versátil. Permite al atacante elegir entre un número elevado de configuraciones dependiendo de las restricciones que existan entre el tráfico enviar al servidor y la eficiencia a obtener en la denegación de servicio.

El atacante dispone de herramientas que le permite determinar los valores de los parámetros de ataque. Dichos mecanismos, como el modelo matemático.

El ataca dispone de mecanismos de control en la fase de ejecución del ataque, como la estrategia del umbral de capturas, que le permiten ir ejecutando de forma gradual el taque con la finalidad de eludir existencia de sistemas de seguridad en el entorno de la víctima.

Se ha realizado la implementación de este ataque en un entorno real y se ha concluido que dicha implementación no implica dificultades reseñables. (State, 2013).

5.1.5. Definición Spoofing.

Es la suplantación de la dirección o identidad de un ordenador ajeno, al atacante se hace pasar por otro obteniendo acceso que en condiciones normales tendría restringido. (Mauricio Muñoz, 2010)

- Spoofing Activo: el intruso interfiere con el tráfico legítimo que fluye a través de la red.
- Spoofing Pasivo: el intruso monitorea el tráfico de la red.

Por otro lado (CONASSOL, 2005). En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Se pueden clasificar los ataques de spoofing, en función de la tecnología utilizada. Entre ellos tenemos el IP spoofing, (quizá el más conocido), ARP spoofing, DNS spoofing, WEB spoofing o email spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantación de identidad.

5.1.5.1.1.1 Definición de IP Spoofing.

La clave para este ataque es usurpar la dirección IP de una máquina. Esto permite al cracker ocultar el origen de su ataque (usando un ataque de Denegación de Servicio) o para beneficiarse de una relación de confianza entre dos máquinas. (CONASSOL, 2005).

5.1.5.1. Modo de ataque.

El principio básico de este ataque consiste, para el cracker, en crear sus propios paquetes IP (con programas con hping2 o némesis) en los cuales cambiaremos, entre otras cosas, la dirección IP de origen. IP Spoofing es llamado frecuentemente Blind Spoofing. Las respuestas a los falsos paquetes no pueden ir a la máquina del cracker, y ya que el origen ha sido alterado, van hacia la maquina burlada. Sin embargo, hay dos tipos de métodos para hacer que las respuestas regresen:

- Soucer Routing: el protocolo IP tiene una opción llamado Source Routing (ruteo de origen) que permite definir la ruta que los paquetes IP deben tomar. Esta ruta es una serie de rutas de dirección IP que los paquetes deben seguir. Suficiente para que el cracker provea una ruta para los paquetes hacia un router que controle. Actualmente la mayor parte de las pilas TCP/IP rechazaron que usen esta opción.
- Re-routing: tablas de enrutamiento usando el protocolo RIP, pueden ser cambiadas enviándoles paquetes RIP con nueva información de enrutamiento. Se hace esto para enrutar los paquetes hacia un router que controle el cracker.

Estas técnicas son muy usadas: el ataque es llevado a cabo sin saber que paquetes son los que vienen del servidor objetivo.

Blind Spoofing se usa contra servicios como rlogin o rdh. Su mecanismo de autentificación solo recae en la dirección IP de origen de la maquina cliente. Este relativamente bien conocido ataque requiere varios pasos:

- Encontrar la dirección IP que está utilizando la máquina de confianza, que indica donde se exporta el sistema de archivos.
- Dejar al host de confianza fuera de servicio usando un SYN Flooding, esto es primordial para evitar que la maquina responda a los paquetes enviados por el servidor/ victima.
- Predicción de los números TCP, todo paquete TCP está asociado a un numero de secuencia inicial. La pila TCP/IP del sistema operativo lo genera de forma lineal, dependiendo del tiempo, aleatorio o seudo- aleatorio, según el sistema. El cracker puede atacar al sistema generando números de secuencia predecibles (generados linealmente independientes del tiempo).
- El atacante consiste en abrir una conexión TCO en el puerto deseado. (Detousen., 2005).

5.1.6. Genbeta

La sensación deja ver con el antivirus de Microsoft se intensifica. Entre mayo y junio escrito casi la misma noticia tres veces; los investigadores de Google Project Zero han descubierto un fallo critico en Windows Defender, por suerte la empresa ya lo ha corregido.

Se trata nuevamente de un fallo en el motor de protección antimalware de Microsoft, la parte nuclear de Windows Defender. La vulnerabilidad que según explica el experto en seguridad (Tavis Ormandy), es sumamente fácil de explotar, permite a un atacante ejecutar código en un ordenador, obtener privilegios elevados y tomar control PC de la víctima.

Lo único que un atacante requerido para infectar a la víctima es hacer que esta entre a un sitio web malicioso, abra un email, lea un mensaje de chat, o descargue un archivo.

No se necesita más interacción por parte del usuario, pues el motor de protección antimalware de Windows Defender escanea automáticamente y de forma inmediata el contenido nuevo que llegue al ordenador, y una vez hecho esto, el ente malicioso tiene el control de tu PC.

El motor de protección antimalware.

A principios de mayo se reportaban el primer exploit critico en Windows Defender. Casi la misma historia: a un atacante le bastaría con enviar un email o mensaje instantáneo infectado que sea escaneado por Windows Defender para usarlo como vector e infectar al usuario.

A finales de mayo, otra vulnerabilidad en el emulador x86 que incluye el otro de protección antimalware. A la hora de que Windows Defender escanease un ejecutable sospechoso y lo procesara, un atacante podría aprovecharse de esto creando un archivo especial y ejecutando de forma remota.

El problema: el motor de protección antimalware es un servicio integrado en el sistema operativo, el hecho d que Microsoft no aislé en su propio contenedor a este servicio, hace vulnerable a Windows a exploits de este tipo.

Si usas el antivirus de Microsoft, asegúrate de tener activas las actualizaciones automáticas y no tendrás que preocuparte por estar cubierto contra este fallo. De no ser así actualiza de inmediato (Kaspersky, 2017).

Capítulo 6. Guía operativa para la protección de datos informáticos.

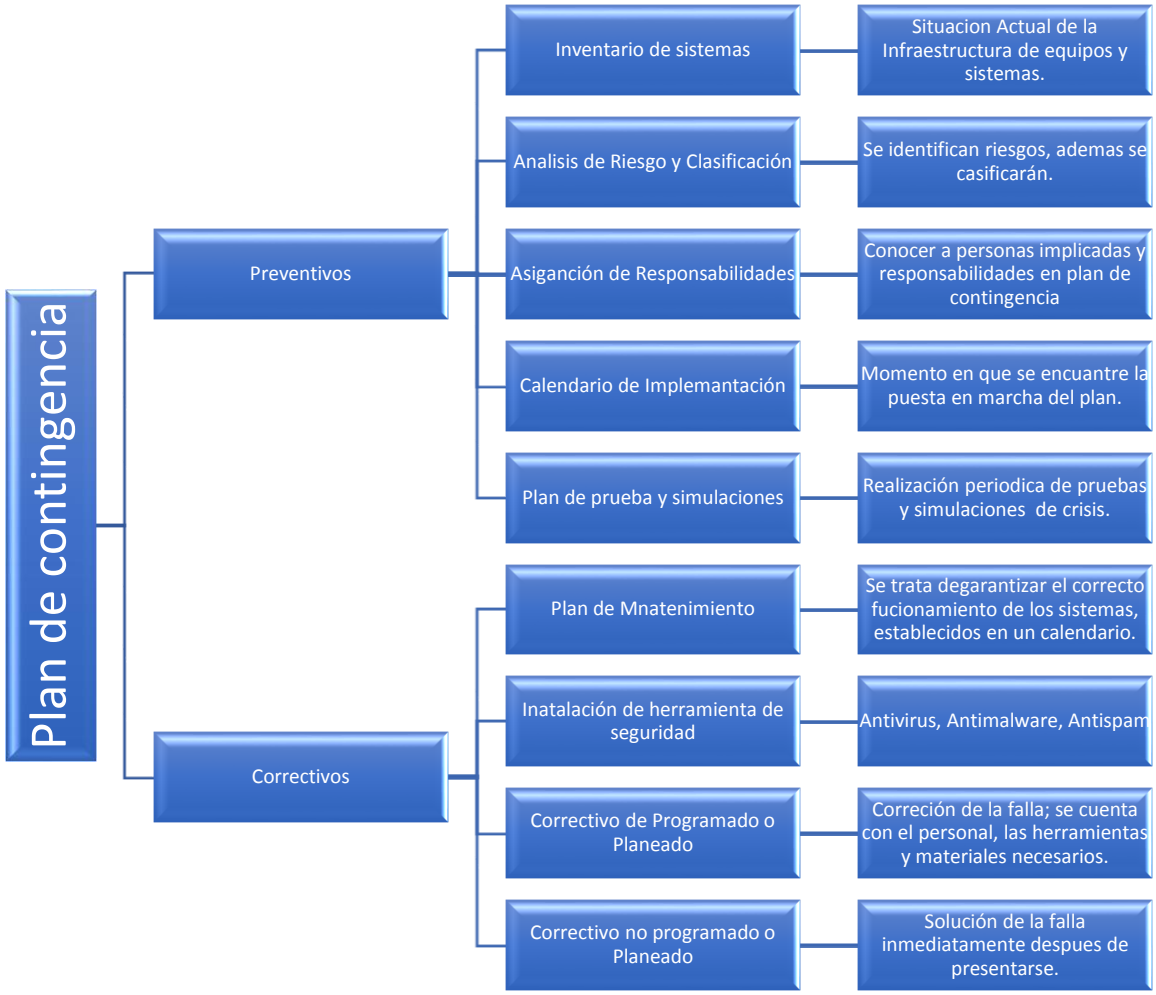
Resumen.

