



UNIVERSIDAD AUTÓNOMA DEL ESTADO DE
MÉXICO.



Centro Universitario UAEM Texcoco.

**“ELECCIÓN Y DISEÑO DE TECNOLOGÍAS SOBRE SEGURIDAD DE
LA INFORMACIÓN PARA DEPENDENCIAS DE GOBIERNO (SSP).”**

TESINA

QUE PARA OBTENER EL GRADO DE
LICENCIADO EN INFORMÁTICA ADMINISTRATIVA

PRESENTA:

LARA CASTRO JOSÉ FABIÁN

DIRECTOR

M. en C. CARLOS OCELOTL RIVERA VILLA

REVISORES

DR. ADRIÁN TRUEBA ESPINOSA

M. en C. YEDID ERANDINI NIÑO MEMBRILLO

TEXCOCO ESTADO DE MÉXICO 2012

Texcoco, México a 13 de Julio de 2012

M. EN C. JUAN MANUEL MUÑOZ ARAUJO
SUBDIRECTOR ACADÉMICO DEL
CENTRO UNIVERSITARIO UAEM TEXCOCO.

COPIA

PRESENTE:

AT'N M. EN FIN. GUADALUPE LIZETH ARCE CHÁVEZ
RESPONSABLE DEL DEPARTAMENTO DE TITULACIÓN.

Con base en las revisiones efectuadas al trabajo escrito titulado "ELECCIÓN Y DISEÑO DE TECNOLOGÍAS SOBRE SEGURIDAD DE LA INFORMACIÓN PARA DEPENDENCIAS DE GOBIERNO (SSP)." que para obtener el título de la licenciatura en Informática Administrativa presenta el sustentante Lara Castro José Fabian, con numero de cuenta 0022424 respectivamente, se concluye que cumple con los requisitos teóricos-metodológicos necesarios para su aprobación, pudiendo continuar con la etapa de impresión del trabajo escrito.

ATENTAMENTE


M. en C. YEDID ERANDINI NIÑO MEMBRILLO
REVISOR


DR. ADRIÁN TRUEBA ESPINOSA
REVISOR


M. en C. CARLOS OCELOTL RIVERA VILLA
DIRECTOR

C.C.P. Sustentante.- Lara Castro José Fabian.
C.C.P. Director.- M. en C. Carlos Ocelotl Rivera Villa.
C.C.P. Titulación.



AGRADECIMIENTOS

A Dios.

Por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mi Mamá Tere y Mi Papá Roberto.

Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mi Esposa Erika y a mi Princesa Camila.

Porque por ustedes mis esfuerzos de perseverancia, amor y dedicación se multiplican ya que son la fuente de inspiración de mi fortaleza diaria y cada día que pasa recibo amor por parte de ustedes.

A mis hermanos.

Porque gran parte de este triunfo les pertenece ya que han estado siempre al pendiente de mis triunfos y fracasos, de los cuales siempre tuve un aliciente por parte de ustedes para levantarme y seguir adelante.

A mis maestros.

Por su gran apoyo y motivación para la culminación mis estudios profesionales y para la elaboración de esta tesina, por su tiempo compartido y por impulsar el desarrollo de nuestra formación profesional y por apoyarnos en todo momento.

Gracias

Índice General

ÍNDICE GENERAL	4
ÍNDICE DE FIGURAS	8
ÍNDICE DE TABLAS	9
INTRODUCCIÓN	10
1 CAPÍTULO 1. INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN.....	11
1.1 CONCEPTOS BÁSICOS.....	12
1.1.1 <i>La Información</i>	12
1.1.1.1 Características de la Información	13
1.1.1.2 Valores de la Información	14
1.1.2 <i>La Informática</i>	14
1.1.3 <i>Activo</i>	15
1.1.3.1 Tipos de Activos	15
1.1.3.2 Tipo de Recursos	16
1.1.4 <i>La Seguridad</i>	17
1.2 SEGURIDAD INFORMÁTICA VS SEGURIDAD DE LA INFORMACIÓN	18
1.3 LA SEGURIDAD INFORMÁTICA	18
1.4 LA SEGURIDAD DE LA INFORMACIÓN:	18
1.4.1 <i>Principios Básicos de Seguridad de la Información</i>	19
1.4.1.1 Confidencialidad.....	20
1.4.1.2 Integridad.....	20
1.4.1.3 Disponibilidad.....	21
1.5 ANTECEDENTES EN MÉXICO DE ROBO DE INFORMACIÓN DURANTE LA PRIMERA DÉCADA DEL SEGUNDO MILENIO. ...	21
2 CAPÍTULO 2 SEGURIDAD INFORMÁTICA	24
2.1 OBJETIVOS DE LA SEGURIDAD INFORMÁTICA.....	25
2.2 RAZONES PARA IMPLEMENTAR LA SEGURIDAD INFORMÁTICA.....	25
2.3 ELEMENTOS A PROTEGER.....	26
2.4 ATAQUES A LA SEGURIDAD INFORMÁTICA	26
2.4.1 <i>Ataque</i>	26
2.4.2 <i>Tipos de Ataques</i>	27
2.4.2.1 Ataques Pasivos.....	27
2.4.2.2 Ataques Activos.....	27
2.4.3 <i>Tipos de Atacantes</i>	29
2.5 VULNERABILIDAD	31
2.5.1 <i>Tipos de Vulnerabilidades</i>	31
2.5.1.1 Vulnerabilidades Físicas	31
2.5.1.2 Vulnerabilidades Naturales	32
2.5.1.3 Vulnerabilidades de Hardware.....	32
2.5.1.4 Vulnerabilidades de Software	32
2.5.1.5 Vulnerabilidades del Medio de Almacenaje	32
2.5.1.6 Vulnerabilidades de Comunicación	33
2.5.1.7 Vulnerabilidades Humanas.....	33
2.6 RIESGO	33

2.6.1	<i>Elementos del Riesgo</i>	34
2.6.1.1	Probabilidad	34
2.6.1.2	Amenazas	34
2.6.1.3	Vulnerabilidades.....	34
2.6.1.4	Pérdidas.....	35
2.6.2	<i>Tipos de Riesgos</i>	35
2.6.2.1	Riesgos lógicos	36
2.6.2.2	Riesgos físicos.....	36
2.6.3	<i>Evaluación de Riesgos</i>	37
2.7	DEBILIDADES DE SEGURIDAD COMÚNMENTE EXPLOTADAS	37
2.7.1	<i>Vulnerabilidad del Factor Humano</i>	37
2.7.1.1	Ingeniería Social	38
2.7.1.2	Factor Insiders	38
2.7.2	<i>Recopilación de Información Pasiva</i>	39
2.7.2.1	OSINT (Open Source Intelligence o Inteligencia de Fuente Abierta)	39
2.7.3	<i>Explotación de vulnerabilidades</i>	41
2.7.3.1	Malware (Códigos Maliciosos)	41
2.7.3.2	Denial of Service (Negación de servicio)	42
2.7.3.3	SQL Injection (Inyección de código SQL)	44
2.8	ETAPAS QUE CONFORMAN UN ATAQUE	45
2.8.1	<i>Fase 1: Reconnaissance (Reconocimiento)</i>	45
2.8.2	<i>Fase 2: Scanning (Exploración)</i>	46
2.8.3	<i>Fase 3: Gaining Access (Obtener acceso)</i>	46
2.8.4	<i>Fase 4: Maintaining Access (Mantener el acceso)</i>	47
2.8.5	<i>Fase 5: Covering Tracks (Borrar huellas)</i>	47
2.9	MÉTODOS UTILIZADOS PARA LA EJECUCIÓN DE ATAQUES	47
2.9.1	<i>Eavesdropping y Packet Sniffing</i>	47
2.9.2	<i>Snooping y Downloading</i>	48
2.9.3	<i>Tampering</i>	49
2.9.4	<i>Spoofing y Looping</i>	49
2.9.5	<i>Jamming o Flooding</i>	50
2.10	HERRAMIENTAS PARA DESCUBRIMIENTO DE VULNERABILIDADES	51
2.10.1	<i>Actividad en Internet</i>	51
2.10.2	<i>Análisis de Red</i>	51
2.10.3	<i>Anti Espionaje (Antispyware)</i>	52
2.10.4	<i>Antispam</i>	52
2.10.5	<i>Antivirus</i>	52
2.10.6	<i>Bloqueo y Restricción</i>	52
2.10.7	<i>Contraseñas</i>	53
2.10.8	<i>Detectores de Agujeros de Seguridad</i>	53
2.10.9	<i>Encriptación de Comunicaciones</i>	53
2.10.10	<i>Firewalls</i>	54
2.10.11	<i>Gestión de Accesos</i>	54
2.10.12	<i>Recuperación de Datos</i>	54
2.10.13	<i>Seguridad en Comercio Electrónico</i>	54
3	CAPÍTULO 3 ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN	55

3.1	INTRODUCCIÓN.....	55
3.1.1	EA (<i>Enterprise Architecture o Arquitectura Empresarial</i>)	56
3.1.2	ISA (<i>Information Security Architecture o Arquitectura de Seguridad de la Información</i>)	57
3.1.3	SI (<i>Security Information o Seguridad de la Información</i>)	58
3.2	EISA (ENTERPRISE INFORMATION SECURITY ARCHITECTURE O ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN EMPRESARIAL).....	59
3.2.1	Objetivo de la EISA.....	60
3.2.2	Implementación de la EISA	61
3.2.3	Transición de la organización implementando la EISA	62
3.2.4	Relación de la EISA con otros marcos o frameworks	63
3.2.4.1	FEA (Federal Enterprise Architecture o Arquitectura Empresarial Federal)	64
3.2.4.2	DoDAF (Architecture Framework the U.S. Department of Defense o Marco de Arquitectura del Departamento de Defensa de los E. U.).....	65
3.2.4.3	MODAF (British Ministry of Defence Architecture Framework o Marco de Arquitectura del Ministerio de Defensa Británico).....	66
3.2.4.4	TOGAF (Architecture Framework The Open Group o Marco de Arquitectura de Open Group)	66
3.2.5	Beneficios al implementar una EISA	67
4	CAPÍTULO 4. HERRAMIENTAS DE PROTECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN	68
4.1	HERRAMIENTAS ORIENTADAS A LA SEGURIDAD LÓGICA	68
4.1.1	Router o Enrutador	69
4.1.2	Firewall o Cortafuego	69
4.1.3	IPS (<i>Intrusion Prevention System o Sistema de Prevención de Intrusiones</i>).....	70
4.1.4	IDS (<i>Intrusion detection system o Sistema de Detección de Intrusiones</i>)	71
4.1.5	VPN (<i>Virtual Private Network o Red Privada Virtual</i>)	72
4.1.6	Proxy	72
4.1.7	DLP (<i>Data Loss Prevention o Prevención de Pérdida de Datos</i>)	73
4.1.7.1	Funcionalidad de DLP	73
4.1.7.2	Características de DLP	74
4.2	ANÁLISIS DE RIESGO EN LA IMPLEMENTACIÓN DE NUEVAS TECNOLOGÍAS.	75
5	CAPÍTULO 5. LA PÉRDIDA DE DATOS EN LAS ORGANIZACIONES	77
5.1	PRINCIPALES PUNTOS DE FUGA DE LA INFORMACIÓN.....	77
5.2	FACTORES DE FUGA Y PÉRDIDA DE INFORMACIÓN.....	78
6	CAPÍTULO 6. ANÁLISIS DE TECNOLOGÍAS SOBRE PREVENCIÓN DE PERDIDA DE DATOS EN LA SSP....	80
6.1	DESCRIPCIÓN GENERAL DEL ANÁLISIS.....	81
6.2	SITUACIÓN ACTUAL DEL MERCADO SOBRE PROVEEDORES DE DLP	81
6.3	ASPECTOS ESTABLECIDOS POR LA SSP PARA ELEGIR EL PROVEEDOR DE DLP	83
6.4	ANÁLISIS DE PROVEEDORES DE DLP.....	84
6.4.1	Cuadro de comparación resultados	86
6.5	ELEMENTOS DE PRUEBA PARA LA EVALUACIÓN DEL PROVEEDOR DE DLP EN LA SSP	87
6.5.1	Matriz de evaluación DLP.	88
6.5.2	Requerimientos técnicos para la evaluación de las soluciones de DLP.....	88
6.5.3	Criterios de prueba sobre información sensible.....	89
6.6	RESULTADO DE LA EVALUACIÓN DE PROVEEDORES DE DLP	90
	CONCLUSIONES Y RECOMENDACIONES	92

BIBLIOGRAFÍA	95
ANEXO 1	100

Índice de Figuras

FIGURA 1 ESQUEMA DE IMPORTANCIA DE ACTIVOS	15
FIGURA 2 TRIADA CIA.....	20
FIGURA 3 ATAQUE DE INTERRUPCIÓN.....	28
FIGURA 4 ATAQUE DE INTERCEPCIÓN	28
FIGURA 5 ATAQUE DE MODIFICACIÓN	28
FIGURA 6 ATAQUE DE FABRICACIÓN	29
FIGURA 7 ATAQUE DE DESTRUCCIÓN	29
FIGURA 8 TIPOS DE INTRUSOS	30
FIGURA 9 ELEMENTOS DEL RIESGO	33
FIGURA 10 EJEMPLO INYECCIÓN DE CÓDIGO	44
FIGURA 11 INFORMACIÓN OBTENIDA	44
FIGURA 12 ETAPAS DE UN ATAQUE	45
FIGURA 13 ROUTER O ENRUTADOR.....	69
FIGURA 14 FIREWALL O CORTAFUEGO	70
FIGURA 15 IPS O SISTEMA DE PREVENCIÓN DE INTRUSIONES.....	70
FIGURA 16 IDS O SISTEMA DE DETECCIÓN DE INTRUSIONES	71
FIGURA 17 VPN O RED PRIVADA VIRTUAL	72
FIGURA 18 SERVIDOR PROXY	72
FIGURA 19 CUADRANTE MÁGICO SOBRE PROVEEDORES DE DLP	81
FIGURA 20 MATRIZ DE EVALUACIÓN DLP	100

Índice de Tablas

TABLA 1 RIESGOS LÓGICOS	36
TABLA 2 RIESGOS FÍSICOS	36
TABLA 3 COMPARATIVO TÉCNICO PROVEEDORES DLP.....	86
TABLA 4 COMPARACIÓN DE CUMPLIMIENTO PROVEEDORES DLP	86
TABLA 5 CRITERIOS DE PRUEBA SOBRE INFORMACIÓN SENSIBLE	89

Introducción

Hoy día, en México las dependencias de gobierno y cualquier organización que almacene información sensible, necesitan dotar sus sistemas e infraestructuras informáticas de políticas y medidas de protección adecuadas, que garanticen el continuo desarrollo y sostenibilidad de sus actividades diarias. Es imprescindible disponer de protección adecuada en los sistemas informáticos que asegure desde la privacidad de los datos hasta la seguridad en las transacciones de información, pasando por el análisis de flujo de información, el control de acceso, los protocolos de comunicación y las transferencias de datos.

En la Secretaría de Seguridad Pública (SSP) comúnmente se presentan usos indebidos de la red mismos que pueden afectar de manera directa a la seguridad de la misma, ya que no cuenta con las suficientes medidas para asegurar la información que fluye dentro y fuera de la red de datos, dando como resultado posible fugas de la información ya sea confidencial o sensible tales como Información a directores, contratos, proyectos futuros, configuración de equipos y contraseñas de acceso, pudieran enviarla fuera de las instalaciones sin ninguna restricción. Aunque la SSP cuenta con herramientas para la gestión de permisos o acceso a la red (Firewall y Proxy), no hay aplicativos que permitan estar analizando permanentemente la información que fluye hacia afuera de la red.

Es por esto que se realiza un análisis que facilite la integral protección de la información en las diferentes capas de flujo de información, permitiendo conocer y esquematizar los puntos débiles de la red, así como analizar entre las diferentes opciones existentes en el mercado que sirva como base para el cumplimiento de las normas de calidad estipuladas para dependencias que manejan información personal y privada. Es importante mencionar que en dicho análisis no se contempla la parte correspondiente a la seguridad física.

Capítulo 1. Introducción a la Seguridad de la Información.

Desde el surgimiento de la raza humana en el planeta, la información estuvo presente bajo diversas formas y técnicas. El humano buscaba representar sus hábitos, costumbres e intenciones en diversos medios que pudiesen ser utilizados por él y por otros de su especie, además de la posibilidad de ser llevados de un lugar a otro. La información valiosa era registrada en objetos preciosos y sofisticados como pinturas magníficas, que se almacenaban con mucho cuidado en lugares de difícil acceso, a cuya forma y contenido sólo tenían acceso quienes estuviesen autorizados o listos para interpretarla.

Al día de hoy, la información es el activo de mayor valor con el que las organizaciones cuentan a diario. El progreso de la informática y de las redes de comunicación presenta un nuevo escenario que las organizaciones necesitan cubrir con herramientas que le permitan ayudarle a lograr un nivel óptimo de seguridad en el manejo de la Información durante todo su ciclo, así como contar mecanismos de pronta respuesta en el caso de que se vulnere alguna de sus medidas de protección.

Por esto y otros motivos, que la seguridad de la información es un asunto tan importante para todos, pues afecta directamente a las actividades diarias de una organización.

1.1 Conceptos Básicos

Con cierta frecuencia se confunden conceptos básicos relacionados con la seguridad de la información. Por ello, se considera oportuno incluir la siguiente terminología básica que puede ayudar a fundamentar conceptos que resultan claves para entender en toda su dimensión el alcance de los distintos capítulos.

1.1.1 La Información.

(Diebold, 1979), introdujo el concepto de que la información debía ser manejada como un recurso fundamental en la organización. Más tarde, (Synott, 1991) inauguraron una línea de pensamiento basada en la convicción de que la información merecía recibir una mayor consideración por las organizaciones.

La información es un recurso estratégico más de la organización. El personal, los medios materiales y económicos son considerados recursos de la misma porque generan utilidades, es decir, son productivos. Pero la información también produce beneficios ya que tiene la misión de informar, revelar alternativas, reduce incertidumbres, ayuda a la toma de decisiones y devela soluciones entre otras cosas. (Hornos, 1998).

La información puede llegar a ser un elemento decisivo que determine el éxito o el fracaso de un negocio, con el fin de lograr la máxima utilidad de la información ésta debe administrarse de manera correcta, como ocurriría con cualquier otro recurso de la organización.

En la actualidad, la globalización permite el acceso a enormes volúmenes de información depositados en soportes cada vez más complejos, con increíbles posibilidades de almacenamiento y conexión con otras fuentes. Me refiero a las bases de datos, las redes de transmisión de datos y la red de Internet.

1.1.1.1 Características de la Información

En el momento en que la organización decide hacer uso de la información, ésta debe ser correcta y actual, debe cumplir con las necesidades de quien la requiere y debe de estar disponible cuando se le requiera.

Lo que caracteriza a la información en una organización, según (Alin, 1997), es su capacidad de intercambio. La información es un producto perecedero que si se decide solo almacenada esta pierde interés y valor. Lo verdaderamente importante es poder contar con información de contenido actual que sirva como factor determinante en la toma de decisiones.

Hoy en día la información tiene una estructura interna y puede ser calificada según varios aspectos:

- **Efectiva:** la información entregada debe ser oportuna, correcta, consistente, utilizable y referida al nivel de la organización al cual se dirige.
- **Eficiente:** que la provisión de la información se realice a través de la utilización óptima de recursos, es decir, de la forma más productiva y económica.
- **Confiable:** que la provisión de información sea la apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.
- **Cumplimiento:** se refiere a que la información proporcionada debe cumplir con leyes, regulaciones y acuerdos contractuales a los que el proceso de negocio está sujeto.
- **Confidencial:** la información debe estar protegida de divulgaciones no autorizadas.
- **Íntegra:** se refiere a la precisión y suficiencia de la información y su validez de acuerdo a los valores y expectativas de negocio.

- Disponible: la información debe estar disponible cuando es requerida por el proceso de negocio.

1.1.1.2 Valores de la Información

El valor de la información, se deriva del aumento que debe originar en el rendimiento de la organización. (Escobar, 1997)

(Solay, 2010), dice que “el valor de la información ha tomado una posición de altísima relevancia en todos los ámbitos. En los negocios, en el gobierno, en la educación y en la vida personal.”

Es así que se deben reconocer valores a la información, esta debe garantizar la continuidad del proceso, debe ser conocida por el personal que la necesita y que la usa y debe ser manejada como un activo de gran valor.

Los valores reconocidos a la información son:

- Crítica, Información necesaria para llevar a cabo una acción determinada y para evaluar su grado de cumplimiento.
- Valiosa, es un activo corporativo que tiene valor en sí mismo.
- Sensitiva, debe ser conocida únicamente por las personas que necesitan los datos.

1.1.2 La Informática

El diccionario de la Real Academia Española 2011, define a la informática como el “conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras.”

En cuanto al contenido de la Informática, se encarga de estudiar todo lo relacionado con las computadoras que incluye desde los aspectos de su arquitectura y fabricación hasta los aspectos referidos a la organización, seguridad y almacenamiento de la información.

1.1.3 Activo

(Peltier, 2001). “Un activo es algo que tiene valor o utilidad para la organización, sus operaciones y su continuidad. Los activos necesitan protección para asegurar las correctas operaciones del negocio y la continuidad de la organización.”

Es de suma importancia determinar cuáles son los activos importantes de la organización y cuál sería el impacto que produciría si llegasen a faltar.

1.1.3.1 Tipos de Activos

- La Información en todo su contenido.
- Los Equipos que la soportan (Software y Hardware)
- Las Personas que la utilizan o usuarios.

Se debe crear una lista de los activos que posee la organización, todo aquel que tenga que ver con la red de datos y su desempeño, una vez obtenidos, éstos se clasifican en una tabla de prioridad, para ello utilizando el esquema de importancia, se tiene un criterio para clasificarlos mediante el efecto que tendría en la organización si el activo faltase.

La Figura 1 muestra el esquema de importancia en que se pueden agrupar los activos. La técnica es enfocarse primero en los activos que su falla es imprescindible o muy importante y luego en los de menor jerarquía

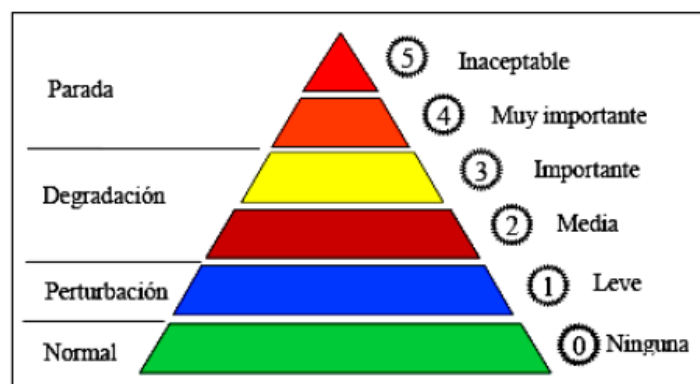


Figura 1 Esquema de importancia de activos

Cada activo debe estar claramente identificado, valorado apropiadamente y conocer quien es el responsable directo de la administración del activo. El ISO 17799:2005 o bien 27002:2005, (código para la práctica de la gestión de la seguridad de la información), clasifica los activos de la siguiente manera:

- Activos de información. Bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo y planes de continuidad
- Documentos impresos. Contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes del negocio
- Activos de software. Software de aplicación, software de sistemas y herramientas de desarrollo
- Activos físicos. Equipos de comunicación, computación, medios magnéticos y otros equipos técnicos
- Personas: Personal, clientes, suscriptores, entre otros

1.1.3.2 Tipo de Recursos

Se debe de entender por recursos, a los activos productivos de la organización. Para tener una visión más completa es útil identificar los tres principales tipos de recursos:

- Recursos Tangibles: Físicos.
- Recursos Intangibles: Tecnológicos y Reputación.
- Recursos humanos: Personal.

Los recursos tangibles, son los más fáciles de identificar y evaluar, ya que se refiere a todos los recursos físicos de la organización, mismos que pueden ser representados en los estados contables, en los recursos financieros. Con estos se pretende comprender su potencial para crear una ventaja competitiva.

Los recursos intangibles, contribuyen mucho más que los tangibles al valor de sus activos totales suele referirse a aquellos activos que por su naturaleza acrecientan su valor ya sea monetario o de aceptación.

Las marcas registradas y otras marcas comerciales son una forma de activos relacionados con la reputación: su valor reside en la confianza que infunden a los clientes. Al igual que la reputación, la tecnología es un activo intangible cuyo valor no se evidencia con claridad en la mayoría de las inversiones de las organizaciones.

Los recursos humanos, son las personas que ofrecen sus servicios productivos a la organización, relacionados con sus habilidades, conocimientos y capacidad para razonar y tomar decisiones. Identificar y evaluar los recursos humanos de una organización es complejo y difícil.

Las organizaciones deben de apoyar la iniciativa, el potencial de aprendizaje y la habilidad para trabajar en equipo de sus empleados, ya que una buena cultura organizacional se relaciona con los valores, tradiciones y normas sociales, que afectan a la destreza y a la motivación de los empleados.

1.1.4 La Seguridad

De acuerdo con el Diccionario de la Real Academia de la Lengua Española (consultado en marzo de 2011).

- Seguridad; Cualidad de seguro.
- Seguro: libre y exento de todo peligro, daño o riesgo.

1.2 Seguridad Informática vs Seguridad de la Información

1.3 La Seguridad Informática

Es la forma más habitual de referirse a todo aquello que tiene que ver con la seguridad de los servidores y los sistemas. Seguridad Informática es un término que puede resultar muy familiar, pero que hoy en día es un poco complejo.

(Aguirre, 2006), define a la seguridad informática como “el conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas”.

La Seguridad Informática nació en la época en la que no existían las redes de banda ancha, los teléfonos móviles o los servicios de internet como las redes sociales o las tiendas virtuales. Es por ello que la Seguridad Informática suele hacer un especial énfasis en proteger los sistemas, es decir, los servidores, las redes, la información y el resto de infraestructuras en las organizaciones.

1.4 La Seguridad de la Información:

Es evidente que cuando se protege un servidor, un dispositivo, una infraestructura de comunicación o un servicio, en realidad lo que se está protegiendo es la información que es almacenada, enviada, transmitida y modificada en dichos servicios, infraestructuras o dispositivos, ya que la tecnología es un elemento cada vez más perecedero, y que se requiere cambiar constantemente.

(Zendejas, 2000), define a la seguridad de la información o SI como la función de control o supervisión que permite, a una institución u organización conservar las características de Integridad, confidencialidad y disponibilidad de sus sistemas de información computarizados, esta función de control se realiza con recursos y tecnologías que se emplean a efecto de reducir las variables que afecten el escenario de seguridad: La amenaza y la vulnerabilidad convertidas en riesgos.

Para la SI se tiene en cuenta la protección de la información desde tres puntos de vista: técnico, organizativo y legal.

La SI se ha convertido en el enfoque de referencia ya que dispone de normas estandarizadas que permiten la implantación de sistemas que facilitan la gestión en la seguridad de la Información siguiendo criterios, metodología y medidas estandarizadas que facilitan la labor a las organizaciones evitando futuros problemas.

1.4.1 Principios Básicos de Seguridad de la Información.

La SI exige que se tenga el cuidado necesario para evitar accesos inadecuados, modificación o manipulación de los datos.

La SI debe ser un camino para identificar malos hábitos y usos inadecuados de los recursos de la organización, y buscar la manera de implementar buenas prácticas y hábitos más correctos y responsables.

La SI debe identificar los riesgos y las amenazas a las que están expuestas las organizaciones, en qué medida las pueden afectar y cómo poder minimizarlas. Y, en el caso de que se produzca algún desastre, ayuda a establecer pautas y procedimientos para reducir sus consecuencias.

La SI se logra llevando a cabo un conjunto conveniente de controles, incluyendo las políticas, los procesos, procedimientos, estructuras orgánicas y funciones del hardware y software. Estos controles deben ser establecidos, implementados, supervisados, revisados y mejorados para asegurar que se cumple con la seguridad y los objetivos de negocio en la organización.

La SI es universal y aplicable en cualquier actividad, organización, proceso o actividad y en definitiva, donde exista información que tenga importancia para una organización o para una actividad.

De acuerdo con (Pfleeger, 1997), “la seguridad de la información es la preservación de la *Confidentiality* o Confidencialidad, *Integrity* o Integridad y *Availability* o Disponibilidad (CIA) de la información y recursos de información”, ver Figura 2.



Figura 2 Triada CIA

La correcta gestión de la SI busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de éstas características falla no se está ante nada seguro.

1.4.1.1 Confidencialidad

(ITIL¹, 2006), define a la confidencialidad como “la propiedad que asegura que la información es accedida solamente por personal o entidad autorizados a tal efecto.”

1.4.1.2 Integridad

(Trevor, 2003), la define como “la protección de la información de daño o manipulación deliberada.”

La integridad se refiere a que la información debe permanecer completa y no sufrir alteraciones cuando se utilice, a menos que existan los privilegios adecuados para hacerlo.

¹ Information Technology Infrastructure Library o Biblioteca de Infraestructura de Tecnologías de la Información

1.4.1.3 Disponibilidad

(Nichols, 2002), la define “como la información que está libre para ser utilizada por los usuarios autorizados cuando fuere requerida.”

La disponibilidad además de ser importante en el proceso de seguridad de la información, es variada en el sentido de que existe más de un mecanismo para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en la infraestructura tecnológica, servidores de correo electrónico, de bases de datos y web, mediante el uso de equipos en alta disponibilidad, la gama de posibilidades dependerá de lo que se quiere proteger y el nivel de servicio que se quiera proporcionar.

Es preciso anotar, además, que la seguridad de la información no es ningún estado final, es más un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que puede suceder, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener para la toma de medidas de seguridad oportunas.

1.5 Antecedentes en México de robo de información durante la primera década del segundo milenio.

Tomando como referencia a (Urrutia, 2003):

De acuerdo con la investigación hecha por la Contraloría Interna del Instituto Federal Electoral (IFE), Juan López Bedolla, quien laboró en Vanguardia en Informática empresa que daba servicio al Registro Nacional de Población de ser el responsable de haber sustraído aparentemente en forma ilegal la información del Registro Nacional de Población (RENAPO).

En conferencia de prensa, el contralor del IFE, Mario Espínola Pinedo, deslindó al organismo de cualquier responsabilidad en la venta del padrón electoral a la empresa estadounidense “*ChoicePoint*”. Explicó que se realizaron dos investigaciones paralelas: Una interna y la otra a cargo de la Fiscalía Especializada para la Atención de Delitos Electorales (FEPADE) de la Procuraduría General de la República (PGR), las cuales determinaron que ningún funcionario o trabajador del IFE tuvo que ver con este ilícito.

Tomando como referencia a (Fuentes, 2008):

El allanamiento y robo sufrido este fin de semana en las instalaciones de Comunicación e Información de la Mujer AC (CIMAC) es un acto condenable y representa un atentado a la labor de difusión e investigación a los derechos humanos de las mujeres que realiza esa institución.

No se llevaron equipos informáticos nuevos, los dejaron a cambio de llevarse equipos más viejos, pero con información sustantiva. Hay evidencias de la revisión, realizada por los delincuentes, de la información que trabaja CIMAC porque algunos de los equipos se encontraron encendidos.