Esta guía esta propuesta para la protección lógica de la información tomando en cuenta sus propiedades de confidencialidad, integridad y disponibilidad en computadoras de punto final. No se completa la seguridad física del equipo de cómputo, robo físico del mismo, destrucción y desastres naturales. Es únicamente preventiva, detectiva y correctiva, los controles son planteados tomando en cuenta la evaluación de riesgos desde los puntos de vista: riesgo de la información en la organización desde la aplicación de punto final.

Objetivo del Capítulo.

Proponer recomendaciones básicas de seguridad, que ayuda a proteger la información del ordenador conectando al internet de forma rápida y atacando a las principales vulnerabilidades que embisten la seguridad, así mismo se irán haciendo proposiciones con mayor profundidad, para cada uno de los principales riesgos.

6.1 Plan de Contingencia.



6.2 Recomendaciones básicas de seguridad.

Menciona (Alvares Marañon Gonzalo, 2004) diez puntos básicos para la protección de una computadora de punto final.

I. Uso de programas de protección o “antivirus” y su actualización.

Asegúrese de que tiene por lo menos un programa Antivirus en su computadora, dos es lo más recomendable. El Antivirus está diseñado para proteger la computadora contra virus conocidos, así que no hay de que preocuparse. Pero ya que nuevos virus emergen diariamente, los programas antivirus requieren de actualizaciones periódicas continuas. De igual manera, se requiere que se actualice

cada año la versión del antivirus, ya que puede cambiar de forma importante la maquinaria de búsqueda (por ejemplo, algunos utilizan técnicas heurísticas que necesitan actualizar de forma en que realizan sus búsquedas). Por lo tanto, asegúrese de actualizar su antivirus regularmente.

II. No abrir correo electrónico de fuentes desconocidas.

Una regla muy simple de seguridad es que, si no se conoce a una persona que está enviando un correo electrónico, hay que tener cuidado al abrirlo, lo mismo, para cualquier archivo adjunto a él, si recibe un correo sospechoso, se recomienda borrar el mensaje completo, incluyendo los archivos adjuntos. Incluso si se conoce a la persona que lo está enviando, se debe ejercitar la precaución y actuar con desconfianza, y más aún si tiene ligas a lugares raros o no usuales de los que maneja con esa persona o entidad.

III. Use contraseñas difíciles de adivinar.

La contraseña mantiene lejos a los intrusos, solo si son difíciles de adivinar, no comparta su contraseña, y no use la misma clave en más de un lugar, si alguien descifra su contraseña, no es deseable que tenga posibilidades de usarla en otros lugares, por ejemplo, en su cuenta bancaria. Las reglas de oro en la selección de contraseñas son: una contraseña debe tener mínimo ocho caracteres, y sea tan incomprensible como sea posible, utilizando mayúsculas, minúsculas, y caracteres especiales entre otros. Es necesario cambiar las contraseñas regularmente, al menos cada 90 días, no le confié su contraseña nadie.

IV. Proteger la computadora de intrusos de internet, usando firewalls personales.

Equipe la computadora con un firewall persona. Estos crean un muro de protección entre su computadora y el método exterior. Vienen de dos formas, cortafuego, tipo software que corren en su computadora personal y los de tipo hardware que protegen un numero de más de dos computadoras al mismo tiempo. Trabajan filtrando datos peligrosos y no autorizados que provienen de la internet, mientras que permiten el tráfico confiable que llega a sus computadoras. Se pueden

encontrar firewall o cortafuegos en la red, ya sean de uso gratuito como el ZoneAlarm y el Tiny Firewall que vienen como tutoriales sencillos, que emergen después de una instalación simple, otros buenos y comerciales son los que produces Symantec y Network Associates, por ejemplo: Norton Personal Firewall. El seguir esta guía segura, ayuda a no permitir a los intrusos que entren en su computadora.

V. No comparta el acceso a su computadora con extraños, aprenda acerca del riego de compartir recursos.

el sistema operativo de su computadora puede consentir que computadoras en una red, incluyendo la Internet acceda a su disco duro con el fin de compartir recursos. Esta opción puede permitir a los intrusos infectar su equipo con troyanos a ver sus archivos. Por tanto, a menos que sea realmente necesario que comparta archivos, deshabilite esta opción. Vea los archivos de ayuda, del modo en que su sistema operativo comparte archivos y no permita que los extraños entren en su computadora.

VI. Desconéctense de Internet cuando no lo esté utilizando.

Recuerde que el camino digital tiene una comunicación en los dos lados. Usted envía y recibe información por medio de él. Desconéctese de internet si no la está utilizando, no de oportunidad que alguien se cuelgue a su máquina. Si no tiene antivirus, ni Firewall, alguien puede infectar su computadora y entrar en ella.

VII. Respalde los datos e información de su computadora.

Expertos en computación sabe que hay dos tipos de gente: aquellos que han perdido información y los que van sufrirla. Respalde pequeñas cantidades de información importante que usted en memoria USB y CD. La mayoría de la gente debe hacer respaldo semanal de su información importante. Además, asegurarse de tener discos de rescate a la mano de su sistema por si ocurre algún evento.

VIII. Baje regularmente actualizaciones de seguridad, o parches de seguridad.

La mayoría de las empresas proporcionan actualizaciones de sus programas regularmente. Algunas veces, se detectan errores de programación que pueden afectar la seguridad de su computadora y permitir que intrusos la penetren. Cuando son descubiertos, las compañías y los distribuidores los pone al alcance en sus sitios Web. Se debe estar seguro de que se tienen las últimas actualizaciones e instalarlas. Cheque regularmente dichas actualizaciones o permitir que el actualizador automático lo haga, ya que muchas compañías lo incluyen como una opción más.

IX. Cheque su seguridad en una base de seguridad o regular o probada y normalizada. Esto puede ser por periodos de tiempos regulares y reevalúe la seguridad de su computadora periódicamente.

Los programas y sistemas operativos incluyen varias utilerías que facilitan el trabajo, pero lo pueden dejar vulnerable a intrusos y virus. Se debe evaluar la seguridad en la computadora al menos dos veces al año. Los exploradores de Internet vienen en su menú de preferencias con un apartado de seguridad, póngalo el que se adecue a sus necesidades de preferencia ponga uno arriba de lo que requiere como mínimo.

X. Asegúrese que sus usuarios finales sepan que hacer si su computadora resulta afectada o ya ha sido violada en su integridad.

Asegúrese que todo aquel que use el equipo tenga una formación de seguridad informática y sepa que hacer si está infectado, que sepa actualizar sus antivirus, bajar parches y como crear una contraseña difícil de adivinar.

6.3 Guía para minimizar los riesgos en las computadoras.

Esta guía se desarrolla partiendo desde la instalación y configuración adecuada del sistema operativo, hasta evaluación del software de seguridad para sugerir al lector las herramientas necesarias que le convienen, en base a sus necesidades de usuario.

- Configuración segura de la instalación del sistema operativo Windows.

El inicio de todo surge desde la instalación del sistema operativo, por lo que a continuación se presenta algunas recomendaciones para proteger el sistema operativo, antes de instalar algún otro tipo de aplicaciones. Esto depende del sistema operativo instalado. Las versiones de Windows actualmente se trabajan en la empresa de estudio es Windows con tecnología XP. En las versiones de Microsoft Windows se recomienda aplicar las siguientes recomendaciones y actualizaciones. (Pérez, 2010).

6.3.1 Habilitar la opción para poder ver las extensiones verdaderas de los archivos.

Recordemos la forma en que por lo general el código malicioso intenta ocultar su extensión, invitando al usuario ejecutar archivos que pueden comprender la integridad de la información.

Ejemplo.

Los *.VBS son ejecutables de Visual Basic Script, pero pueden modificar su extensión por .TXT .VBS, y la extensión .VBS quedará oculta por lo general, por lo tanto, aparentará ser un archivo de texto: TXT, donde se pueden aprovechar de la inocencia del usuario. para que esto no ocurra, recomendamos DESMARCAR dicha opción, a efectos de no caer en estas trampas, y poder ver siempre la verdadera extensión de un archivo. Para ello, proceda así:

En Windows NT/XP:

Seleccione Mi PC,

Menú Ver,

Opciones (u Opciones de carpeta). (Hernández, 2007).