Tomando como referencia a Senado de la Republica (2010):

El Senado de la República aprobó por unanimidad expedir la Ley Federal de Protección de Datos Personales en posesión de los particulares, a fin de salvaguardar y regular el tratamiento legítimo, controlado e informado de las bases de datos, garantizando la privacidad y el derecho a la autodeterminación informativa de las personas.

Con esta ley se otorga protección a los llamados datos sensibles, relacionados con las preferencias sexuales, origen étnico o racial o estado de salud, que podrían ser mal utilizados para discriminar o excluir a una persona.

Entre las obligaciones de los sujetos que utilizar la información de las personas están que sólo se haga uso de los datos personales para los fines por los que fueron recabados, observando medidas de seguridad que eviten su pérdida, robo o acceso no autorizado.

Capítulo 2 Seguridad Informática

El concepto de seguridad informática no debe ser confundido con el de seguridad de la información, ya que la seguridad informática se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

(Cano, 2004), describe la seguridad informática como “la disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así contar con estrategias para avanzar ante cualquier eventualidad.”

En términos generales, la seguridad informática puede entenderse como una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software, bases de datos, metadatos², archivos e información privilegiada o confidencial, que signifique un riesgo si ésta llega a manos de otras personas.

La seguridad informática es necesaria ya que existen personas que buscan tener acceso a la red empresarial, aplicaciones, bases de datos, para modificar, sustraer datos y borrar datos sensibles o de importancia para la organización.

Esta situación se puede presentar gracias a los esquemas ineficientes de seguridad informática con los que cuentan la mayoría de las organizaciones, originando la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño considerable.

² Son datos altamente estructurados que describen información

2.1 Objetivos de la Seguridad Informática

Entre los principales objetivos de la seguridad informática, propuestos por (Gómez, 2007), se destacan los siguientes:

- Minimizar y administrar los riesgos y detectar los posibles problemas y amenazas de seguridad dentro de la organización.
- Garantizar el uso adecuado de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con las regulaciones vigentes y con el marco legal.

2.2 Razones para Implementar la Seguridad Informática.

- Para permitir el correcto funcionamiento de la actividad empresarial,
- Es una obligación legal normativa en México para dependencias de gobierno que manejen información personal. Lo anterior de acuerdo a Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), (6 de julio de 2010) y Ley de Servicios de la Sociedad de la Información (LSSI) en 2002,
- Puede actuar de factor diferenciador (certificación ISO 17799 o ISO 27002), es un estándar para la seguridad de la información,
- Protege ante posibles fallos humanos, intencionales o no,
- Evita que usuarios internos puedan atacar sistemas externos (con la responsabilidad legal que ello conlleva),
- Previene la entrada de intrusos en los sistemas,
- Impide que usuarios descontentos puedan causar daños importantes que lleguen a alterar o incluso a detener las actividades de la organización.

2.3 Elementos a Proteger.

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos.

- Por hardware entendemos al conjunto de todos los sistemas físicos del sistema informático: computadoras personales, servidores, cableado, impresoras, CD, DVD, cintas, componentes de comunicación
- El software son todos los elementos lógicos que hacen funcional al hardware: sistema operativo, aplicaciones, utilidades
- Los datos que son un conjunto de información lógica y estructurada que manipula el software y el hardware: bases de datos, documentos, archivos

Además, algunos autores hacen mención de un cuarto elemento llamado fungible³; que son aquellos que se gastan o desgastan con el uso continuo: papel, tóner, tinta, cintas magnéticas, disquetes. De los cuatro elementos, los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo son imposibles de recuperar, se debe de pasar obligatoriamente por un proceso de *backup* o copias de seguridad.

2.4 Ataques a la Seguridad Informática

2.4.1 Ataque

(Mieres, 2009), dice que un ataque consiste en aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

³ Del latín *fungi*, gastar y *ble*; que se consume con el uso (Diccionario de la Real Academia de la Lengua)

2.4.2 Tipos de Ataques

Un ataque no es más que la materialización de una amenaza. Los dos tipos generales de ataques son:

2.4.2.1 Ataques Pasivos

El atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico.

Generalmente se emplean para:

- Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

2.4.2.2 Ataques Activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se les puede subdividir en cinco categorías:

- **Interrupción:** hace que un objeto del sistema se pierda, quede inutilizable o no disponible, ver figura 3.

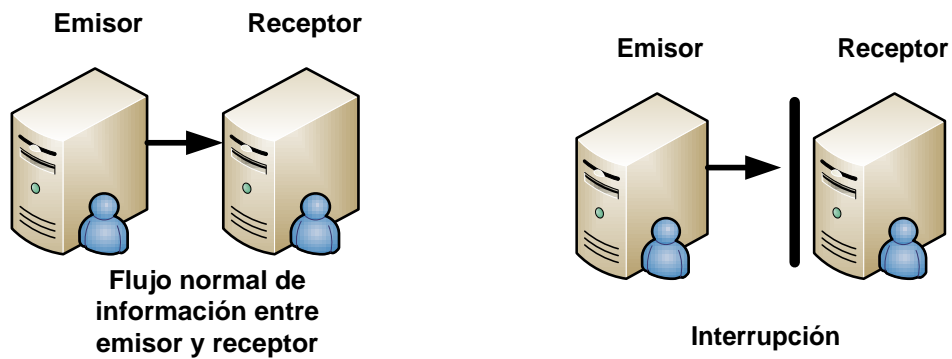


Figura 3 Ataque de Interrupción

- **Intercepción:** hace que un elemento no autorizado consiga el acceso a un determinado objeto del sistema, ver figura 4.

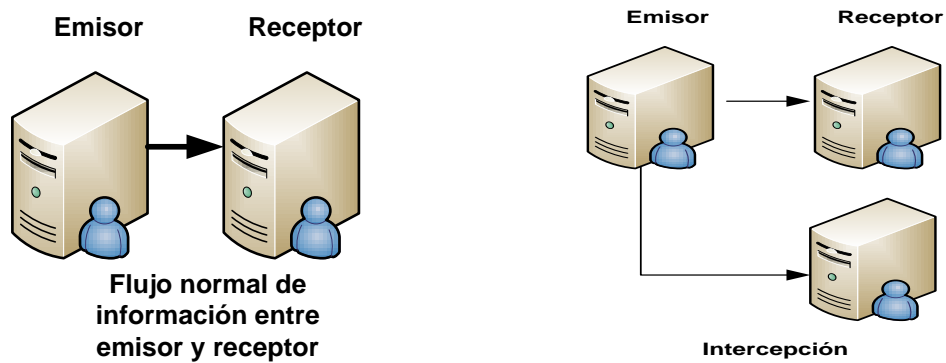


Figura 4 Ataque de Intercepción

- **Modificación:** si además de conseguir el acceso consigue hacer una transformación del objeto, ver figura 5.

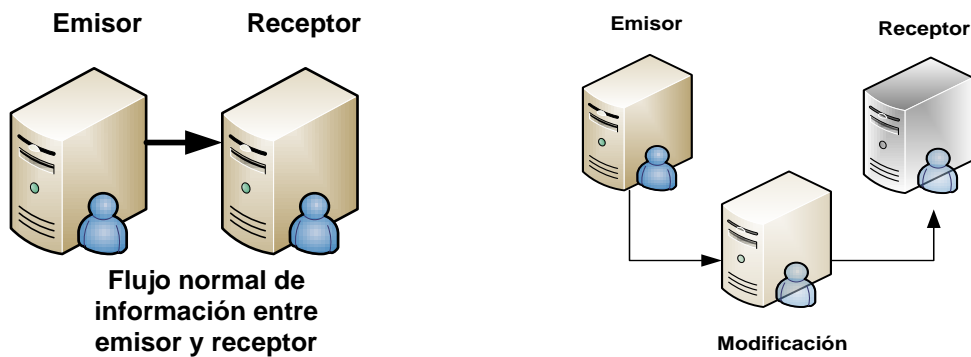


Figura 5 Ataque de Modificación

- **Fabricación:** se desarrolla un objeto similar al original atacado de forma que es difícil distinguirlos entre sí, ver figura 6.

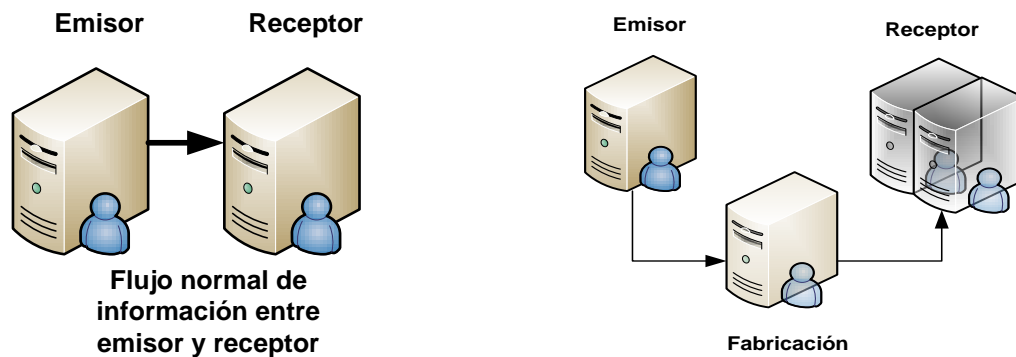


Figura 6 Ataque de Fabricación

- **Destrucción:** es una modificación que elimina o inutiliza el objeto, ver figura 7.

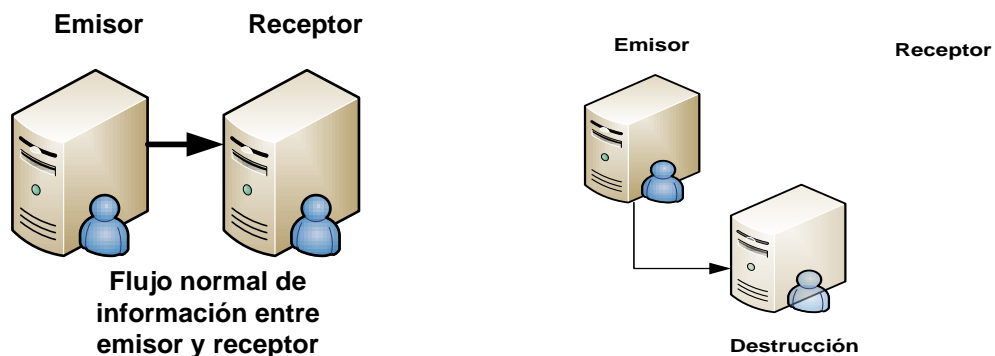


Figura 7 Ataque de Destrucción

2.4.3 Tipos de Atacantes

Se llama intruso o atacante a la persona que accede o intenta acceder sin autorización a un sistema ajeno, ya sea en forma intencional o no.

Ante la pregunta de los tipos de intrusos existentes (Ardita, 2009), contesta lo siguiente:

Los tipos de Intrusos podríamos caracterizarlos desde el punto de vista del nivel de conocimiento, formando una pirámide como se puede observar en la figura 8.

- **Clase A:** es el 80% que se refiere a los nuevos intrusos que bajan programas de Internet y los prueban, están solo jugando, son pequeños grupitos que se juntan y deciden probar.
- **Clase B:** es el 12% son más peligrosos, saben compilar programas aunque no saben programar, prueban programas que circulan por la red, escanean las vulnerabilidades e intentan ingresar por ellas.
- **Clase C:** es el 5% es gente que tiene conocimiento en programación, conocen como detectar el sistema operativo que usa la víctima. A partir de aquí buscan todos los accesos remotos e intentan ingresar.
- **Clase D:** el 3% restante son expertos con conocimiento avanzado saben que buscar y como vulnerar determinados sistemas, utilizan herramientas para borrar sus huellas y no ser identificados.

Para que un intruso pueda avanzar de una clase base a una clase superior se requiere en primer lugar tiempo y que vaya adquiriendo nuevas habilidades que le permitan identificar las vulnerabilidades en objetivos específicos así como la forma para poder evitar ser detectados. Ver figura 8.

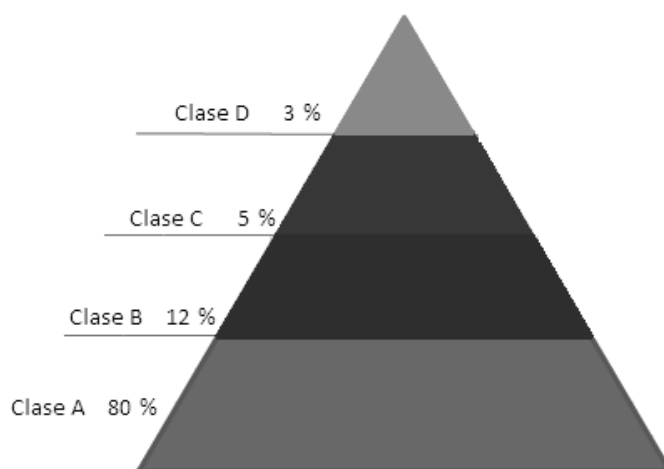


Figura 8 Tipos de intrusos

Fuente: CYBSEC, Security Systems 2009, <http://www.cybsec.com/ES/default.php>

2.5 Vulnerabilidad

El *Internet Engineering Task Force (IETF)* en su *Internet Security Glossary*, define a la vulnerabilidad como un desperfecto o debilidad en el diseño, implementación u operación y manejo de un sistema que puede ser explotado para violar la política de seguridad de dicho sistema.

Así mismo la mayoría de los sistemas tienen algún tipo de vulnerabilidad, pero esto no significa que el sistema sea defectuoso para su uso. No toda amenaza resulta en un ataque, y no todo ataque tiene éxito. El éxito depende del grado de la vulnerabilidad, la fuerza del ataque y la efectividad de cualquier contramedida aplicada.

Las vulnerabilidades son el resultado de *Bugs* o errores de software, o de fallos en el diseño del sistema, también pueden ser el resultado de las propias limitaciones tecnológicas. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales conocidas como *Exploits*⁴.

Las vulnerabilidades en las aplicaciones suelen corregirse con un *service pack*, *Hotfixs*⁵ o con cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático.

2.5.1 Tipos de Vulnerabilidades

A continuación se describen cada uno de ellos:

2.5.1.1 Vulnerabilidades Físicas

Están presentes en los ambientes en los cuales la información se está almacenando o manejando.

- Instalaciones inadecuadas.
- Ausencia de equipos de seguridad.
- Cableados desordenados, expuestos o de mala calidad.
- Falta de Identificación de personas, equipos y áreas restringidas.

⁴ Son una secuencia de comandos con el fin de automatizar el aprovechamiento de una vulnerabilidad

⁵ Son un paquete que puede incluir varios archivos y que sirve para resolver un *bug* específico

2.5.1.2 Vulnerabilidades Naturales

Los puntos débiles naturales son aquellos relacionados con las condiciones ambientales que puedan colocar en riesgo la información.

- Desastres naturales y sismos.
- Inundaciones e Incendios.
- Humedad y filtraciones.
- Polvo.
- Temperaturas indebidas (mayores o menores a las requeridas por los equipos).

2.5.1.3 Vulnerabilidades de Hardware

Los posibles defectos en la fabricación o configuración de los equipos de la organización que pudieran permitir el ataque o alteración de los mismos.

- Ausencia de actualizaciones.
- Conservación o mantenimiento inadecuado.

2.5.1.4 Vulnerabilidades de Software

Los puntos débiles de aplicaciones permiten que ocurran accesos indebidos a sistemas informáticos incluso sin el conocimiento de un usuario o administrador de red.

- Configuración e instalación indebida de los programas.
- Sistemas operativos mal configurados, mal organizados o piratas.
- Ausencia en la aplicación de parches o actualizaciones.
- Ejecución de macro virus.