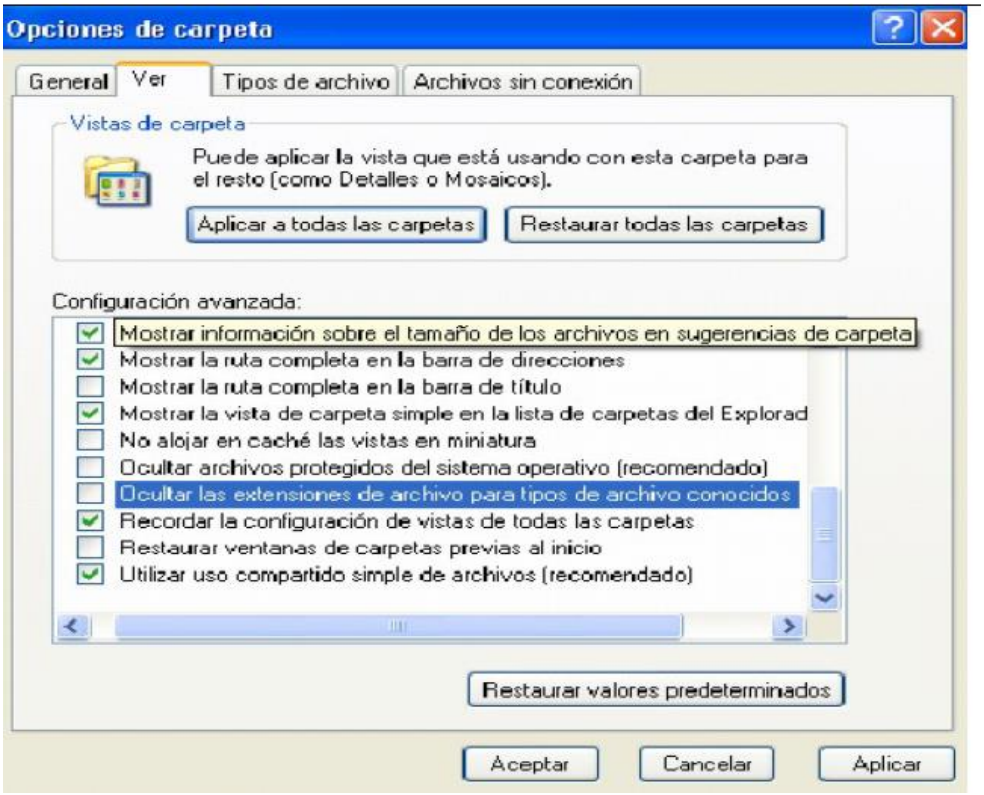


Ilustración 21 Configuración para visualizar archivos en Windows XP.

Deshabilitar servicios innecesarios (Sistema Windows XP). Se debe tener conciencia en gran parte de los riesgos, surgen por tener servicios de red innecesariamente abiertos, por lo tanto, se recomienda cerrar los puertos que o sean utilizados de acuerdo a sus necesidades:

- Los sistemas Windows NT/XP instalan aplicaciones con servicios de red por lo que es necesario identificarlos y dar de baja los servicios no utilizados de acuerdo a las necesidades.

Para dar de manejo los servicios innecesarios abiertos, se debe acceder al Menú Herramientas administrativas, en la opción de servicios, y cuando se abra la ventana correspondiente, dar de baja los servicios que utilizan los puestos identificados poniéndole “stop”, y posteriormente con click derecho modificar su estado de activación, seleccionado “manual”, o bien, “desactivado”. Se recomienda tener cuidado al dar de baja los servicios que no son necesarios, pues algunos de ellos son requeridos por el sistema y el dejarlos inactivos causará algunos problemas. (Pérez, 2010).

6.4. Planeación de la instalación del Sistema Operativo.

Es importante hacer una planeación del sistema operativo para estar preparado en casos de emergencias para ello se debe considerar el uso al que va hacer destinado.

En forma predeterminada, las computadoras personales de marca vienen con el sistema Windows pre- instalado, y proveen un disco de rescate y restauración. El disco de restauración contiene una imagen del sistema operativo preinstalado y reconfigurado con los controladores de hardware de la computadora, por lo que es conveniente conservarlo en buen estado para lo que se requiera. (Pérez, 2010).

Es muy conveniente y recomendado el tener dos o más discos duros por lo siguiente:

- Se puede respaldar fácilmente la información.
- En caso de algún desastre, que el sistema operativo no quiera iniciar correctamente, algún virus haya cambiado a configuración del sistema, un intruso haya hecho averías, o alguna otra circunstancia, la información contenida en el disco duro puede ser rescatada con mayor facilidad y copiada a alguna otra partición. (Pérez, 2010).

6.4.1. Aplicar parches de seguridad.

Posteriormente se recomienda bajar los parches de seguridad para Microsoft Windows en el sitio http://update.microsoft.com, donde se tiene una aplicación de actualización por ActiveX, que suele tardar un poco, dependiendo de la conexión, o bien visitando el sitio www.microsoft.com y poniendo en la cajita de texto “Windows update”, o en un sitio de seguridad y tecnología http://technet.microsoft.com, en la sección de “Service Parcks”, buscar los de la versión del sistema operativo Windows correspondientes, bajarlos y aplicarlos.

Es importante bajar también los parches de seguridad que se encuentren disponibles y aplicarlos, en especial los llamados “hotfixes”, que son quienes

proveen de parches de seguridad contra riesgos que son muy explotados y de gran impacto, generalmente los más recientes en la época. (Sanchez, 2014).

6.5. Configuración segura de la instalación de Microsoft Office.

A continuación, se presenta una propuesta de instalación segura de Microsoft Office, dado que, de acuerdo al análisis de riesgo, estas aplicaciones presentan los mayores riesgos de incidentes por infección de virus. Se ha desarrollado una propuesta para instalación de Microsoft Office.

La aplicación de Microsoft Word proporciona un abundante campo de desarrollo para los programadores de virus, quienes principalmente explotan deficiencias de seguridad en los lenguajes Visual Basic que acompañan a esta suite, específicamente en los lenguajes para macros y componentes dinámicos de MS Office.

De ahí que exista la clasificación de Virus de Macro, dado que estos utilizan el lenguaje mencionado con código malicioso. Para establecer controles preventivos en contra de posibles infecciones d virus de marco, así como otro tipo de virus que vienen del cliente de correo electrónico o del navegador Web aprovechando vulnerabilidades en los componentes Microsoft Office, nos basamos en la idea de que, estos tipos de virus al no encontrar el lenguaje de macros Visual Basic en el entorno del sistema, no tendrán oportunidad de sufrir efecto su código malicioso. (Pérez, 2010).

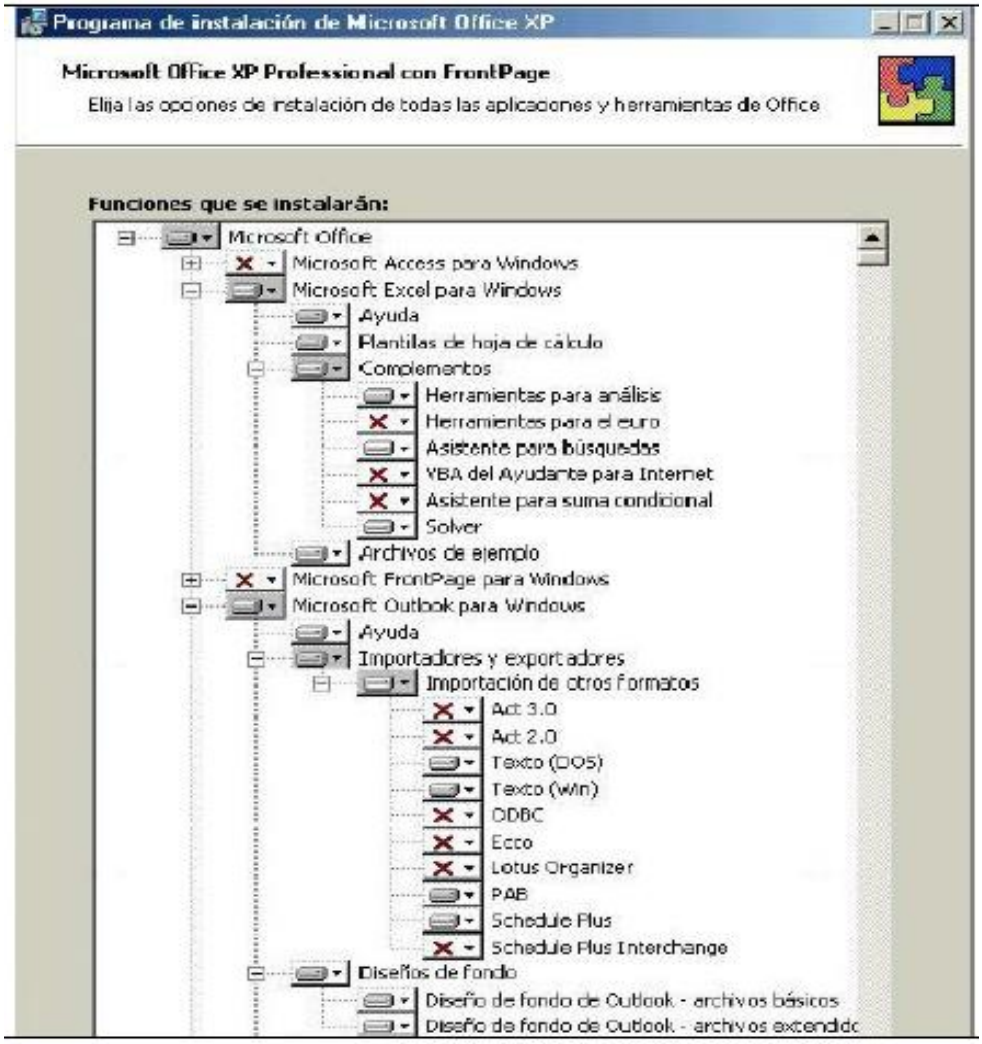


Ilustración 22 Configuración segura de la instalación de MS Office.