2.5.1.5 Vulnerabilidades del Medio de Almacenaje

La utilización inadecuada de los medios de almacenaje afecta directamente a la integridad, confidencialidad, y disponibilidad de la información.

- Plazos de validez y caducidad de los medios (licenciamiento y garantía).
- Defectos de fabricación del medio.
- Uso incorrecto del medio en relación a la forma de manejo del mismo.
- Mala calidad, o uso de medios genérico.
- Áreas o lugares de depósito inadecuados (humedad, calor, magnetismo).

2.5.1.6 Vulnerabilidades de Comunicación

Esta abarca todo el tránsito de la información, ya sea cableado, satelital, fibra, u ondas de radio inalámbricas.

- El desempeño de los equipos, involucrados en la comunicación.
- Caídas de servicio a los usuarios.
- Información disponible a usuarios incorrectos.

2.5.1.7 Vulnerabilidades Humanas

Son los daños que las personas pueden causar a la información, a los equipos o a los ambientes tecnológicos, los puntos débiles humanos pueden ser causados intencionados o no.

- Desconocimiento de las medidas de seguridad adecuadas.
- Falta de capacitación y conciencia específica a los usuarios.
- Uso de contraseñas débiles u obvias.

2.6 Riesgo

La ISO 27001 (SGSI – Sistema de Gestión de seguridad de la información), define riesgo como “la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños.”

En la definición anterior se pueden identificar varios elementos que se deben comprender adecuadamente para entender integralmente el concepto de riesgo. Estos elementos son: probabilidad, amenazas, vulnerabilidades, activos y pérdidas, ver figura 9.



Figura 9 Elementos del Riesgo

En lo relacionado con seguridad, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (por ejemplo el riesgo de perder datos debido a rotura de disco o virus informáticos).

2.6.1 Elementos del Riesgo

A continuación se describen cada uno de ellos:

2.6.1.1 Probabilidad

Establecer la probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción favorable, o sea, debe considerarse en cada caso qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

Existen amenazas, como por ejemplo incendios, para las cuales hay información suficiente (series históricas, compañías de seguros y otros datos) para establecer con razonable objetividad su probabilidad de ocurrencia. Otras amenazas presentan mayor dificultad en establecer cuantitativamente la probabilidad.

2.6.1.2 Amenazas

Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la organización. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, facilidad de acceso a las instalaciones. Las amenazas pueden ser de carácter físico o lógico, como ser una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso.

2.6.1.3 Vulnerabilidades

Son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevan a esos activos a ser vulnerables.

Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

2.6.1.4 Pérdidas

Las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo. Se puede establecer que las más comunes son: la pérdida directa de dinero, la pérdida de confianza, la reducción de la eficiencia y la pérdida de oportunidades de negocio. Otras no tan comunes son la pérdida de vidas humanas y afectación del medio ambiente.

2.6.2 Tipos de Riesgos

En la actualidad existe discrepancia en una clasificación estándar para los tipos de riesgos ya que dependiendo a la actividad humana que se está desarrollando es el tipo y nivel de clasificación del riesgo.

(Reynolds, 1991), los clasifica de la siguiente manera de acuerdo a los riesgos más significativos así como la probabilidad e impacto de que ocurran, ver tabla 1 y tabla 2.

Probabilidad:

Real Academia de la Lengua (consultado en mayo de 2011).

- Probabilidad; Cualidad de probable, que puede suceder.
- Probable: Que se puede probar.

Impacto

Diccionario libre "*The Free Dictionary*" (consultado en mayo de 2011).

- Impacto; Conjunto de consecuencias provocadas por un hecho o actuación que afecta a un entorno o ambiente social o natural.

2.6.2.1 Riesgos lógicos

Son aquellos daños que los activos pueden sufrir en su estado lógico o de procesamiento interno y que perjudican directamente a su software.

Riesgos lógicos	Probabilidad	Impacto
Caída de la red	Media	Alto
Caída de servicios en ambientes de producción	Media	Bajo
Extracción, modificación y destrucción de información confidencial	Baja	Alto
Ataques de virus informáticos	Alta	Alto
Pérdida y Fuga de información	Media	Alto
Inadecuados controles de acceso lógicos (contraseñas débiles)	Baja	Alto
Falta de disponibilidad de aplicaciones críticas	Baja	Alto
Descontrol del personal	Medio	Bajo

Tabla 1 Riesgos Lógicos

2.6.2.2 Riesgos físicos

Se entiende como aquellos riesgos que el activo puede sufrir en su estado físico o material, que perjudica directamente al hardware.

Riesgos Físicos	Probabilidad	Impacto
Inadecuados controles de acceso físico	Alta	Bajo
Instalaciones inadecuadas	Media	Alto
Incendio	Baja	Bajo
Robo	Media	Alto
Desastres naturales	Baja	Alto

Tabla 2 Riesgos Físicos

2.6.3 Evaluación de Riesgos

El análisis o evaluación de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas.

- Se debe poder obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis, contra el costo de volverla a producir o reproducir.
- Se debe tener en cuenta la probabilidad que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.
- Se debe conocer qué se quiere proteger, dónde y cómo, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se deberá identificar los recursos de hardware, software, información, personal, accesorios, con que se cuenta y las amenazas a las que se está expuesto.

2.7 Debilidades de seguridad comúnmente explotadas

A continuación se expondrán algunos de los ataques perpetrados principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de persona, red o sistema operativo, usando diferentes protocolos.

2.7.1 Vulnerabilidad del Factor Humano

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los *Insiders* (personas con acceso a información exclusiva), utilizaban sus permisos para alterar archivos o registros. Los *Outsiders* (alguien que observa un grupo desde fuera), ingresaban a la red simplemente averiguando una contraseña válida.

2.7.1.1 Ingeniería Social

Existen estrategias de ataque que se basan en el engaño y que están netamente orientadas a explotar las debilidades del factor humano por lo que los atacantes saben cómo utilizarlas y lo han incorporado como elemento para llevar a cabo cualquier tipo de ataque.

Si bien esta estrategia es utilizada en cualquier ámbito, en informática, consiste en la obtención de información sensible y/o confidencial de un usuario cercano a un sistema u organización.

Sin lugar a dudas, las personas constituyen uno de los problemas más importantes de seguridad para cualquier organización porque a diferencia de los componentes tecnológicos, son el único elemento, dentro de un entorno seguro, con la capacidad de decidir romper las reglas establecidas en las políticas de seguridad informática, ya sea por ignorancia, negligencia o coacción, pueden permitir a un atacante obtener acceso no autorizado, para eludir los complejos esquemas y tecnologías de seguridad implementados en la organización. Por ejemplo, en este sentido, la confianza y la divulgación de información son dos de las debilidades más explotadas para obtener datos relacionados a un sistema.

2.7.1.2 Factor Insiders

Cuando se habla sobre las personas que se dedican a atacar sistemas informáticos, se asume que se trata de alguien desconocido que realiza el ataque y maneja todo desde un lugar remoto llevándolo a cabo a altas horas de la noche. Aunque en algunos casos puede ser cierto, pero se han demostrado que la mayoría de las violaciones de seguridad son cometidas por los mismos empleados en horarios de oficina, desde dentro de la institución u organización.

Una de las formas más eficaces que posee un atacante para romper los esquemas de seguridad, es desde el interior de la organización. Por ejemplo, el atacante podría conseguir un empleo en la organización que desea atacar y obtener el suficiente nivel de confianza en la organización para luego explotar los puntos de acceso.

Del mismo modo, cualquier integrante puede convertirse en un empleado disgustado y decidir robar información y/o causar daños como una forma de venganza. Cuando este tipo de actos es cometido con intenciones de obtener beneficios económicos a través de información corporativa, es denominado *Insiders Trading* (comercio del personal interno).

2.7.2 Recopilación de Información Pasiva.

Los atacantes, aprenden constantemente estrategias de ataque que le permiten penetrar los esquemas de seguridad por más complejos que sean.

2.7.2.1 OSINT (Open Source Intelligence o Inteligencia de Fuente Abierta)

Una de las primeras facetas de un ataque informático, consiste en la recolección de información a través de diferentes técnicas como *reconnaissance* (reconocimiento), *discovery* (descubrimiento), *footprinting* (huella digital) o Google Hacking y precisamente, *Open Source Intelligence* se refiere a la obtención de información desde fuentes públicas y abiertas.

La información recolectada por el atacante, no es más que la consecuencia de una detallada investigación sobre el objetivo, enfocada a obtener toda la información pública disponible sobre la organización desde recursos públicos. En este aspecto, un atacante gastará la mayor parte de su tiempo en actividades de reconocimiento y obtención de información porque cuanto más aprende el atacante sobre el objetivo, más fácil será llevar a cabo con éxito el ataque.

Generalmente, los atacantes hacen inteligencia sobre sus objetivos durante varios meses antes de comenzar las primeras interacciones lógicas contra el objetivo a través de diferentes herramientas y técnicas como el *scanning* (exploración), *banner grabbing* (captura de titulares) y rastreo de los servicios públicos.

Aun así, estas actividades son sólo sondeos sutiles que buscan verificar los datos obtenidos.

Los responsables de las organizaciones se sorprenderían al ver el enorme caudal de información que se puede encontrar en Internet sobre, no sólo las actividades propias de la organización, sino que también, información sobre las actividades de los empleados y su familia.

A través del siguiente listado se refleja algunos ejemplos concretos sobre el tipo y sensibilidad de la información que un atacante podría obtener haciendo OSINT:

- Los nombres de sus altos jefes/ejecutivos y de cualquier empleado pueden ser obtenidos desde comunicados de prensa.
- La dirección de la organización, números telefónicos y números de fax desde diferentes registros públicos o directamente desde el sitio web.
- Qué, o cuáles, organizaciones proveen el servicio de Internet (*ISP* o *Internet service provider*) a través de técnicas sencillas como *DNS lookup* y *traceroute*.
- La dirección del domicilio del personal, sus números telefónicos, currículum vitae, datos de los familiares, puestos en los que desempeña funciones, antecedentes penales y mucho más buscando sus nombres en diferentes sitios.
- Los sistemas operativos que se utilizan en la organización, los principales programas utilizados, los lenguajes de programación, plataformas especiales, fabricantes de los dispositivos de *networking* (red), estructura de archivos, nombres de archivos, la plataforma del servidor web y mucho más.
- Documentos confidenciales accidentalmente, o intencionalmente enviados a cuentas personales de personas que en la actualidad no guardan relación alguna con la organización, más allá del paso por la misma.
- Vulnerabilidades en los productos utilizados, problemas con el personal, publicaciones internas, declaraciones, políticas de la institución.
- Comentarios en blogs, críticas, jurisprudencia y servicios de inteligencia competitiva.

En la mayoría de los casos, las organizaciones brindan una enorme cantidad de datos que hacen de la tarea de recolectar información una cuestión sencilla.

2.7.3 Explotación de vulnerabilidades

A través de los años se han desarrollado estrategias cada vez más sofisticadas de ataque para explotar agujeros en el diseño, configuración y operación de los sistemas.

2.7.3.1 Malware (Códigos Maliciosos)

El *Malware* o códigos maliciosos, constituyen también una de las principales amenazas de seguridad para cualquier institución u organización ya que suele ser motivo de importantes pérdidas económicas. Esta amenaza se refiere a programas que causan algún tipo de daño o anomalía en el sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, *spyware*, *backdoors*, *rootkits*, *keyloggers*, entre otros.

Actualmente, la mayoría de los ataques informáticos son llevados a cabo por códigos maliciosos, a través de programas troyanos.

Este tipo de malware ingresa a un sistema de manera completamente encubierta activando una carga dañina denominada *payload* o carga útil, que despliega las instrucciones maliciosas.

La carga dañina que incorporan los troyanos puede ser cualquier cosa, desde instrucciones diseñadas para destruir algún sector del disco duro, por lo general la *master boot record* (sector cero o de arranque), eliminar archivos, registrar las pulsaciones que se escriben a través del teclado, monitorear el tráfico de la red, entre tantas otras actividades.

Los atacantes suelen utilizar troyanos de manera combinada junto a otros tipos de códigos maliciosos. Por ejemplo, cuando han ganado acceso a través del troyano, implantan en el sistema otros códigos maliciosos como *rootkits* que permite esconder las huellas que el atacante va dejando en el equipo, y *backdoor* (puerta trasera), para poder ingresar al sistema cuantas veces considere necesario; todo, de manera remota y sin que, en la mayoría de los casos, los administradores de la red adviertan su actividad.

Si bien cualquier persona con conocimientos básicos de computación puede crear un troyano y combinar su *payload*, con programas benignos a través de aplicaciones automatizadas y diseñados para esto, los troyanos poseen un requisito particular que debe ser cumplido para que logren el éxito: necesitan la intervención del factor humano, en otras palabras, tienen que ser ejecutados por el usuario.

Es por ello que estas amenazas se diseminan por medio de diferentes tecnologías como dispositivos USB, mensajería instantánea, redes P2P (compartición de archivos y recursos), e-mail y a través de alguna metodología de engaño, aparentando ser programas inofensivos bajo coberturas como protectores de pantalla, tarjetas virtuales, juegos en flash, diferentes tipos de archivos, simulando ser herramientas de seguridad, entre tantos otros.

2.7.3.2 Denial of Service (Negación de servicio)

Es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos. Algunos ejemplos de este tipo de ataque son:

- Tentativas de inundar (*to flood*) una red, evitando de esta manera el tráfico legítimo de datos en la misma.
- Tentativas de interrumpir las conexiones entre dos máquinas evitando, de esta manera, el acceso a un servicio.
- Tentativas de evitar que una determinada persona tenga acceso a un servicio.
- Tentativas de interrumpir un servicio específico a un sistema o a un usuario;

Cabría tener en cuenta que, el uso ilegítimo de recursos puede también dar lugar a la negación de un servicio. Por ejemplo, un hacker puede utilizar un área del FTP (Protocolo de Transferencia de Archivos) anónimo como lugar para salvar archivos, consumiendo de esta manera espacio en el disco y generando tráfico en la red.

Como consecuencia, los ataques de negación de servicio pueden esencialmente dejar inoperativa una computadora o una red. De esta forma, toda una organización puede quedar fuera de Internet durante un tiempo determinado.

Algunos ataques de negación de servicio se pueden ejecutar con recursos muy limitados contra un sitio grande y sofisticado.

Por ejemplo, un atacante con una vieja computadora y un módem puede poner fuera de combate a máquinas rápidas y sofisticadas. Últimamente, esto es común con ataques de los denominados *Nukes*, que consiste en enviar paquetes de datos ICMP que son mensajes de error fragmentados o de alguna otra forma inválidos a un objetivo en específico.

Hay tres tipos de ataques básicos de negación de servicios:

- a) Consumo de recursos escasos, limitados, o no renovables.- Las computadoras y las redes necesitan para funcionar ciertos recursos: ancho de banda de la red, espacio de memoria y disco, tiempo de uso de la computadora, estructuras de datos, acceso a otras computadoras y redes, entre otros
- b) Destrucción o alteración de información de configuración.- Una computadora incorrectamente configurada puede no funcionar bien o directamente no arrancar. Un hacker puede alterar o destruir la información de configuración del sistema operativo, evitando de esta forma se pueda usar una computadora o red.
- c) Destrucción o alteración física de los componentes de la red.- Es muy importante la seguridad física de la red. Se debe resguardar contra el acceso no autorizado a las computadoras, los *routers*, los racks de cableado de red, los segmentos de red, y cualquier otro componente crítico de la red.

2.7.3.3 SQL Injection (Inyección de código SQL)

La inyección de código SQL pertenece al tipo de ataques de validación de información ingresada por el usuario y consiste en la modificación del comportamiento de las consultas mediante la introducción de parámetros no deseados en los campos a los que tiene acceso el usuario.

En la figura 10 se muestra un apartado tomado de una página pública de una dependencia de Gobierno en México que sirve de ejemplo para la inyección de código SQL.

Ingreso a la Bolsa de Trabajo (BAE)

*USUARIO: [input field]

*CONTRASEÑA: [input field]

Los campos marcados con * son requeridos

Ingresar Cancelar

Soy un nuevo usuario: [Quiero Registrarme](#)

Figura 10 Ejemplo Inyección de código

Este tipo de errores puede permitir a usuarios malintencionados acceder a datos a los que de otro modo no tendrían acceso y, en el peor de los casos, modificar el comportamiento de las aplicaciones, ver figura 11.

Presiona los botones del menú superior para capturar tus datos. Deberás registrar los valores requeridos marcados con *

Actualizar Datos de RAUL

NO: 1

*NOMBRE: RAUL

*APELLIDO PATERNO: [input]

APELLIDO MATERNO: [input]

USUARIO: [input]

CONTRASEÑA: [input]

LUGAR DE NACIMIENTO: LEON, GTO.

*FECHA DE NACIMIENTO: 17 Julio 1978

*RFC: CAVR7807172E0 No editable

*MESES DESEMPLEADO: BUSCANDO OTRA OPCION

*ESTADO CIVIL: SOLTERO(A)

*SEXO: MASCULINO

*NACIONALIDAD: MEXICANA

*ESTADO: GUANAJUATO

*MUNICIPIO: LEÓN

*COLONIA: MIGUEL HIDALGO

*CALLE: SAN JOSE ESQUILON

Figura 11 Información obtenida

2.8 Etapas que conforman un Ataque

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del reforzamiento a la seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

En la figura 12, se muestra las cinco etapas por las cuales suele pasar un ataque al momento de ser ejecutado:

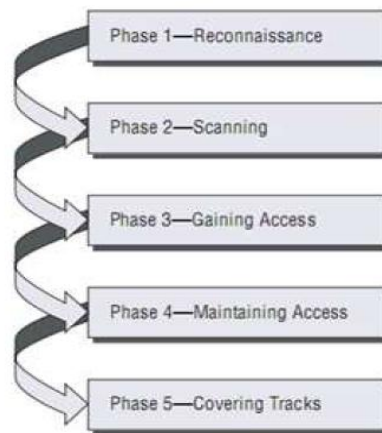


Figura 12 Etapas de un ataque

Fuente: Graves, K. (2007), *Official Certified Ethical Hacker*, Sybex.

2.8.1 Fase 1: Reconnaissance (Reconocimiento).

Esta etapa involucra la obtención de información o *Information Gathering*⁶, con respecto a una potencial víctima que puede ser una persona u organización. Implica la recopilación de información sobre un objetivo potencial, sin el individuo afectado o el conocimiento de la organización. El reconocimiento pasivo puede ser tan simple como ver un edificio para identificar cuando los empleados entran en el edificio y cuando ellos salen. Sin embargo, la mayoría de los reconocimientos es cuando los *hackers* están buscando información sobre un posible blanco, realizada sentado delante de una computadora.

⁶ Técnica de obtener información sensible de alguna persona o institución.

Comúnmente realizan una búsqueda en Internet sobre una persona u organización para obtener información.

La ingeniería social y el *dumpster diving* o buceo en el basurero, también se consideran métodos de recopilación de información pasiva.

Sniffing u Olfateando, es otro medio de reconocimiento pasivo de la red y puede producir útil información como rangos de direcciones IP (*Internet Protocol*), convenciones de nombres, servidores o redes ocultas, y otros servicios disponibles en el sistema o red. *Sniffing* es similar a estar monitoreando el flujo de red, un hacker puede monitorear el flujo de datos para ver a qué hora determinadas operaciones tienen lugar y hacia donde el tráfico se va. Muchas veces esto incluye nombres de usuario, contraseñas y otros datos sensibles.

2.8.2 Fase 2: Scanning (Exploración).

En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el *network mappers*, *port mappers*, *network scanners*, *port scanners*, y *vulnerability scanners*, y otras.

2.8.3 Fase 3: Gaining Access (Obtener acceso).

En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema o *Flaw Exploitation*⁷, descubiertos durante las fases de reconocimiento y exploración. Algunas de las técnicas que el atacante puede utilizar son ataques de *buffer overflow*, *denial of service (DoS)*, *distributed denial of service (DDoS)*, *password filtering* y *session hijacking*.

⁷ Es la técnica que explota una falla o vulnerabilidad detectada

2.8.4 Fase 4: Maintaining Access (Mantener el acceso).

Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades *backdoors*, *rootkits* y *troyanos*.

2.8.5 Fase 5: Covering Tracks (Borrar huellas).

Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del sistema de detección de intrusos (IDS).

2.9 Métodos utilizados para la ejecución de ataques

Los nuevos métodos de ataque han sido automatizados, por lo que, en muchos casos, solo es necesario tener un conocimiento técnico básico para realizarlos.

Los métodos de ataque descritos a continuación son algunos de los métodos utilizados por los atacantes y que pueden estar relacionadas entre sí, ya que el uso de un método permite apoyarse de otros métodos. Por ejemplo: después de *Crackear* o romper una clave de acceso, un intruso ingresa como usuario legítimo a una red para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente, el atacante puede adquirir derechos de ingreso a lugares que le permitan dejar un virus o instalar bombas lógicas para paralizar todo un sistema antes de huir.

2.9.1 Eavesdropping y Packet Sniffing

Cada día es más relevante el uso de métodos de interceptación pasiva de la información, mejor conocidas como *eavesdropping* o escuchar secretamente, que son utilizadas para perpetrar ataques a la seguridad informática.

Este puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden en forma remota o interceptando el tráfico de red.

La mayoría de las redes son vulnerables al *eavesdropping*, o interceptación pasiva sin modificación del tráfico de información que circula por ellas.

En Internet esto es realizado por *packet sniffers*, son programas que monitorean los paquetes direccionados a la computadora donde están instalados. El *sniffer* puede ser colocado tanto en una estación de trabajo conectada a la red, como a un enrutador o a un *Gateway*⁸ de internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

El principal objetivo del *eavesdropping* es capturar información sensible como: números de tarjetas de crédito y direcciones de correo electrónico entrantes y salientes.

Los ataques *eavesdropping* pueden servir a varios objetivos que incluyen fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema.

Las herramientas utilizadas en *eavesdropping* son:

- Windows: Netstumbler, Airopeek, AirLine, Wireshark
- GNU/Linux: AirSnort, Kismet, AirTraf
- O. MAC: iStumbler, KisMAC, MacStumbler
- PocketPC: Ministumbler

2.9.2 Snooping y Downloading

Este método tienen el mismo objetivo que el *sniffer* obtener la información sin modificarla. Sin embargo los métodos son diferentes. En el *Snooping* o espionaje, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de email y a otra información almacenada en la computadora huésped, para luego *downloading* o descargarla a su propio servidor.

⁸ Nodo en una red informática que sirve de punto de acceso a otra red

El *snooping* puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.

Las herramientas utilizadas en *snooping* son:

- Windows: Cyber Snoop, Snooper

2.9.3 Tampering

Tampering o manipulación, hace referencia a la manipulación o modificación no autorizada de datos, y la alteración del software instalado, incluyendo el borrado de archivos.

Este método de ataque es particularmente serio cuando el que lo realiza ha obtenido derechos de administrador, con la capacidad de ejecutar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. Esta actividad puede ser ejecutada por *insiders* u *outsiders*, generalmente con propósitos de fraude o para dejar fuera de servicio a un competidor.

Ejemplos de casos incluyen la creación de cuentas para sustraer fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes o contribuyentes fiscales que pagan para que se les anule la deuda de impuestos. Otros ataques incluyen sitios web cuyas páginas han sido alteradas con imágenes terroristas o humorísticas, o la incorporación de virus y troyanos en aplicaciones y software de las organizaciones.

2.9.4 Spoofing y Looping

Este método se utiliza para actuar en nombre de otros usuarios, usualmente para realizar tareas de *snoofing* o *tampering*. Una forma común de *spoofing* o suplantación de identidad, es conseguir el nombre y clave de un usuario legítimo para, una vez dentro de su cuenta, tomar acciones en nombre de él, como puede ser el envío de emails falsos.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado *looping*, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país.

Rastrear el *looping* es casi imposible, ya que el investigador debe contar con la colaboración del administrador de cada red utilizada en la ruta, y pueden estar en distintas jurisdicciones y países. Los protocolos de red también son vulnerables al *spoofing*.

Las herramientas utilizadas en *spoofing* son:

- Windows: IP Spoofing
- Windows: DNS Spoofing
- Windows: Web Spoofing

Con el *IP Spoofing*, el atacante genera paquetes de Internet con una dirección de red falsa en el campo *from*, pero que es aceptada por el destinatario del paquete

Con el *DNS Spoofing*, este ataque se consigue mediante la manipulación de paquetes *UDP* (intercambio de datagramas), pudiéndose comprometer el servidor de nombres de dominios *DNS* o *Domain Name Server*.

Con el *Web Spoofing* el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las contraseñas, números de tarjeta de créditos.

2.9.5 Jamming o Flooding

Este método desactiva o satura los recursos del sistema, usualmente para realizar tareas de *jamming* o interferencia u *flooding* o inundación, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red para que nadie más pueda utilizarla.

Proveedores de Internet han sufrido bajas temporales del servicio debido a que han sufrido ataques a los protocolos *TCP/IP*⁹. Con este método, el atacante satura el sistema con mensajes que solicitan establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP ósea este ataque involucra *spoofing*. El sistema responde al mensaje, pero como no recibe respuesta y acumula *buffer* o espacio en memoria con información de las conexiones abiertas, no dejando espacio a las conexiones legítimas.

2.10 Herramientas para descubrimiento de vulnerabilidades

Es importante destacar que una herramienta que es utilizada para la protección, también puede ser utilizada por personas externas para la realización de ataques el conocimiento de las misma sirven para prevenir y mitigar dichos ataques.

2.10.1 Actividad en Internet

Herramientas más utilizadas para el monitoreo en tiempo real de los registros, sucesos, servicios, procesos, así como los datos de configuración del sistema aplicaciones específicas, los registros de vigilancia y detección.

- Internet Manager
- Internet Risk Management
- Net Focus
- System Activity Manager
- Web Spy

2.10.2 Análisis de Red

Herramientas más utilizadas para el monitoreo de la red, mediante la detección de fallos en tiempo real, permiten conocer el consumo de ancho de banda, el recuento de paquetes, errores de red y peticiones entre direcciones IP.

- NT Manager
- NTRama
- Sentinel Software Security
- Wireshark
- WebTrends Netware Management

⁹ Protocolo de control de transmisión/Protocolo de Internet

2.10.3 Anti Espionaje (Antispyware)

Herramientas más utilizadas para la detección, bloqueo y eliminación de programas espías, así como el monitoreo de la información que es enviada en tiempo real.

- Ad-Aware SE Personal
- Spyware
- Spybot - Search & Destroy
- Win pooch
- Spyware Blaster

2.10.4 Antispam

Herramientas más utilizadas para el filtrado y bloqueo de correo electrónico no deseado o spam (basura).

- Spam Buster
- Spam killer
- Spammer Slammer

2.10.5 Antivirus

Herramientas más utilizadas para prevenir o evitar la activación de los virus, así como su propagación y contagio.

- MacAfee Virus Scan
- AVG
- Avira
- Kaspersky Anti-Virus
- Norton Antivirus

2.10.6 Bloqueo y Restricción

Herramientas más utilizadas que permiten el bloqueo a ciertos programas como a juegos, *Messenger*, así como monitorizar y detectar los períodos de actividad no productiva.

- Absolute Security
- Desktop Locker
- Mind Soft Guardianship y Mind soft Restrictor
- System Security

2.10.7 Contraseñas

Herramientas más utilizadas que permiten la creación de contraseñas seguras y difíciles de conseguir, así como la administración de las mismas.

- Password Generator
- Password Guardian
- Password Power
- Password Tracker
- Random Password Generator

2.10.8 Detectores de Agujeros de Seguridad

Herramientas más utilizadas que permiten el escaneo de red, de aplicativos y gestión de parches, principal responsable de agujeros de seguridad.

- Check Point Real Secure
- Lan Guard Network Scanner
- Lucent Real Secure
- Secure Net Pro Software
- Web Trends Security Analyzer

2.10.9 Encriptación de Comunicaciones

Herramientas más utilizadas que permiten el cifrado de redes para el intercambio de datos, cifrado de información interna para evita el robo de identidad, protección de datos enviados por internet.

- F-Secure VPN
- Guardian PRO VPN
- Krypto Guard LAN and VPN
- Safeguard VPN
- VPNWare System

2.10.10 Firewalls

Herramientas más utilizadas que permiten o bloquean las transmisiones dentro de una red, así como para evitar que intrusos puedan acceder a información confidencial.

- Checkpoint
- Guardian PRO Firewall
- Hack Tracer
- Norton Personal Firewall
- Zone Alarm Pro

2.10.11 Gestión de Accesos

Herramientas más utilizadas que permiten la autenticación de los usuarios que interactúan con aplicaciones y con información de misión crítica.

- Palladium Secure Remote Access
- RSA SecurID
- SafeGuard Easy

2.10.12 Recuperación de Datos

Herramientas más utilizadas que permiten la recuperación de datos, ya sea por pérdida o para análisis forense de los mismos.

- Encase Tableu
- Easy Recovery
- Lost & Found
- Picture Taker Personal Edition
- System Snapshot

2.10.13 Seguridad en Comercio Electrónico

Herramientas más utilizadas que permiten el envío de información personal a través de internet mediante el uso de certificados de seguridad.

- Commerce Protector
- Crypto Swift
- ETrust
- NetSecure
- RSA Keon

Capítulo 3 Arquitectura de Seguridad de la Información

3.1 Introducción

En este capítulo se presenta la estructura en la que se desarrollan los sistemas de información en la dependencia actualmente, la cual permite poder minimizar el impacto de las vulnerabilidades que pudieran ser explotadas por los diferentes atacantes. Se inicia con describir el ámbito de la Arquitectura Empresarial (EA por sus siglas en inglés), reforzándose con la implementación de procedimientos de seguridad formando la Arquitectura de Seguridad de la Información (ISA por sus siglas en inglés) y apoyándose en estándares de Seguridad de la Información (SI por sus siglas en inglés). Por último se realiza una integración entre los conceptos anteriores para formar la Arquitectura de Seguridad de la Información Empresarial (EISA por sus siglas en inglés).

(Fehskens, 2008), define la arquitectura como "las propiedades de una cosa y su entorno que son necesarias y suficientes para que sea apto para el propósito para su misión". En su opinión, la arquitectura debe centrarse en lo esencial, sobre "las cosas que importan". Una arquitectura diferente implica una misión diferente, mientras que diferentes diseños pueden dirigirse a la misma misión.

La arquitectura de un sistema es un diseño estructural, integrado; sus elementos y definiciones dependen de los requerimientos proporcionados. Una estrategia de seguridad de la información debe apoyarse en un diseño que combine una infraestructura propia de seguridad y un esquema de servicios adecuado, que permita el cumplimiento en el manejo de la información.

Una estrategia de operación involucra la definición de un modelo a la medida que permitan cubrir la mayor parte de las necesidades de la organización, en la cual se puede tener una infraestructura básica de seguridad de la información con una inversión propia y complementarla con un servicio de protección de datos y de monitoreo que correlacione todos los eventos de seguridad.

3.1.1 EA (Enterprise Architecture o Arquitectura Empresarial)

El campo de la Arquitectura Empresarial o EA, básicamente se inició en 1987, con la publicación en el Diario de sistemas de IBM de un artículo titulado "Un marco para la Arquitectura de Sistemas de Información ", por Jhon A. Zachman. En ese documento, estableció tanto el reto y la visión de las arquitecturas empresariales que guían el campo para los próximos años. El reto consistía en gestionar la complejidad de los sistemas cada vez más distribuido.