6.6. Políticas de seguridad para minimizar riesgos de usuario en Internet.

Navegue seguro siguiendo las siguientes medidas de protección:

Si se navega sin ningún tipo de protección, puede usted llegar a ser atacados por virus, que observé lo que hacemos en tercero, o dejar puertos abiertos para un virus, que observé lo que hacemos un tercero, o dejar puertos abiertos para que conozcan todo lo que contengamos en nuestros ordenadores. Por tanto:

- Utilice una configuración de conexiones seguras entre su navegador y el servidor al cual se conecta.
- Haga caso a los cambios de modalidad y asuma los riesgos más necesarios de acuerdo a sus necesidades (conexiones seguras, a las que no son) para así saber en cuales se está intercambiando información cofrada entre su ordenador y el servidor.
- Configure los niveles de seguridad que bien predeterminados en su ordenador de acuerdo al nivel de seguridad que desee.
- Activar y hacer uso de las advertencias en los distintos navegadores para saber si en un proceso pasa algo fuera de lo recomendable (entrar a una zona desprotegida, conectar con un sitio inseguro).
- Desactive archivos de comando en los navegadores.
- Organice las páginas Web en zonas de seguridad en su navegador, (zona local de Intranet y l zona de Internet).
- Borre el historial de Internet en los distintos navegadores.
- Utilice un servidor intermedio entre cada enlace con servidores (se recomienda anonymizer) para que no puedan recabar información que está dada sin protección). (Kaspersky, 2017).

6.6.1 Las Cookies.

Permitir o no que las cookies se almacenen en el equipo. Una cookie es un elemento de información de tamaño reducido enviado por el servidor para que el navegador lo guarde de manera que se pueda recuperar su valor en cualquier momento. Podemos elegir no almacenar las cookies en nuestro equipo ganado ciertamente en seguridad y privacidad, pero no necesarias en gran cantidad de páginas, tendremos que ver la posibilidad de activarlas solo cuando nos interese resulta práctica. Según versión del navegador, podremos desactivar desde la misma ventana “configuración de seguridad” a la que hemos accedido, recordemos, personalizar nivel, desde el botón. (Hernández, 2007).

En la versión 7, sera desde la pestaña” privacidad” desde donde podreos bloquear la descarga de cookies, impedir que los sitios web lean el contenido de las cookies

almacenadas, seleccionar sitios de confianza y algunas configuraciones más, siendo la principal el asignar un nivel de aceptación de nuestras cookies acorde a nuestras necesidades, lo que haremos subiendo o bajando el botón de la izquierda al nivel conveniente. Existen, los cuales van desde la admisión libre de todas las cookies, al bloqueo total de las mismas.

Ilustración 23 Privacidad (Hernández, 2007).

Descargas.

Mantendremos la opción de descarga de archivos activada. Al pedirnos autorización para ello, siempre elegiremos guardar el archivo en disco, y esto es de vital importancia, nunca autorizaremos a abrir el archivo al terminar la descargar. Una vez en el disco, haremos el chequeo del archivo descargado con nuestro antivirus. (Pérez, 2010).

Parches de Microsoft.

Al ser el navegador más popular sus numerosos fallos de seguridad son ampliamente explotados. Dichos fallos pueden causar que ciertos recursos maliciosos, como exploits en páginas que visitemos o mensajes de correos infectados ejerzan sus acciones sobre nuestro sistema. Los efectos de dichas acciones maliciosas pueden variar, desde bloqueos del sistema, a que este pueda ser controlado por la entidad ajena, pasado por revelar información almacenada en nuestro equipo entre otros. Por ello es de suma importancia mantener el navegador correctamente actualizado, actualizamos el navegador, podemos vernos afectados por alguno de esos recursos maliciosos creados a expensas de las debilidades comentadas. (Pérez, 2010).

Para aplicar los parches que solucionan dichas vulnerabilidades, así como otras conocidas: Sección Vulnerabilidades de I.E.

Es importante instalar la última actualización acumulativa disponible, o Servicie Pack (según configuración), para evitar que reaparezcan antiguas vulnerabilidades al instalar parches anteriores.

6.7. Configuración segura de Outlook.

El Outlook de Microsoft, es el cliente de correo electrónico más usado, por lo tanto, es necesario saber configurarlo para que sea un cliente de correo seguro. En un principio, se pueden mejorar las condiciones de seguridad de Outlook sustancialmente, para lo cual se recomienda seguir los siguientes pasos:

Deshabilitar el panel de vista previa. Esta medida es de gran importancia, algunos virus pueden activar su código malicioso con esta pre-visualización (no olvidemos que, si abrimos el mensaje, aunque no lo hayamos pre-visualizado, el código se activara). Para desactivar la vista previa nos dirigimos al comando “Ver”, “Diseño”: en el apartado “Panel de vista” se desmarca la casilla correspondiente.

Seleccionar Zona de Seguridad Abrimos Outlook, en el menú “Herramientas”, “Opciones”, “Seguridad”, seleccionamos en zonas de seguridad la opción: zona de

sitios restringidos (más segura)". Aplicamos los cambios y cerramos. Si estamos utilizando la versión 7 de Outlook Express, en esta misma ventana encontramos la opción de evitar el acceso a los archivos adjuntos de correo. Desde esta ventana, es posible establecer la configuración para el correo cifrado de Microsoft, pero se necesita previamente un identificador digital

No olvidemos que hay que tener el navegador configurado correctamente para aumentar la efectividad de esas configuraciones de seguridad.

Existen varios métodos para controlar los mensajes de correo no deseados y de noticias que puede ver en Outlook Express. Esto puede impedir que determinadas personas le envié correo, también ocultar las conversaciones que no le interesen y configurar los niveles de seguridad para proteger frente al envió de código perjudicial en el correo. (Hernández, 2007).

6.7.1 Políticas de seguridad para minimizar riesgos por código malicioso.

Las siguientes son políticas de seguridad que ayudan a reducir los riesgos, por lo que es recomendado que sean consideradas para áreas de computo, áreas dentro de organizaciones, así como para usuarios que manejes el Internet. Las políticas que se mencionan son en general, por lo que se puede ir escogiendo algunas de ellas de acuerdo a las necesidades de usuarios.

El código dañino o código malicioso ha sido una amenaza para la seguridad de las computadoras personales desde hace ya un buen tiempo debido al impacto negativo que ha tenido para los usuarios de computadoras debido al impacto negativo que ha tenido para los usuarios de computadoras personales, representado también como herramientas de trabajo. Por lo tanto, es necesario tener una serie de buenas prácticas en el tratamiento de la información que entra, sale y reside en las computadoras de punto final

A continuación, se listan algunas políticas para minimizar riesgos por código malicioso: virus, troyanos, y lo referente a lo visto en capítulos anteriores, en la

sección “de riesgos de código malicioso”, de lo cual se puede tomar los que sean necesarios de acuerdo a las necesidades de la organización.