(Zachman, 1987), dijo "El costo y el éxito de la organización reside en función cada vez más en sus sistemas de información que requieren un enfoque disciplinado para la gestión de esos sistemas."

La administración de las grandes organizaciones en relación a su sistema de información, es difícil; ya que dicho sistema cuenta con un conjunto de procesos que operan sobre una gran colección de datos estructurados que dependen en gran medida a las necesidades de la organización. Se recopila, elabora y distribuye la información, necesaria para las operaciones diarias de la organización y que son necesarias para las actividades de dirección, control y toma de decisiones en la organización.

Es por ello que la EA tiene como principal objetivo mejorar la eficacia o eficiencia de la propia organización. Mediante innovaciones en la estructura de la organización, la centralización o la diversificación de los procesos de negocio, la calidad, la oportunidad comercial y la mejora continua en los proceso de Tecnologías de la Información (TI).

3.1.2 ISA (Information Security Architecture o Arquitectura de Seguridad de la Información)

La arquitectura de seguridad de la información (ISA) es una parte integral de la EA en la organización. Esta representa la parte específicamente direccionada al sistema de información y al suministro de la estructura de la información para la implementación de los diferentes niveles de seguridad.

(Killmeyer, 2001), define a la ISA como el ámbito de la protección de datos, de carácter personal, así como la implementación de códigos de buenas prácticas o recomendaciones sobre gestión de la seguridad de la información y de certificaciones internacionales, éstas últimas, relacionadas con la auditoría de los sistemas de información.

El propósito principal de la ISA es asegurar que la misión de los procesos de negocio impulsados por los requisitos de seguridad de la información sea consistente, rentable y que los sistemas operen en equilibrio con la gestión de riesgos de la organización.

Tiene como objetivos:

- Apoyar, permitir y ampliar las políticas de seguridad, proporcionando seguridad orientada a la toma de decisiones. El resultado será estratégicamente alineado y coherente en toda la organización
- Proporciona seguridad relacionada con la aplicación de TI, así como los lineamientos en el diseño de la tecnología, sistemas y aplicaciones
- Reforzamiento de los eslabones más débiles de la organización y promover la coherencia
- Aplicabilidad en todo lo relacionado a la legislación y los requisitos reglamentarios existentes

En última instancia, la ISA proporciona una guía detallada que permite el seguimiento de los objetivos de mayor nivel y objetivos estratégicos de las organizaciones, a través de las necesidades específicas de protección de la misión, negocio, soluciones específicas de seguridad de la información proporcionada por las personas, procesos y tecnologías.

3.1.3 SI (Security Information o Seguridad de la Información)

Consejo Nacional de Investigación, Gobierno de EE.UU. (2002), “La Seguridad de la Información es la protección de la información y sistemas de información del acceso, uso, divulgación, alteración, modificación o destrucción con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información utilizada en una organización”. Dependiendo del entorno de la organización, se pueden tener diferentes amenazas que comprometan a los objetivos previamente mencionados

“La SI como concepto es muy amplio, generalmente, se basa en normas que pueden proporcionar un componente importante en el entorno de seguridad de la información pero no se debe confiar a ciegas.” (Mercurio, 2003),

Varias de las fuentes tienen diferentes puntos de vista, por ejemplo:

- Algunos se centran en la gestión de la seguridad (por ejemplo, ISO 1997, ISO 2000),
- Algunos se centran en los aspectos de seguridad para los procesos (por ejemplo, ITGI (*IT Governance Institute*) 2000 y 2004, e ITIL 2004),
- Algunos aspectos específicos de seguridad (por ejemplo, NIST (*National Institute of Standards and Technology*) 1995, ISO 1996, y SEI (*Software Engineering Institute*), 2003).

3.2 EISA (Enterprise Information Security Architecture o Arquitectura de Seguridad de la Información Empresarial)

La EISA es el proceso de instituir una solución de seguridad de la información integral en la organización, que permita apoyar la seguridad en cada punto de la arquitectura, para que se alineen con las metas comunes y la dirección estratégica.

El término EISA se le atribuye a (Gartner¹⁰ 2006). *Gartner* trata de reunir tres componentes indispensables que son: los dueños del negocio, los especialistas de la información y los implementadores de la tecnología.

Si usted puede tener estos tres grupos juntos y unirlos detrás de una visión común que impulse el valor del negocio, usted ha tenido éxito, si no, ha fracasado. El éxito se mide en términos prácticos, como manejar la rentabilidad, no por la comprobación de los elementos de una matriz de proceso (Gartner, 2006).

La EISA es considerada como una herramienta que une la misión de negocio y la estrategia de TI de una organización. Vincula la estrategia de inversiones en TI, permitiendo asegurar una estrecha integración entre el negocio, las aplicaciones, la información, y las capas de la arquitectura de infraestructura. Involucra el desarrollo de una visión arquitectónica y la proyección del negocio hacia una meta u objetivo.

Una vez que esta visión se entiende bien, un conjunto de pasos intermedios se crean para ejemplificar el proceso de cambio en relación a la situación actual.

La EISA define un esquema de acción estratégico en la organización, mediante el cual se establecen las directrices a nivel de seguridad de la información que se proyecta implementar en cada uno de los procesos de negocio.

¹⁰ Empresa mundial de consultoría dedicada a la innovación e investigación de TI

3.2.1 Objetivo de la EISA

El objetivo de la EISA es poder garantizar la integridad, confidencialidad, disponibilidad y privacidad de la información que se maneja y procesa en la organización, así como una operación con un nivel de riesgo aceptable derivada del uso de las TI asegurando la tranquilidad de directivos, funcionarios, clientes y socios de negocio.

Para cumplir con los objetivos se prevé el uso e implementación de métricas que permitan obtener un panorama general relacionado con el cumplimiento de los siguientes propósitos:

- Permitir la evaluación de la seguridad y el riesgo en la organización.
- Evaluar la situación actual de la seguridad de la información empresarial.
- Evaluación de los activos de información.
- Evaluación de los riesgos asociados con la implementación de nuevas tecnologías.
- Permitir la alineación del negocio hacia la seguridad
- Proporcionar una estructura, coherencia y cohesión con los procesos de negocio
- Asegurar que todos los modelos e implementaciones puedan ser diseñados hacia la estrategia de seguridad
- Establecer un lenguaje común para la seguridad de la información dentro de la organización
- Establecer procesos de mejora continua
- Establecer métricas de desempeño por cada área.

El cumplimiento de dichos propósitos sirve de base para que la EISA se ajuste a las cambiantes necesidades tecnológicas, permitiendo responder a las nuevas amenazas y peligros. A manera de identificar los elementos y componentes requeridos para definir, normar, implantar, monitorear y auditar los requerimientos necesarios de seguridad.

La práctica de la EISA, conlleva el uso de modelos conceptuales que detallan las organizaciones, los roles, las entidades y las relaciones que existen o deberían existir para llevar a cabo los procesos de negocio.

El producto final es una serie de modelos que describen en varios grados de detalle la operación actual del negocio y la identificación de los controles de seguridad que serán requeridos.

Dichos modelos, sirven de base para la toman de decisiones informadas sobre dónde invertir recursos, hacia dónde reorientar las metas organizacionales, los procesos, y las políticas en función del negocio.

3.2.2 Implementación de la EISA

Para implementar la EISA, generalmente se inicia documentando la estrategia de la organización. El proceso continua con la documentación de los procesos internos de negocio, y la forma en que la organización interactúa consigo misma y con sus clientes, proveedores, y otras entidades gubernamentales.

Habiendo documentado la estrategia y estructura de la organización, el proceso de la arquitectura se enfoca en los componentes tecnológicos tales como:

- Cuadros de organización, actividades, y flujo de procesos sobre cómo la *TI* de la organización opera
- Ciclos, periodos y distribución en el tiempo de la organización
- Proveedores de tecnología hardware, software y servicios
- Inventarios y diagramas de aplicaciones y software
- Interfaces entre aplicaciones (eventos, mensajes y flujo de datos)
- Intranet, Extranet, Internet, *e-commerce* (Comercio Electrónico)
- Clasificación de datos, bases de datos y modelos de datos soportados
- Hardware, plataformas, *hosting* (hospedaje web), servidores, componentes de red y dispositivos de seguridad

- Diagramación de los Niveles o Capas de seguridad de la organización
- Monitoreo y control de Accesos
- Redes de área local y abiertas, diagramas de conectividad a internet
- Sistemas de gestión para el tratamiento de la información interna.

La EISA, documentará el estado actual de los componentes técnicos de seguridad listados arriba, así como un estado ideal futuro deseado y finalmente un estado meta futuro resultado de los sacrificios y compromisos de ingeniería frente al ideal. Esencialmente el resultado es un conjunto de modelos anidados e interrelacionados.

Las dependencias de las TI se han apoyado con el concepto ITIL ya que contiene una serie de procesos para las mejores prácticas en el manejo de la información y mejora continua de los mismos.

Junto con los modelos y diagramas se debe implementar un conjunto de mejores prácticas dirigidas a la adaptabilidad de la seguridad, escalabilidad y manejabilidad de los procesos. Estas mejores prácticas de sistemas de ingeniería no son únicas a la EISA, pero son esenciales para su éxito.

La aplicación exitosa de la EISA, requiere una integración adecuada en la organización, ya que al tener todos los componentes técnicos documentados estos servirán de base para el crecimiento hacia las nuevas tecnologías requeridas por la organización a implementar.

3.2.3 Transición de la organización implementando la EISA

La organización debe diseñar e implementar un proceso que asegure el movimiento continuo desde el estado actual al estado futuro. Para poder llegar a un estado futuro será mediante la realización de uno o los dos procesos siguientes:

- Disminución de la distancia presente entre la estrategia actual de la organización y apoyar la capacidad para dimensionar la evolución sobre seguridad en TI.
- Mejoras y sustituciones necesarias que deben hacerse sobre la arquitectura de seguridad de TI basadas en la factibilidad de proveedores del hardware y software, los requerimientos regulatorios conocidos o anticipados, y otros aspectos para la gestión funcional de la organización.

La EISA prevé convertirse en una práctica habitual dentro de las organizaciones, ya que las políticas de seguridad que se implementan son las líneas maestras de dicho contexto empresarial. La arquitectura que se obtiene es una combinación funcional de los procesos y la tecnología para alcanzar la meta de negocio. La EISA permite lograr la seguridad, y prestar asistencia jurídica y cumplimiento normativo.

El propósito fundamental de implantar una EISA, es para asegurar que la estrategia de negocio y la seguridad de las tecnologías de la información están alineadas. Como tal, la EISA permite la trazabilidad desde la estrategia de negocio actual hasta la tecnología subyacente.

3.2.4 Relación de la EISA con otros marcos o frameworks

Enciclopedia libre Wikipedia (consultada en septiembre de 2011). Define como *framework* “a un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular, que sirve de referencia para enfrentar y resolver nuevos problemas de índole similar.”

Una serie de *framework* han sido desarrollados desde los orígenes de la EA en 1987 y que ha servido de base para la gestión de la complejidad de los sistemas cada vez más distribuidos.

Es por ello que la EISA, se apoya de otros *framework* de seguridad de los cuales retoma los aspectos encaminados a la SI y la gestión de los procesos de TI.

En la actualidad, en el campo de la arquitectura empresarial, existen varios métodos desarrollados por los gobiernos y otras instituciones de gran tamaño, entre los más reconocidos se encuentran los siguientes:

3.2.4.1 FEA (Federal Enterprise Architecture o Arquitectura Empresarial Federal)

La FEA es la arquitectura empresarial que proporciona una metodología común para la adquisición, uso y gestión de TI.

La FEA, es una iniciativa de los E. U. que tiene como objetivo cumplir con la Ley de Clinger-Cohen¹¹, al comprometer a las oficinas de Informática de las instituciones federales a promover el desarrollo y el mantenimiento de sistemas de TI integrados. Está diseñada para facilitar el intercambio de información y recursos a través de las agencias federales, reducir costos y mejorar los servicios en el uso de TI.

La FEA es una base de información de valor estratégico que detalla al negocio, la información necesaria para operar las tecnologías necesarias que sirvan de apoyo en sus operaciones y los procesos de transición para la aplicación de las nuevas tecnologías en respuesta a las necesidades cambiantes del negocio.

La FEA provee un conjunto de modelos de referencia diseñados para facilitar el análisis e identificación de las funciones de toda institución federal que permitan fortalecer la gestión de la función gubernamental.

¹¹ Clinger-Cohen (1996) "What is the Clinger-Cohen Act, and how does it affect people with disabilities?" AccessIT University of Washington Disponible en: <http://www.washington.edu/accessit/articles?104>.

3.2.4.2 DoDAF (Architecture Framework the U.S. Department of Defense o Marco de Arquitectura del Departamento de Defensa de los E. U.)

DoDAF es el marco de arquitectura para el departamento de defensa estadounidense que proporciona una orientación para el desarrollo de arquitecturas empresariales y operaciones de negocio. El DoDAF se divide en tres puntos de vista de negocio y estructura de tecnología de la información: operativa, sistemas y normas técnicas

El punto de vista operativa, se ocupa de describir las actividades, las capacidades, las organizaciones, los roles, y los datos necesarios para ejecutar las operaciones del Departamento de Defensa.

El punto de vista de sistemas, describe los componentes automatizados y los intercambios de información necesarios para aplicar el punto de vista operacional.

El punto de vista de normas técnicas, describe la infraestructura técnica que se debe poner en práctica para los puntos de vista operacionales y sistemas.

Los tres puntos de vista de arquitectura definen un conjunto de puntos de vista que actúan como mecanismos para visualizar, entender y asimilar el alcance y la complejidad de la arquitectura a mediante el apoyo de medios visuales o gráficos.

Es especialmente adecuado para sistemas de gran tamaño con la integración de los complejos retos de la interoperabilidad¹², detalla el funcionamiento del ambiente externo en el que el desarrollo del sistema va a operar.

¹² Habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada

3.2.4.3 MODAF (British Ministry of Defence Architecture Framework o Marco de Arquitectura del Ministerio de Defensa Británico)

El MODAF es un marco de arquitectura que define una forma estándar de organizar la EA, desarrollado originalmente para la adquisición de TI por el Ministerio de Defensa del Reino Unido.

MODAF define el marco en que el Ministerio de Defensa puede manifestar su nivel de organización, su flujo de procesos, sistemas y la forma en la que organiza su gente. Además, facilita la planificación de adquisiciones futuras de TI, para que los niveles de capacidad se puedan mantener o mejorarse mediante la presentación de la información necesaria para la toma de decisiones de planificación en un formato simple y fácil de entender.

El modelo establece una base firme para el, cumplimiento eficiente y oportuno de las tareas del proyecto requeridas para pronosticar con un mínimo riesgo

3.2.4.4 TOGAF (Architecture Framework The Open Group o Marco de Arquitectura de Open Group)

El TOGAF es un marco de EA que proporciona un enfoque para el diseño, planificación, implementación y gobernanza de la información. Esta arquitectura es modelada por lo general con cuatro niveles o dimensiones: negocios, tecnología, datos y aplicaciones. Cuenta con un conjunto de arquitecturas base que buscan facilitarle al equipo de arquitectos a definir el estado actual y futuro de la arquitectura.

Más conocido como ADM, sigla en inglés de "*Architecture Development Method*", es el método definido por TOGAF para el desarrollo de una arquitectura empresarial que cumpla con las necesidades de la empresa y de tecnología de la información de una organización. Puede ser ajustado y personalizado según las necesidades propias de la organización y una vez definido se utiliza para gestionar la ejecución de las actividades de desarrollo de la arquitectura.