- Utilizar un buen antivirus y actualizarlo. Un antivirus es un programa informático especifico diseñado para detectar y eliminar virus. Sin embargo, cada di aparecen nuevos virus que los antivirus no son capaces de reconocer. Para la detección y eliminación de estos virus es necesario actualizar frecuentemente nuestros antivirus. Por lo tanto, la efectividad de un programa antivirus reside, en gran medida, en la capacidad de actualización, preferentemente diariamente.
- Asegúrese que el antivirus este activo. Un antivirus está activo cuando dispone de una protección permanente capaz de vigilar constantemente todas las operaciones realizadas en el ordenador. La manera de comprobar que esta protección esta activa es a través de un icono fijo en la barra de atareas, junto a la información horaria, o en la propia configuración del programa antivirus. Estar protegido contra los virus requiere una protección permanente, tanto de archivo como de correo electrónico.
- La mejor manera para detectar un troyano es revisar los archivos recibidos por Internet con antivirus o con cualquier otro programa específico para troyanos (anti troyanos). Se podrían también configurar los distintos administradores de descarga de archivos para que apliquen un antivirus a todos los archivos que se bajen de Internet por medio del propio gestor.
- Es recomendable también tener un antivirus y/o anti troyanos monitoreando continuamente el sistema. Además, los anti troyanos suelen tener características de sistema. Además, los anti troyanos, suelen tener características de firewall personales, por lo que son capaces de detectar también posibles intentos de conexión por parte de un cliente troyano a nuestras computadoras personales vía Internet o la comunicación de un servidor de troyano instalado ya en nuestra computadora personal con su respectivo cliente en caso de estar ya infectado por él.
- Utilizar algún programa firewall personal, considerando que la mayoría del firewall nos protegen contra troyanos, a pesar de que casi ningún firewall

protege contra virus. Para obtener mayor información acerca de firewall personales se puede consultar lo siguiente:

- Evitar el uso de un mismo disquete o cualquier medio de almacenamiento externo en varias computadoras, porque se puede infectar los archivos almacenados en este medio, y en algún caso también infectar los archivos de todas las demás computadoras en cuestión.
- En caso de ser necesario el uso de un mismo dispositivo de almacenamiento en varios equipos, es recomendable revisar con un antivirus antes de introducirlo en una nueva computadora revisar con un antivirus antes de introducirlo en una nueva computadora para asegurase de no tener algún archivo infectado. Analizar los disquete y memorias, es una buena norma mediante un buen antivirus. Al utilizarlos en otros ordenadores es aconsejable protegerlos contra escritura, bajando la pestaña de la parte inferior derecha del disquete, en su parte trasera.
- Retirar los disquetes de la unidad floppy al arrancar o pagar la PC. A pesar de que Internet es uno d los medios de propagación de virus más habituales, los disquete y memorias siguen siendo una vía de infección, la maquina será de gran magnitud, al iniciar con un disquete infectado con virus de boot, la maquina será víctima de este tipo de virus al no presentar protección al momento de iniciar la máquina. Por si se olvida hacerlo, es conveniente contar con un antivirus capaz de comprobar en tales circunstancias la existencia de disquete infectados (características para evaluar un antivirus).
- Analizar el contenido de los archivos comprimidos. Los archivos comprimidos son muy útiles por contener en su interior múltiples archivos y ocupar espacio, sin embargo, son un medio ideal para almacenar virus en estado latente. Por lo tanto, una característica para evaluar un antivirus estado latente. Por tanto, una característica para evaluar un antivirus es que este dicte el mayor número de formatos comprimidos posibles. Antes de abrir directamente uno de estos archivos, como los de formato ZIP, es aconsejable guardarlos en carpetas temporales creadas por usuarios y cuyo archivo puedan ser posteriormente borrados en lugar de abrirlos sobre directorios de

trabajo, por ejemplo, la carpeta Windows, Mis Documentos, el Escritorio, o su directorio de almacenamiento preferido.

- No instalar Software de dudosa procedencia, ya que no se sabe cuál será el efecto en su computadora al instalarlo. (Freeware y Shareware).
- Cuando navegue en el internet no visitar páginas pornográficas o de dudosa procedencia, ya que este tipo de contienen diversos tipos de códigos maliciosos (virus, espías, y otro tipo mencionados en el análisis de riesgos), considerado que algunos virus se pueden alojar en Applets de Java, animaciones de Flash, JavaScript, código ActiveX y VisualBasic Scripts, y estos sitios generalmente lo hacen utilizando vulnerabilidades en el navegador, y mediante el uso de ventanas emergentes (pop-up´s).
- No abrir correo o abrir o descargar archivos de remitentes desconocidos, ya que el correo electrónico es medio de transmisión preferido por los virus y más explotados, por lo que hay que tener especial cuidado en su uso. Cualquier correo recibido puede contener virus, aunque no le acompañe el símbolo de datos adjuntos. Además, no es necesario ejecutar el archivo adjunto de un mensaje de correo para ser infectado; en algunos sistemas basta únicamente con abrir el mensaje, o visualizarlo mediante la “vista previa”, especialmente con los clientes de correo Microsoft Outlook. Para prevenir esto, lo mejor es verificar los mensajes inesperados o que provengan de una fuente poco habitual.

Un indicativo de posible virus es la existencia en el asunto del mensaje de palabras en un idioma al utilizado normalmente por el remitente. Se recomienda también el uso de interface WebMail en lugar de clientes de correo electrónico para revisar los mensajes de mail si es que se tiene disponible. Nunca abrir archivos adjuntos de correo electrónico con extensiones ejecutables .exe, .pif, .shs, .com, .scr, .bat, .doc (no es ejecutable pero es posible portador de virus) o con doble extensión : “protect_your_credit.htmal.pif” sin antes escanearlos con un antivirus actualizado, ya que son archivos ejecutables o generados por aplicaciones, teniendo algún virus escondido, pudiendo hacer cambios en el sistema sin darse cuenta.

En caso de requerir abrir alguno de los archivos mencionados, es mejor tener a la mano algún antivirus para revisar los archivos adjuntos, ya que puede ser sorprendido por algún virus o caballo de Troya.

No descargar archivos de páginas que no tengan un certificado de seguridad, porque muchas páginas de Internet permiten la descarga de programas y archivos a las computadoras de los internautas. Cabe la posibilidad de que estos archivos estén infectados con virus. Como no existen indicadores claros que garanticen su fiabilidad debemos evitar la descarga de programas desde sitios Web que no nos ofrezcan garantías. Por lo general, son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen, también los avalados por organizaciones tales como editoriales, organismos oficiales.

Rechazar archivos no solicitados, ya que gracias a Internet es posible intercambiar información y conversar en tiempo real sobre temas muy diversos mediante los grupos de noticias y los chats respectivamente. Los grupos de noticias (news), como no son listas de correo, usan su propio sistema de transmisión por Internet (NNTP), también necesitan de una protección eficaz y constante. Ambos sistemas, además de permitir la comunicación con otras personas, también facilitan la transferencia de archivos. Aquí es donde hay que tener especial cuidado y aceptar solo lo que llegue de un remitente conocido y de confianza.

Si es posible y no ha sido estandarizado el uso de Micrisoft Outlook en la organización. ¡evítelo!, ya que, por su gran popularidad, es un software de escasa seguridad y por lo tanto es vulnerable a todo tipo de virus. Use un programa como Eudora, Netscape Componer, o Mozilla Mail. No le protege totalmente, pero le hace un poco menos vulnerable. Muchos de los virus actuales no sufren efecto en estos clientes de correo electrónico.

No recibir software de personas que han sido conocidas por Internet, el movimiento es que a la persona del otro lado de la pantalla no la conocemos y por lo tanto no sabemos cuáles puedan ser sus intenciones.

Las empresas antivirus proveen de lista de coreo para él envió de boletines de seguridad, por lo que se recomienda suscribirse a algunos, por ejemplo, Panda Antivirus tiene su sistema de lista de coreo Oxygen, donde se envía información de los virus que vengan apareciendo contantemente. Se recomienda también suscribirse a la lista, " The CERT Advisory Mailing List" enviado un correo electrónico a la dirección de correo majordomo@cert.org con el subject "suscribe", y seguir las instrucciones recibidas, con esto estará al tanto de las vulnerabilidades de diferentes aplicaciones en varios sistemas operativos.

No permitir que otros se contaminen. Si el programa de antivirus detecta que alguien le ha enviado un archivo infectad, o si recibe un mensaje extraño de una persona conocida y está seguro de que el no hizo el mensaje por lógica social, favor de avisarle de inmediato a quien se lo envió, que tiene un problema de virus, de esta manera evita la proliferación y propagación de estas plagas.

Cambiar la configuración de arranque de la computadora de punto final. Cambie la configuración de la secuencia de inicio, para que el equipo siempre intente iniciar el sistema desde el disco duro. De esta manera se evitará la acción de cualquier virus de boot en disquete que se pueda haber quedado olvidado en la unidad floopy. Cuando deba bootear desde un disquete, tan solo deberá cambiar nuevamente la configuración de la secuencia de booteo. Los usuarios finales normalmente no requieren indicar desde disquete, por lo que el cambiar la configuración de boot será para fines de mantenimiento.

Comprobar que el antivirus incluya soporte técnico, ya que el servicio de soporte técnico, bien a través de correo electrónico o por teléfono, es de gran ayuda ante problema o duda que pueda surgir relacionado con virus o con el funcionamiento del antivirus. En el supuesto de verse afectado por algún virus de reciente creación, se debe contar con un servicio de resolución urge de nuevos virus capaz de eliminarlos en el menor tiempo posible. Otros servicios fundamentales son las alertas sobre nuevos virus peligrosos, por ejemplo, a través de listas de correo.

Añadir las opciones de seguridad de las aplicaciones que usa normalmente a su política de protección antivirus. Los programas informáticos más utilizados se

convierten, precisamente por esa razón, en blanco de los autores de virus. Tal es el caso de los navegadores Web, procesadores de texto, programas de correo, entre otros, que disponen de características para asegurar un poco más la información. Si no se está familiarizado con ello, se puede acudir a la ayuda del propio programa y realizar una búsqueda del término “seguridad” para saber cómo utilizarlas. Es conveniente aprovechar estas opciones específicas de seguridad además de contar con un antivirus constantemente actualizado.

Realizar periódicamente copias de seguridad es una buena forma de minimizar el impacto de un antivirus, tanto a nivel corporativo como particular. Realizar copias periódicas y frecuentes de nuestra información más importante es una magnifica política de seguridad. De esta manera, una pérdida de datos, causada por ejemplo por un virus, puede ser superada mediante la restauración de la última copia.

Tener un disquete bootebale libre de virus para poder iniciar la computadora de punto final infectada. Para esto se necesita crear uno en el momento en que se instala el sistema operativo. Se recomienda crear imágenes de disquete de inicio, existe software para ello, tales como “Floppy Imge”, donde se genera un archivo imagen del disquete, y mediante ese programa en cualquier momento se puede crear un disquete booteable desde cualquier máquina y para el sistema operativo del que se haya hecho la imagen.

Esto es similar a lo visto con Norton Ghost, solo que es para disquete. Se recomienda también instalar un programa firewall personal, ya que si usted en dado caso, se ha ejecutado un caballo de Troya, el firewall, evitara de todas formas de punto final, ya que el firewall filtra el tráfico de red, bloqueando puertos que no son de uso común, conocidos como inseguros y puertos que sean indicaos, además este tipo de aplicaciones pide la autorización del usuario para que alguien se conecte a su equipo con la advertencia de seguridad correspondiente, así como permitirle a las aplicaciones el acceso a Internet.

Utilizar certificados digitales en sitios para realizar transacciones, esto permite tener mayor confianza de que es un sitio seguro. Esto se puede observar en el navegador, en una pantalla que aparece al establecer comunicación con el navegador, en una

pantalla que aparece al establecer comunicación con los navegadores donde nos indica si es o no un lugar conocido y certificado. De lo contario, se asume el riesgo de acceder “desconocidos”.

Es recomendable que para guardar el anonimato cuando se navega en Internet para evitar ser presa tan fácil de aquellos que siguen la actividad de los demás (personas dedicadas al marketing, intrusos). Se recomienda que la información que envía el navegador sea mínima, esto para proteger la identidad, dirección y toda aquella información que le pueda ser útil a los espías y que, con la recolección de esta, intente aprovechar del conocimiento sobre nosotros y cobre nuestras vulnerabilidades. Por eso se recomienda el uso de un servidor intermedio al que se dirija de software anonymizer (www.anonymizer.com) el cual funciona de manera sencilla, se accede a el y después solo es necesario introducir la dirección de la página Web solicita software para pasar inadvertido.

Usar unos programas detectores de troyanos como “The cleaner” o software antivirus que tengan la capacidad de reconocer este código. La mayoría de los antivirus actuales tiene en su búsqueda este tipo de código como punto de verificar su existencia u comportamiento. Además, se recomienda verificar que programas son los que están residentes en memorias ala cargar el sistema (en Windows se verifica con la combinación de teclas ctrl. + Alt + Supr emergiendo la pantalla de administrador de programas, en caso de ver algún programa que no hayamos instalado, se recomienda buscar su origen y borrarlo.

6.7.2 Acciones preventivas: recomendaciones para evitar algunos virus.

Algunos virus que hayan atravesado las barreras planteadas hasta el omento pueden encontrarse en estado latente en la máquina, por lo que los siguientes consejos son para provenir de estos riesgos.

- Habilitar la opción para poder ver las extensiones verdaderas de los archivos.
- Deshabilitar el Windows Scripind Host en nuestro PC.

Algunos tipos de virus, en particular los de VBS, son incapaces de ejecutarse si se deshabilitan las opciones de Windows Scripting Host (WSH), es un intérprete de

Java Script y de Visual Basic Script, y puede ayudar a automatizar varias tareas dentro de Windows, pero también puede ser explotado por virus del tipo VBS. Un usuario común no requiere de estas tareas, ya que estas opciones suelen ser usadas solamente por usuarios avanzados o expertos.

Windows Scripting Host habilita la ejecución de scripts (guiones o archivos del tipo de proceso por lotes), directamente desde el escritorio Windows o desde la línea e comandos, sin la necesidad de incluir estos scripts en un documento HTML. los scripts pueden ser ejecutado, de manera similar a un archivo. BAT.

Para desactivar el Windows Scripting Host de su escritorio, se debe proceder alguna de las siguientes maneras:

En todas las versiones de Windows delante de windows2000, existe un programa de Symantec que modifica el registro de forma automática, y funciona en todas las versiones de Windows. Su nombre es NOSCRIPT.EXE (127Kb).

6.7.3 Antivirus.

En las secciones anteriores se han presentado sugerencias para la protección de una computadora de punto final en Internet: navegadores Web, clientes de correo, entre otras. Sin embargo, se sugiere como solución adicional para evitar las infecciones producidas por cualquier tipo de gusano de correo electrónico, independientemente del método que utilice para su propagación, instalar un sistema antivirus eficaz y de calidad reconocida, que cuente con actualizaciones diarias y con un servicio de soporte técnico permanente, capaz de hacer frente a cualquier eventualidad. El software antivirus debe ofrecer protección para discos, correo electrónico y protocolos y conexiones en red. Los programas antivirus deben rastrear en forma constante los virus nuevos. Por último, pero no menos importante, el software se debe actualizar en forma regular para enfrentar las nuevas amenazas de virus. (Váron, 2004)

Organizaciones como AV-Test.org (www.av-test.org), ICSA Labs (www.icsalabs.com) y Virus Bullentin VB100 (www.virusbtn.com) realizan pruebas

continuas para determinar el éxito del software antivirus al detectar los virus más recientes. (Váron, 2004)

6.7.4 Recomendaciones contra el Spyware o espionaje vía la navegación en la red.

Es recomendable la utilización del programa de Lavasoft: AD-Aware 5. Es un programa eficaz y además gratuito, de sencilla utilización, de uso específico para eliminar este tipo de archivos parásitos, con total seguridad y garantizar. Con el instalado, no necesitaremos otro software de detección y eliminación de Spyware.

El uso de navegación o browsers mejor diseñados y por tanto más seguros como al Mozilla basado en Netscape y de libre uso mejoran el performance final de seguridad contra Spyware. Otras aplicaciones que ayudan al respecto es The cleaner, que mejora mucho la lucha contra aplicaciones espías.

Lavasoft: AD-Aware 5 y su modo de funcionamiento y de informes, paso a paso hace que en todo momento conozcamos los archivos detectados, su ubicación y podemos eliminarlos fácilmente. Su velocidad de análisis es muy alta. Es muy recomendable instalar junto con este programa la aplicación Refupdate, disponible en la misma página de descarga, de esta manera podremos mantener actualizado el AD.Aware de una manera muy sencilla y cómoda, así como el módulo de lenguaje Español. (Váron, 2004)

Otros programas anti-espías gratuitos.

- SpyBlocker
- OptOut
- Spychecher
- No-aura
- Internet CleanUp de OnTrack
- XCleaner de XBlock.

Es importante saber que, eliminar estos archivos espías no causaran ningún daño a nuestro sistema, como mucho puede ocasionar que el programa con el que vinieron incorporados deje de funcionar. La prevención y alerta de este tipo de software, también se consigue mediante la utilización de un elemento

imprescindible en nuestro sistema. El firewall, mediante su empleo cerraremos los puertos que estas aplicaciones utilizan, y detectaremos sus intentos de conexión, pues el firewall nos avisara, pidiendo autorización para efectuar dicho acceso a Internet. (Váron, 2004)

6.7.5 Como eliminar el Spam del correo electrónico.

Actualmente, no hay manera de asegurar 100 por ciento que su bandeja de entrada del correo electrónico este libre e spam. Sin embargo, puede hacer cosas para dificultar a los spammers la tarea d obtener su dirección de correo electrónico. Hay también pasos que usted puede seguir cuando el correo electrónico no deseado llega a su buzón. Además, usted puede preguntar a su proveedor de servicios de Internet (ISP) y otras organizaciones para ayudarlo a identificar los orígenes de correo spam. Se puede usar esa información para tratar de bloquear futuros correos de spammers conocidos. (Mcnab, 2004).

Aquí se presentan algunos consejos para prevenir que el spam no llénela bandeja de correo electrónico:

Evite anunciarla dirección de correo electrónico en público. Muchos spammers compran listas de direcciones de correo electrónico de vendedores que compilan sus listas de las direcciones que encuentran en grupos de noticias, sitios Web, espacios para chat, directorios de membresías para servicios en línea, entre otras fuentes. Se debe manejar el BCC. Cada vez que mande un e-mail a más de 3 destinatarios y no sea importe que se vean entre si, como por ejemplo un archivo, use el BCC: o también conocido como CCO:. Para usarlo en Netscape, haga click y deje apretado en el campo To:. Y seleccione BCC. Ahí adentro ponga los destinatarios. (Mcnab, 2004).