3.2.5 Beneficios al implementar una EISA

Dentro de los beneficios a corto plazo que se esperan con la implementación de una EISA, es la de liderar e integrar de manera efectiva todos los asuntos relacionados con la arquitectura de negocio y de arquitectura tecnológica de TI en un ambiente institucional.

Los beneficios a la organización son:

- Lograr los objetivos estratégicos que dependen de recursos y capacidades de negocio asociadas con TI.
- Mejorar el desempeño del negocio al maximizar la eficiencia de TI a través de la organización.
- Incrementar la agilidad de la organización para identificar oportunidades y problemas potenciales, tomar decisiones y reaccionar rápidamente ante cambios.
- Establecer correctamente las prioridades de programas y proyectos, en cuanto a los requerimientos que rigen las soluciones basadas en TI.
- Vincular múltiples componentes asociados con TI, como lo son aplicaciones, sistemas, bases de datos y redes a través de la organización.
- Compartir eficientemente información entre líneas o unidades de negocio, así como con otras organizaciones.
- Integrar diversas aplicaciones y redes que carecían de estándares abiertos.
- Reducir los recursos duplicados de TI a través de la organización.
- Proteger integralmente los datos y activos críticos de información y de TI de acuerdo al nivel mínimo de riesgo aceptable para la organización.
- Asegurando inversiones de valor en TI.
- Mejorar la gestión del capital humano en áreas que requieren conocimiento y habilidades en TI, áreas tanto usuarias, como técnicas y operativas.

Capítulo 4. Herramientas de protección para la seguridad de la Información

En la actualidad, las dependencias de gobierno se han vuelto cada vez más dependientes de las TI. Hoy, prácticamente no hay usuario sin un equipo informático con acceso a la gran red ni organización que no utilice Internet como una parte importante para la administración de su negocio.

Por otro lado, si bien las herramientas para la seguridad han ido evolucionando notablemente en la seguridad del usuario, no existe una aplicación que brinde toda la protección frente a la amplia diversidad de problemas potenciales a los que se exponen las organizaciones cotidianamente al hacer uso de las tecnologías.

Bajo este escenario, las organizaciones necesitan contar con una amplia gama de herramientas que permitan cubrir la mayor cantidad de vulnerabilidades existentes en las organizaciones, ya que existen ciertos aspectos de la seguridad que resultan fundamentales para evitar que los sistemas, los usuarios internos, y las redes de trabajo en su conjunto, constituyan objetivos sumamente vulnerables frente a diferentes tipos de amenazas.

4.1 Herramientas Orientadas a la Seguridad Lógica

El uso de herramientas orientadas a la seguridad lógica son las soluciones más utilizadas en las organizaciones para la defensa de su red, basado en el establecimiento de recursos para el aseguramiento del perímetro externo de la red a diferentes niveles.

La seguridad lógica se basa en la protección de todo el sistema informático de una organización, es decir; poner una coraza que proteja los elementos sensibles de ser atacados dentro y fuera de un sistema informático.

Dentro de las herramientas esenciales para la seguridad lógica en las organizaciones se encuentran las siguientes.

4.1.1 Router o Enrutador

Es un sistema para la interconexión de redes informáticas que permite asegurar el enrutamiento o direccionamiento de paquetes entre las diferentes redes y también se encargan de resolver cual es la mejor ruta para el envío del paquete de datos.

Como herramienta de seguridad, algunos enrutadores proporcionan un complemento más a la seguridad, ya que permiten la asignación de direcciones NAT (*Network Address Translation* o Traducción de Dirección de Red), que resulta en transformar una dirección IP pública en varias direcciones IP privadas, de tal forma que resulta difícil para los intrusos detectar la dirección IP de alguna computadora detrás de un *router*, ver figura 13.

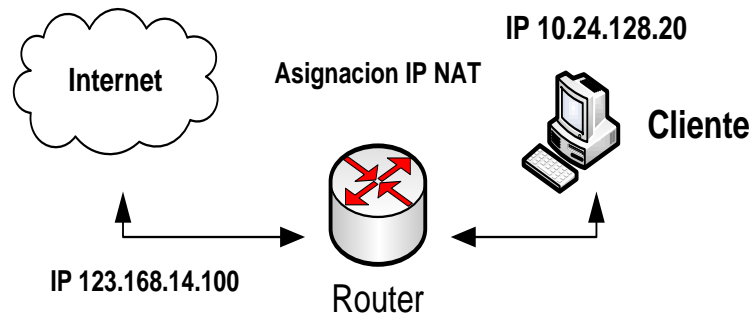


Figura 13 Router o Enrutador

4.1.2 Firewall o Cortafuego

Es un sistema de defensa ubicado entre dos redes y que sirve como un filtro para permitir o bloquear el acceso a un servicio, dependiendo de reglas previamente establecidas. Consta de un dispositivo o conjunto de dispositivos de software o de hardware configurados para prevenir accesos no deseados a una red como primer punto de contención.

El cortafuego funciona definiendo una serie de permisos para la comunicación, tanto de entrada como de salida, mediante reglas. Estas reglas se pueden hacer teniendo en cuenta los puertos de comunicación, los programas o las *IP* de conexión.

Las reglas pueden ser tanto restrictivas como permisivas, es decir, pueden ser reglas que denieguen o autoricen las comunicaciones de entrada, de salida o ambas a un determinado puerto, ver figura 14.

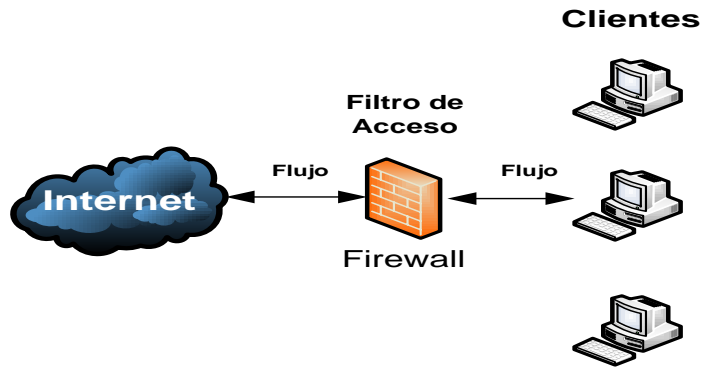


Figura 14 Firewall o Cortafuego

4.1.3 IPS (Intrusion Prevention System o Sistema de Prevención de Intrusiones)

Son sistemas de seguridad de red que monitorean, analizan y controlan el acceso de los usuarios a las actividades de la red en relación a actividades maliciosas.

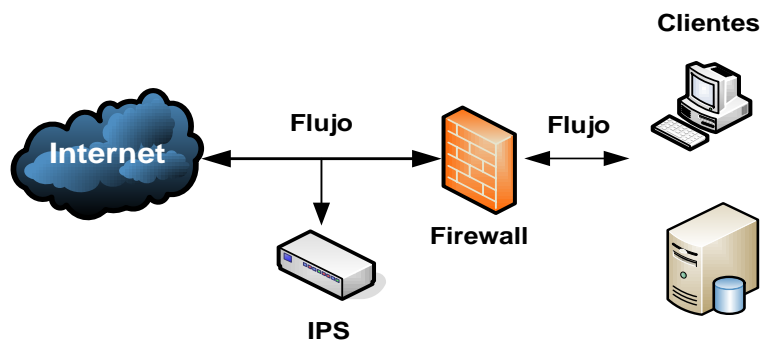


Figura 15 IPS o Sistema de Prevención de Intrusiones

A diferencia de los Firewall, los IPS comparan el tráfico contra una base de datos con registros de intrusiones, puede ser configurado para que no permita el paso de los paquetes y también que tome ciertas acciones específicas. Es decir, funciona evitando tráfico de ciertas direcciones como prevención y primer punto de contención. Generalmente se pone antes de un firewall, para aumentar la seguridad de los equipos, ver figura 15.

Los IPS se categorizan según el modo en el que detectan el tráfico malicioso:

- Basado en Firmas: compara el tráfico que fluye en la red con firmas de ataques conocidos, debiendo tener la lista de firmas actualizada.
- Basado en Políticas: se definen políticas de seguridad estrictas, si el tráfico está permitido el IPS permite el tráfico, si no lo está lo bloquea.

Los IPS buscan anomalías o comportamientos anómalos en la red, comprueban, monitorean la actividad del sistema de archivos, buscan *rootkits*¹³ en el sistema y demás.

4.1.4 IDS (Intrusion detection system o Sistema de Detección de Intrusiones)

Es un sistema de seguridad que se encarga de identificar posibles violaciones de seguridad o mal uso de recursos, hace un análisis en tiempo real del tráfico en la red mediante el uso de librerías de registros o firmas.

Cuando encuentra una anomalía o uso no autorizado solo genera alertas. Generalmente se pone después de un firewall, para evitar falsos positivos o coincidencias que no representan una amenaza, ver figura 16.

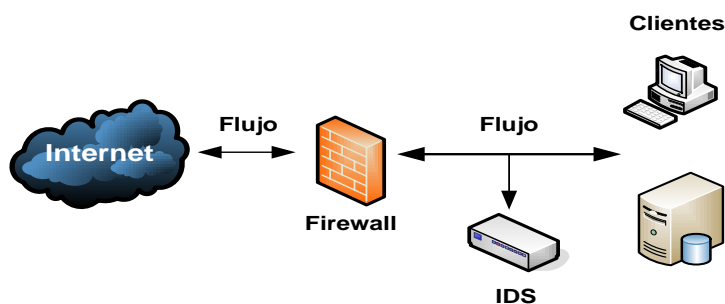


Figura 16 IDS o Sistema de Detección de Intrusiones

El IDS por sí mismo no está diseñado para capturar y responder a las violaciones de la seguridad, pero si a notificar mediante alertas si se produce un evento.

¹³ SearchMidmarketSecurity "Definition rootkit" Disponible en: <http://searchmidmarketsecurity.techtarget.com/definition/rootkit>.

4.1.5 VPN (Virtual Private Network o Red Privada Virtual)

Es un sistema de seguridad que posibilita la comunicación desde cualquier punto entre dos equipos mediante Internet por medio de una conexión cifrada segura.

Las VPN hacen uso de una tecnología denominada *tunneling* o túnel a la hora de establecer la comunicación entre los dos equipos, es decir crea un túnel por el que circulan todos los datos desde un extremo a otro pero de manera cifrada por lo que resulta difícil descifrar dicha información en caso de ser interceptada, ver figura 17.

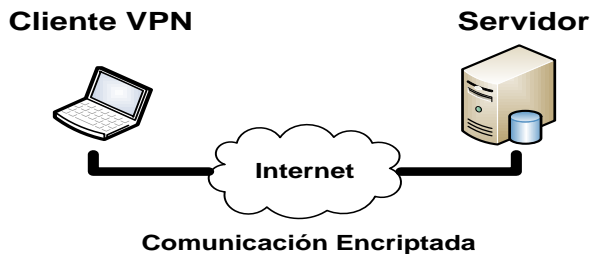


Figura 17 VPN o Red Privada Virtual

4.1.6 Proxy

Son sistemas de seguridad de red que permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el Proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial, ver figura 18.

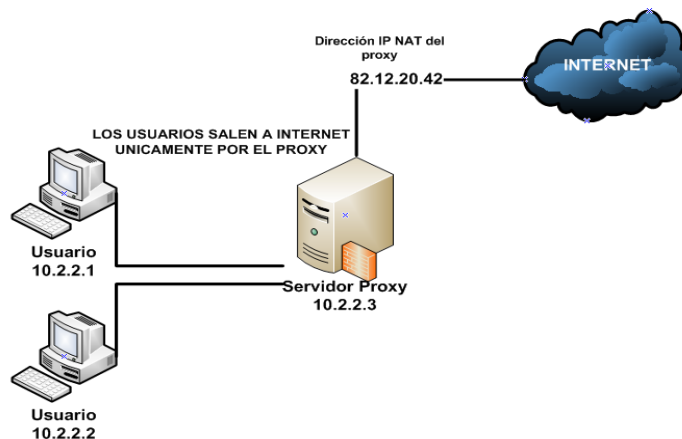


Figura 18 Servidor Proxy

4.1.7 DLP (Data Loss Prevention o Prevención de Pérdida de Datos)

El término DLP, surge de la necesidad que presentan las organizaciones para proteger su información sensible con la fuga de datos existentes. Así como los productos de seguridad como los firewalls, IPS e IDS, entre otros, la tecnología de DLP han ido mejorando considerablemente y empieza a influenciar la industria de la seguridad.

(Securosis, 2009), define el término DLP como "Productos que, basados en políticas centrales, identifican, monitorean, y protegen datos en reposo, en movimiento, y en uso, a través de un profundo análisis de contenido."

4.1.7.1 Funcionalidad de DLP

De acuerdo con (Kanagasingham, 2008) "La función de un DLP es la de identificar, monitorear, detectar e intentar prevenir la fuga de información o uso no autorizado de la misma. Apoyándose de herramientas que cuenten con una gestión centralizada para permitir el monitoreo y control de los datos en el puesto de trabajo".

Las tecnologías DLP protegen datos sensibles y proveen información acerca del uso de contenidos dentro de la organización, ayudan a los administradores a entender mejor su información y mejorar su habilidad de clasificar y manejar contenidos.

La meta de DLP es la protección de la información a través de todo su ciclo de vida y cumplir con los lineamientos establecidos para el manejo de información sensible.

4.1.7.2 Características de DLP

En el artículo publicado por Securosis¹⁴ “Understanding and Selecting a DLP solution Websense” menciona que “Los DLP ayudan a las organizaciones a comprender mejor sus datos y mejorar su capacidad para clasificar y administrar el contenido; también ayudan a proteger los datos sensibles y proporcionar información sobre el uso de los contenidos dentro de la empresa.”

Las características más marcadas de DLP son:

- Profundo análisis de contenido: Es la capacidad que tienen los productos para analizar la información a profundidad.
- Gestión de políticas centrales: Administración de los diferentes puntos de detección, creación y gestión de las políticas, flujos de trabajo y presentación de informes.
- Reducir la propagación de datos confidenciales en los centros de datos de las organizaciones, oficinas remotas y equipos de usuarios finales.
- Supervisar, monitorear y proteger las comunicaciones con contenido confidencial a sitios web públicos.
- Definición e implementación de políticas universales en la organización.

Es conveniente resaltar que las herramientas mencionadas en este punto ofrecen una excelente protección contra las amenazas de la red, mas sin en cambio hay ciertas amenazas que combinan varios escenarios, por lo que las organizaciones deben apoyarse de otras formas de protegerse como las que son generadas por usuarios internos que pretendan robar datos, hacer daño al hardware y software, o la modificación de programas propios de la organización; es por ello que las amenazas desde adentro requieren de medidas de seguridad internas.

¹⁴ Securosis, empresa de consultoría para la investigación de seguridad de la información, dedicada a la mejora de la práctica de la seguridad de la Información. Disponible en <https://securosis.com/>

4.2 Análisis de Riesgo en la implementación de nuevas tecnologías.

Como se mencionó anteriormente, cualquier organización se encuentra sometida a amenazas o peligros de diversos orígenes, desde atacantes externos que desean apoderarse de la información de la organización, hasta usuarios internos que buscan obtener algún beneficio de la información con la que trabajan a diario.

Es por ello que las organizaciones pueden estar o no correctamente preparadas para enfrentar los peligros o amenazas latentes. Este aspecto es el que se denomina como vulnerabilidad y representa las debilidades que la organización presenta frente a cada una de las eventuales amenazas.

Se debe de entender como amenaza al conjunto de los peligros a los que están expuestos los sistemas de información y sus recursos tecnológicos relacionados, los que pueden ser de tipo:

- Accidental: es decir que no existe un deliberado intento de perjudicar a la organización.
- Intencional: su móvil es perjudicar a la organización u obtener beneficios en favor de quien comete la acción.