Con el Outlook vaya al menú Ver y selecciones ver casilla CCO, y va a aparecer debajo del CC: Ponga los destinatarios en CCO:. MUY FACIL DE HACER. EL BCC hace que NO FIGURE la lista de destinatarios en el mensaje

Otra más es que cuando haga un farward (reenvió) de un mensaje así; se tome 1 segundo y Borre las direcciones de e-mail del mensaje anterior.

Alterne su dirección de correo electrónico antes de anunciarlo públicamente. La lista de vendedores es cosechada con programas de computación que escudriñan paginas Weby grupos de noticias en la búsqueda de direcciones de correo electrónico. Usted puede ser capaz de frustrar estos programas que cosechan alterando el anuncio de sus dirección de correo electrónico en una manera obvia, tal como cambiar robertofigueroa@mail.com a robertoH8SJUNKMAILfigueroa@mail.com. La mayoría de los humanos sabrán que deben quitar H8SJUNKMAIL de la dirección antes de usarla, pero los programas de computación no. (Mcnab, 2004).

Nunca responda a un correo electrónico de spam, aun para no suscribirse. El mensaje de correo electrónico puede incluir instrucciones sobre cómo quitar su dirección de la lista de la organización, tales como contestar con REMOVER en la línea de asunto o llamar un número telefónico. Sin embargo, muchos spammers hacen esto para confirmar que han alcanzado una cuenta verdadera de correo electrónico personal. Es más seguro tirar el mensaje sin responderlo, a menos de que se quiera dar baja de una lista de distribuidores en la que usted se inscribió o que usted conoce al emisor. (Mcnab, 2004).

Revisar los acuerdos de usuario. Cuando se inscribe para servicios basados en Web tales como su banca en línea, para compras o para boletines en línea, debe revisar detenidamente los acuerdos de usuario correspondiente para asegurarse que en su dirección de correo electrónico no se compartirá con otras organizaciones.

Crear una dirección alterna de correo electrónico para usar en el Internet. Su dirección de correo electrónico principal debe ser proporcionado solo a amigos a la familia, a los contactos de negocio, y a gente a quien usted conozca. Considere establecer una segunda dirección de correo electrónico para usar cundo deba llenar las solicitudes de información, las aplicaciones para ofertas especiales y para otros formatos Web.

Establezca filtros para bloquear mensajes de spammers conocidos. Muchos programas de correo electrónico ofrecen una opción de filtro que usted puede usar para mandar correo basura y/o con contenido solo para adultos, automáticamente a una carpeta especifica o a la basura.

Muchos programas permitirán que usted filtre nombres de correo electrónico también. Para asegurar que usted no tira accidentalmente correo de amigos y de familiares, considere crear una carpeta de correo basura para sus mensajes filtrados. Asegúrese de verificar la carpeta antes de vaciarla, o utilice filtros para correo electrónico basura Microsoft Outlook o aprenda más acerca de filtros para spam en el servicio de Internet MSN Informe de Spammers a ISP´s, proveedores de correo electrónico, y a la Comisión Federal de Comercio, (FTC). (Mcnab, 2004).

La mayoría de los proveedores de servicio de Internet (ISP) y proveedores de cuenta tienen una dirección de quejas para asuntos de correo electrónico. Si usted recibe correo no deseado, fíjese en la dirección del remitente. El nombre de ISP debe estar en el centro (entre el signo de @ y el sufijo, por ejemplo, .com), reenvie una copia del correo spam a la dirección de quejas del ISP.

La mayoría de los proveedores tomaran las acciones para eliminar spammers de su sistema. Además, envié una copia de algún correo engañoso o no deseado a la Comisión Federal de Comercio de su país. El Spam parece estar de aquí para quedarse, por lo menos por ahora. Tomar estos pasos lo pueden ayudar a reducir su exposición a este fastidio en línea. Mensajes del tipo HTML. (Mcnab, 2004).

Una forma particularmente peligrosa de correo la constituyen los mensajes de spam en formato HTML. La mayoría de los spammers utilizan la “posibilidad de anular la suscripción” para verificar cuantos de sus mensajes llegan (o feedback) mucho mejor: imágenes.

Se puede comprar este sistema con los contadores de vistas que se encuentran en algunas páginas de la red. El spammer puede ver exactamente cuándo y cuantos de sus mensajes son leídos. Si estudia el spam cuidadosamente verá que algunos casos la URL para imágenes incluidas contiene un numero de secuencia: El

spammer puede ver quien mira el correo y en que momento. Un agujero de seguridad increíble.

Los programas de lectura de correo moderno no mostraran imágenes que se descargan de algún lugar a partir de una URL. Sin embargo, apenas encontraras un lector de HTML moderno y seguro. La última versión de Mozilla mail y Opera mail ofrecen la posibilidad de desactivar las imágenes de recursos externos. La mayoría de los otros programas generaran estadísticas para el spammer. ¿Solución? No utilice un programa que posibilité el correo html o bien descarga el correo primero, desconéctate de Internet y luego lee el correo. Sobre las cadenas de correo electrónico.

No hay ninguna niña muriéndose de cáncer llamada Amy Bruce y si la hubiera, la Fundación Pide un deseo NO va a donar a nada a nadie. Este tipo de emails es fácilmente corroborarle entrando al website de la fundación y buscando el convenio: si fuese cierto, créanme que estaría en el site con todo y la foto de Amy. Para que no vuelvan a caer en esto y ayuden a que internet y nuestro buzón sean lugares más limpios donde trabajar, les explico de que se trata. Las cadenas no son más que instrumentos que utilizan los webmasters de sitios pornográficos, compañías que venden basura, casinos en línea, agencias de esquemas de dinero fácil, empresas que negocian vendiendo listas de correo y otras molestas empresas que utilizan el SPAM para vivir.

La idea es envira una de estas cadenas, que puede ser:

- Ayudar a un niño enfermo.
- Que Ericsson/Nokia/Motorola está regalando celulares.
- Que Volkswagen está regalando el New Beetle.
- Del tipo que amaneció en la bañera sin un riñón.
- Gasolineras que explotan por los celulares.
- Solidaridad con Brian.
- Que gane dinero por vía Internet
- Microsoft paga por cada mensaje reenviado.

De ahí que al poco tiempo todos los usuarios empezaran a recibir Spam cuyo remitente ofrece negocios en los que no se solicitó información. (Mcnab, 2004).

Existen dos maneras de detener esto:

- No reenvíen cadena. - Dar DELETE al mensaje recibido.	- Al colocar las direcciones en el campo BCC, quienes reciben la cadena no podrán ver las direcciones de las demás personas a las que también se les ha enviado y se detiene un poco el Spam. Al menos no vamos a estar dando las direcciones de nuestros familiares y amigos así tan fácilmente. ¿Por qué las personas continúan las cadenas? Básicamente por desconocimiento.

Debemos educarnos y utilizar el correo electrónico en forma apropiada y aprender a distinguir entre lo real y la farsa. Es muy distinto, por ejemplo, que un amigo del trabajo o de la universidad envié un correo solicitando ayuda solidaria a varias personas y estas a su vez difundan la información a otros conocidos, a que reenviemos un e-mail que nos llegó desde fuera de nuestro círculo de amistades a 50 personas conocidas para que una empresa X donde una cierta cantidad de dinero para operar a alguien que vive en X lugar. Es recomendable que se haga caso omiso a este tipo de mensajes, mencionados anteriormente. (Mcnab, 2004).

Capítulo 7. Conclusiones

El derecho siempre va a la saga en los delitos informáticos es por eso que es imperativo la actualización de la legislación en materia de términos informática de esta manera en este trabajo se establecen algunas de las tendencias de los ciberdelitos que podrían ser usados como referente para el diseño de nuevas leyes. A sí mismo, se aporta un manual de prevención a estas tendencias de ciberdelitos. Todas estas formas de ciberdelitos, de acuerdo con (Florez, 2013), para los próximos diez años el cibercrimen se caracterizará por el aumento, la demanda de espionaje comercial, robo de base de datos y ataques a la reputación de las empresas, en 2008 Data Breach Investigations Report, realizo 500 investigaciones forenses en base a 240 millones por ataques de registros vulnerados, y revelaron que el 66% de las empresas que han sido víctimas de ataques cibernéticos perdieron información que no sabían que tenían; 73% de los ataques provinieron de fuentes internas y 18% fueron causados por gente interna; el 75% no fueron detectados por la empresa victima sino por un tercero y que el 42% de los ataques analizados se efectuaron a través de un acceso remoto. Por su parte, la OCDE en el informe sobre Malwares del 2007, hace énfasis en la vulnerabilidad que tienen la economía de internet y las economías ante el “boom” de ataques de software malicioso(que según la empresa ScanSafe se había incrementado en 40% ese año), ya que esta situación puede afectar la confianza de los consumidores, disminuyendo su disposición a realizar diferentes transacciones por esta vía, lo que impone a las empresas la necesidad de realizar esfuerzos por crear una cultura que prevenga este tipo de actos de manera de evitar robos de información que se traduzca en mermas de ingreso por la pérdida de productividad y confianza de sus clientes.

Capítulo 8. Referencias

8.1. Glosario

Sistemas.

Es un conjunto de elementos o individuos que forman un todo organizado, que interactúan entre si y tienen coherente, o bien, como, un conjunto de elementos relacionados entre si de manera que un cambio en el estado de cualquiera de ellos altera el estado de otros elementos. (Gomez, 2000).

Ciberdelitos.

Es un término genérico que hace referencia a la actividad delictiva llevada a cabo mediante equipos informáticos o a través de internet. El ciberdelito puede hacer uso de diferentes métodos y herramientas, como el pishing, los virus etc., normalmente con el objetivo de robar información personal o de realizar actividades fraudulentas. (Ciberseguridad, 2009).

Datos.

Es la representación simbólica, bien sea mediante números o letras de una recopilación de información la cual puede ser cualitativa o cuantitativa, que facilitan la deducción de una investigación o un hecho. (Fuentes, 2013).

Manual.

Es un instrumento de trabajo que contiene el conjunto de normas y tareas que desarrolla cada funcionario en sus actividades cotidianas, y será elaborada técnicamente basados en los respectivos procedimientos, sistemas normas y que resumen el establecimiento de guías y orientaciones para desarrollar las rutinas. (Rural, 2004).

Protección.

Se refiere al acto de proteger y a su resultado, siendo verbo derivado en su etimología del latín “proteger” siendo, “pro” lo que se hace en favor de algo o alguien,

y “tejere” = cubrir, aludiendo al cuidado que se brinda aun objeto o sujeto. (Cardenas., 2016).

Derecho.

Es el conjunto de normas que imponen deberes y normas que confieren facultades, que establecen las bases de convivencia social cuyo fin es dotar a todos los miembros de la sociedad de los mínimos de seguridad, certeza, igualdad, libertad y justicia. (Atienza, 2001).

Legislación.

Se denomina al cuerpo de leyes que regulan determinada materia o ciencia o al conjunto de leyes a través del cual se ordena la vida en un país, lo que popularmente se llama ordenamiento jurídico y que establece aquellas conductas y acciones aceptables o rechazables de un individuo. (Goddard, 2010).

Malware.

Programa maligno. Son todos aquellos programas diseñados para causar daños al hardware, software, redes, como los virus. Es un término que se utiliza al referirse a cualquier programa malicioso. (TECHNOLOGY, 2012).

Software.

Es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora. (Goddard, 2010).

Bibliografía

Alvares Marañon Gonzalo, P. G. (2004). *Seguridad Informatica para las Empresas Particulares.* McGraw-Will.

Amenazas., I. A. (2014). *Symantec Corporation.*

Amercianos, O. d. (2014). *TENDENCIAS DE SEGURIDAD CIBERNETICA EN AMERICA LATINA Y EL CARIBE.* Symantec.

Atienza, M. (2001). *El sentido delderecho .* Barcelona: Ariel.

Bermejo, J. B. (2007). *Ataques DoS en la web.* EAZEL.

Cardenas., F. O. (2016). *ADMINISTRACION DEL RIESGO CIBERNETICO UN ENFOQUE DESDE LA ALTA GERENCIA EMPRESARIAL.* COLOMBIA: Universidad Militar Alta Granada.

Chung, W., Chenb, H., & Changc, W. a. (2004). *Fighting cybercrime: a review .*

Ciberseguridad, D. d. (2009). *El ciberdelito.* ITU.

CONASSOL. (2005). *CONGRESO NACIONAL DE SEGURIDAD Y SOFTWARE LIBRE.*

Corporation, S. (2010). *Underground Economy Servers.* Symantec Security Response.

Corporation, S. (2013). *Ibid. en 48.*

Corporation., S. (2014). *Informe anual sobre amenazas.*

Corporation., S. (28 de agosto de 2013.). *Symantec Security Response.*

Corporation., S. (April 2014). *Informe anual sobre amenazas 19.* Norton.

cybercrimen, R. t. (2001). *Cyber Crimen and Security - The Transnational Dimension .*

Detousen., E. (2005). Ataques Externos. *Linux Focus.org.*, 15.

Florez, M. E. (2013). *América Latina, ¿debe crear un sistema de normas armonizadas para el cibercrimen?* Chile.

Fuentes, D. M. (2013). *Base de Datos.*

Gaytán, E. R. (2009). *Seguridad de la Informacion y Delitos Informaticos .*

Gercke, P. D. (2014). *Comprension del Ciberdelito, Fenomenos dificultades y respuestas.*

Goddard, J. A. (2010). *Ética, Legislación y Derecho.*

Gomez, A. S. (2000). *Sistemas: Conceptos y Cracteristicas.*

Gordon/Ford. (2006). *On the Definition and Classification of Cybercrimen.*

Hernández, F. B. (2007). *Propuesta de Seguridad en la Información.* Instituto Politecnico Nacional.

Ibid. (s.f.). *Ibid. en 40.*

Issue, M. P. (2014). *Ransom Ware' Virus Warning.* México: Associated Press.

Jaén, U. d. (2012). *Sofware Maliciosos.*

Jason Kohn. (2013). *The Internet is Booming in Latin America,.*

Jou, F. (2000). *Desing and implementation of a scalable intrusion detection Information Survability.* Darpa.

Kaspersky, M. a. (2017). *Windows Defender es un gran antivirus.*

KPMG. (2014). *Encuenta de Fraudes en Colombia.* COLOMBIA: Obtenido de http://www.kpmg.com/CO/es/IssuesAndInsights/ArticlesPublications/Documents/Encuesta%20de%20Fraude%20en%20Colombia%202013.pdf.

Krebs., B. (2013). *Inside a 'Reveton' Ransomware Operation.* KrebsOnSecurity.

Leal, J. C. (2010). *LA NORMATIVIDAD INFORÁTICA Y EL ACCESO A LA INFORMACIÓN EN MÉXICO.*

Leal, J. c. (2013). *Normatividad Informatica en México.*

Machicado, J. (2010). *Apuntes Juridicos "DELITO".*

Mauricio Muñoz, S. S. (2010). *Seguridad Informatica .* UNIVERSIDAD TECNICA FEDERICO.

Mcnab, C. (2004). *Seguridad de redes.* Anaya Multimedia.

México, G. d. (2014). *Estadisticas.* México.

MICRO, T. (2013). *Tendencias en la seguridad cibernética.*

Mirkovic, J. a. (2014). *A toxonomy of DDoS attack and DDoS defensemechanisms. SIGCOMM Comput.* Commun, Rev.

Mirkovic, J. D. (2004). *Intenet Denial of SERVICE.*

Murillo, P. L. (2010). *Derecho Informatico.*

NTMX, A. (13 de mayo de 2017). Ciberataque mundial WannaCry sigolpea a empresas de México. *El Sol de México*, pág. 3.

Pérez, R. P. (2010). *Office. Todo Prectica.* Copyright.

Power, R. (2002). *CSI/FBI computer crime and security survey. .* Computer Security Issues & Trends 8.

Pulse, G. (2012). *Big Data for Development: Challenges & Opportunities.* Francia.

Quintero, B. (2011). *Intypedia.* Madrid,España: Hispasec.

Reducers. (2010). Ransomware secuestro digital. *Seguridad*, 3.

Rio, I. F. (2012). *Politica y Legislación Informática.* México: Red de Tercer Milenio S.C.

ROMERO, J. D. (2016). *EL CIBERCRIMEN Y LAS POSIBLES ESTRATEGIAS ADMINISTRATIVAS Y FINANCIERAS A ADOPTAR EN MATERIA DE CIBERSEGURIDAD EN LAS EMPRESAS COLOMBIANAS, A PARTIR DEL ESTUDIO DE CASO: BBVA COLOMBIA.* COLOMBIA: UNIVERSIDAD MILITAR NUEVA GRANADA.

Rural, S. d. (2004). *Manual de Procedimiento s.*

Sanchez, L. H. (2014). *Buenas Practicas para la implemnatcion de la seguridad computacional.* UNAM.

Schuba, C. K. (1997). *Analysis of a denial of service attack on TCP.* Proceedings of the IEE.

State, O. o. (2013). *Tendencias en las seguridad cibernética en America Latina y el Caribe y respuestas de los gobiernos.* OAS Secretariat.

Sueñe Llinás, E. (1986). *Introduccion a la Informatica Juridica y el Derecho de la Informatica.* Madrird España.

Symantec. (2014). *Tendencias de Seguridad Cibernetica en America Latina y el Caribe.*

TECHNOLOGY, E. S. (2012). *Guía de respuesta a una infeccion por malware.* ESET.

Tripwire for servers. (2007).

Union., C. d. (1917). *COSNTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.*

V. Batíz- Álvarez, M. F.-E. (2011). *LEGISLACION INFORMATICA EN MÉXICO.* LIDETEA.

Váron, A. A. (2004). *Protege tu PC.* Anaya Multimedia.

Virtual. (2013). Control en cada punto de venta. *Netcamara pos.*