Es por ello que para prevenir la materialización de las posibles amenazas es recomendable la aplicación de controles.

Se debe de entender como control a las herramientas, políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar que los objetivos de la institución serán entendidos y alcanzados, para que eventos no deseables sean prevenidos, detectados y corregidos.

Los controles relacionados a la seguridad de la Información se establecen para impedir el acceso físico y lógico a los sistemas de información y sus recursos relacionados por parte de personas que no tienen autorización, como también ayuda a reducir el riesgo de que las personas autorizadas cambien o destruyan accidentalmente los datos.

En el proceso de implementar nuevas tecnologías ha sido y será un tema de difícil manejo ya que cuando se planea poner en práctica, esta debe contar con una serie de esquemas que permitan saber: cuál es la postura de los diferentes actores que intervienen en dicho proceso, estimar el costo-beneficio de la implementación y tener identificado en cada proceso cualquier cambio no planeado que pudiera representar un riesgo, llámese: financiero, humano, tecnológico y de seguridad.

Es por ello que para evitar riesgos en la implementación de nuevas tecnologías es recomendable seguir los siguientes pasos:

- Contar con un prototipo de la Implementación
- Establecer los alcances así como sus limitantes
- Análisis del Costo-Beneficio de la implementación
- Desarrollo de la estrategia paso a paso
- Contar con ambiente de pruebas
- Contar con un plan de recuperación
- Establecimiento de controles de mejora continua

Capítulo 5. La Pérdida de Datos en las Organizaciones

Hoy en día, prácticamente cualquiera puede compartir un volumen ilimitado de información, acceder a él y modificarlo. Como consecuencia, prevenir la pérdida de información confidencial se torna más difícil que nunca para las organizaciones.

Los enfoques del pasado en materia de seguridad apuntaban a proteger la red, en la actualidad la prioridad es la de proteger la información en sí.

En el presente capítulo se habla acerca de la pérdida de datos en las organizaciones, así como el riesgo que resulta de la fuga de la misma.

5.1 Principales puntos de Fuga de la Información

(Calvo, 2009), comenta que “existen diferentes amenazas y vulnerabilidades que pueden llevar a la fuga de la información, a continuación se describen algunas de ellas.”

- Redes sociales. Sitios como *Facebook*, *Hi5*, *Twitter* y *Badoo*, entre otros. representan un riesgo para la pérdida de confidencialidad de la información, ya que en algunas ocasiones los usuarios publican información interna de la organización.
- Publicación de videos. Las organizaciones realizan actividades al interior de sus instalaciones que son grabadas, en algunas ocasiones estas grabaciones son subidas a páginas como *YouTube* sin tener en cuenta la información que puede ser revelada, como el nombre de áreas de acceso restringido, controles de seguridad existentes, nombres y cargos de empleados de la organización, lo que puede poner en evidencia información que sólo es relevante para la organización.

- Robo de dispositivos móviles. La información almacenada en estos dispositivos en la mayoría de las ocasiones transita dentro y fuera de la organización sin ningún mecanismo de protección, lo que puede ocasionar que personas ajenas puedan tener acceso a información de carácter confidencial o sensible.
- Falta o inadecuada clasificación de activos de información. El hecho que las organizaciones no cuenten con una adecuada clasificación de activos de información, conlleva a que los empleados no tengan claro cuál es el nivel de protección de cada activo, lo que dificulta la protección de los mismos.
- Falta de sensibilización a los usuarios. Los empleados no están involucrados con los aspectos de seguridad de la información, por lo que no saben como actuar cuando se enfrentan ante un evento que pueda afectar la seguridad.
- Falta de acuerdos de confidencialidad. Las organizaciones hoy en día tienen diversos proveedores y empleados que llegan a conocer información del funcionamiento de la misma, como: información de clientes internos y externos, planes estratégicos, proyectos futuros y proyectos en ejecución, entre otros, la cual en algunos casos debe ser mantenida bajo reserva aún con los mismos empleados.

5.2 Factores de fuga y pérdida de información

Una encuesta realizada por el Instituto *Ponemon*¹⁵, revela que el 85% de las empresas encuestada había experimentado alguna forma de pérdida de datos, la mayoría de los incidentes se produjeron en el interior de la organización, mientras que sólo el 6% de una actividad criminal y el 16% por empleados inconformes, el otro 42% fue causado por el extravió de dispositivos.

¹⁵ Ponemon Institute lleva a cabo investigaciones independientes sobre la privacidad, la protección de datos y la política de seguridad de la información. Disponible en <http://www.ponemon.org/index.php>

Otras causas fueron la negligencia de los empleados con un 16% y 10% restante por infecciones de terceros respectivamente.

En algunas ocasiones se habla sobre los controles de seguridad implementados en la organización para prevenir la fuga de información de posibles empleados deshonestos, de esta falla de comunicación se deriva en vulnerabilidades que luego permiten que personas no autorizadas o las autorizadas pero sin controles suficientes, logren apoderarse de información confidencial, contenido de correos, contraseñas que circulan en la red interna, diagramas de la red interna, base de datos de clientes y proyectos secretos, entre otros; mismos que al ser revelados pueden provocar a la organización grandes pérdidas, llámense financieras y de prestigio que la pueden llevar a la quiebra.

En relación a los incidentes nombrados anteriormente puede adjudicarse a debilidades y errores humanos, pero esperar que todos los empleados tengan un correcto entendimiento de la seguridad de la información no es una estrategia de defensa viable. Quizás lo fue hace una década, pero no en la actualidad. Todos estos incidentes hubieran podido evitarse con la implementación de buenos sistemas de seguridad de TI que aplican de manera proactiva las políticas de seguridad de una organización, que son revisadas en todos los niveles en forma regular. Estos sistemas están disponibles actualmente en compañías especializadas.

Un sistema de prevención de la pérdida de datos probablemente hubiera detectado la actividad inusual en la estación de trabajo en forma regular, permitiendo actuar e investigar en forma oportuna el incidente.

No existe un remedio milagroso para la seguridad, pero con un enfoque holístico que abarque todo el sistema y revise las políticas de seguridad y los sistemas de implementación, cualquier error menor puede ser detectado y remediado antes de que se convierta en un problema mayor para la organización involucrada.

Capítulo 6. Análisis de Tecnologías sobre Prevención de Pérdida de Datos en la SSP

En el año de 2008, la Coordinación General de la Plataforma México, propone al Ejecutivo (Presidente Calderón), la creación del Sistema de la Plataforma México con el propósito de integrar todas las tecnologías de la información y ponerlas accesibles a todo el personal de la seguridad pública, con la finalidad de que cuente con todos los elementos de información para el combate al delito.

Para este escenario la Secretaría de la Seguridad Pública, a través de la Coordinación General de la Plataforma México, requiere la adquisición de tecnologías para el fortalecimiento de la operación del Sistema de Plataforma México, que incluya la instalación, configuración y puesta a punto de las herramientas necesarias para la protección de la información durante todo su ciclo de vida, en cualquier ámbito, ya sea interna o externamente.

La SSP, busca implementar sistemas de información de alta tecnología, esto deriva en inversiones tecnológicas de seguridad informática que le permita controlar las posibles debilidades identificadas y como reforzamiento a sus políticas de seguridad; mas sin embargo, al momento de realizar dicho análisis se presentan varias incógnitas, como son la gran variedad de alternativas existentes en el mercado sobre seguridad informática, los modelos de evaluación no resuelven en su totalidad la necesidad que se desea cubrir, los proveedores de servicios no cuentan con la capacidad para cubrir dicha necesidad y el costo de la implementación sobrepasa a lo presupuestado.

En este capítulo, se ofrece un análisis que permita la integral protección de la información dentro y hacia afuera de la SSP, mediante el uso de soluciones de seguridad que permitan proteger los recursos de información sensible tales como: Información a directores, contratos, proyectos futuros, configuraciones de equipos, contraseñas de acceso, entre otra, así como la información de uso diario generada por lo usuarios internos.

6.1 Descripción General del Análisis

Se realiza la propuesta de análisis de seguridad sobre soluciones orientadas a la prevención de pérdida de datos en las dependencias de gobierno, y como caso especial la SSP.

En el análisis desarrollado en este capítulo, se presenta la siguiente propuesta de análisis sobre proveedores de seguridad para la prevención de pérdida de datos en la SSP.

6.2 Situación Actual del Mercado sobre Proveedores de DLP

Actualmente en el mercado existe una variedad de proveedores de *DLP* con una diversidad de productos que están disponibles para todas las organizaciones que quieran prevenir la fuga de información, tales como la SSP.

Dentro de la búsqueda de información sobre el mercado de DLP, en agosto de 2011, Gartner publico su Cuadrante Mágico, en el cual ubica gráficamente a los proveedores más importantes del mercado *DLP*, ver figura 19.

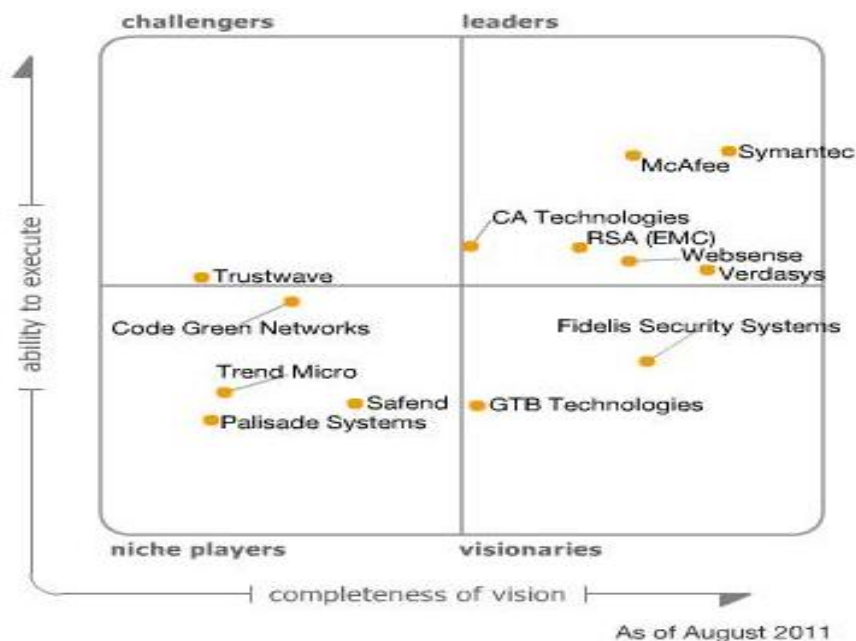


Figura 19 Cuadrante Mágico sobre Proveedores de DLP

Según Gartner (2011), la consolidación de proveedores se ha reducido, y el mercado ha sufrido una bifurcación hacia capacidades empresariales de necesidades altas y capacidades de costos de implementación bajos, ofreciendo más opciones a las organizaciones de todos los tamaños y necesidades.

Tras analizar las distintas soluciones que ofrecen los principales proveedores de seguridad en este mercado se han reconocido como Líderes a Symantec, McAfee, CA Technologies, RSA (EMC), Websense y Verdasys, como se indico en la figura 19, son proveedores que han demostrado una buena comprensión de las necesidades del cliente, para efectos de este trabajo se fija la atención a la solución de RSA, ya que cuenta con el soporte de la empresa EMC, que es una empresa mundial que ofrece servicios de almacenamiento y seguridad en toda Latinoamérica. .

En la categoría de *Challengers*, únicamente figura Trustwave; que su objetivo va mas encaminado al cumplimiento de normas (PCI DDS), referente a seguridad de tarjetas de pago y no a la protección global de la Información en la organización, por lo que este proveedor queda descartado para evaluarse, por no tener una relación directa con las necesidades de la SSP.

En el área de *Players Niche* figuran Code Green Networks, Trend Micro, Safend y Palisade Systems; son proveedores que no cuentan con una tecnología propia para el manejo de *DLP*, ya que tienen que apoyarse de otras soluciones para conformar una solución integral de seguridad de *DLP*.

Finalmente en el cuadrante de *Visionaries* sitúa a Fidelis Security Systems y GTB Technologies, son proveedores que se enfocan en el monitoreo de la actividad en la red, por lo que no cuentan con dispositivos que permitan apoyar la seguridad de la información en todo su ciclo de vida.

Por lo anterior y con base en las capacidades que ofrece cada proveedor de *DLP* se tomara como base de análisis a los proveedores de RSA, McAfee y Websense, por estar ubicados en el cuadrante de Líderes, según la figura 19, y que son los proveedores que pueden satisfacer las necesidades requeridas por la SSP.

6.3 Aspectos establecidos por la SSP para elegir el proveedor de DLP

Para la elección del proveedor de DLP en la SSP, quedaron establecidos una serie de aspectos que servirán de apoyo para dimensionar el alcance de las diferentes soluciones evaluadas, esto con el visto bueno de consultores externos que apoyan las políticas seguridad en la SSP. Los aspectos a ser evaluados así como su capacidad de integración y cumplimiento son:




- Establecer claramente el presupuesto con el que se cuenta para la adquisición, integración y puesta a punto la solución DLP.
- Proyectar el alcance en la implementación de la solución, ya que se deben de identificar las unidades de negocio que participaran.
- Conocer si los agentes de seguridad ofrecidos proporcionan medidas de seguridad en los equipos portátiles para el acceso a la información sensible estando conectados o no a la red interna de la SSP.
- Identificar los protocolos de red a monitorear, analizar o bloquear.
- Conocer las acciones de recuperación que se tomaran en caso de que alguna regla sea violada, ya sea bloquear, censar, educar o simplemente dejar pasar.
- Medir la demanda de información que fluye por la red de la organización.
- Conocer si la solución cuenta con un medio visual para monitorear el flujo de información en tiempo real.
- Conocer si la solución cuenta con una variedad de informes o reportes que permitan una fácil interpretación de la información obtenida.
- Contar con un análisis de como la solución de DLP, se integra y fortalece las herramientas de seguridad actuales en la SSP.
- Analizar el impacto en la implementación de la solución de DLP, para generar los convenios con las áreas involucradas, así como la difusión sobre la funcionalidad y el motivo por el cual se pretende implementar.





































6.4 Análisis de Proveedores de DLP.

En este punto se realiza el análisis comparativo técnico respecto a las funciones que se requiere que cumplan las soluciones de DLP. Se eligieron a los proveedores de RSA, McAfee y Websense, líderes en el área.





















































































El análisis comparativo técnico es realizado sobre soluciones que cuenta con el respaldo y el licenciamiento de los proveedores DLP enunciados anteriormente. Para ello los rasgos seleccionados fueron con base a los requerimientos establecidos por la SSP y los aspectos establecidos para la elegir los proveedores marcados en el punto 6.3.

Para efectos de evaluación se asignan los siguientes parámetros de calificación:

-  SI CUMPLE La solución cumple con lo que ofrece
-  MEDIO CUMPLE Cumple pero solo una parte de lo que ofrece
-  NO CUMPLE No cumple con lo que ofrece

Análisis Comparativo Técnico para Soluciones DLP			
Nombre del Proveedor	 The Security Division of EMC RSA Data Loss Prevention (DLP)	 McAfee Network DLP McAfee Host Data Loss Prevention	 ESSENTIAL INFORMATION PROTECTION™ Websense Data Security Suite
Detalles a Evaluar			
Características Generales			
• Tecnología tipo software y Appliance hardware, dedicado a un proceso en específico	 SI CUMPLE	 MEDIO CUMPLE	 SI CUMPLE
• Requiere Instalación de Agentes de seguridad	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Protección de archivos independientes del SO	 SI CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE
• Protección de datos que fluyen por la red (Network)	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Protección de datos en reposo (Storage y Data Center)	 SI CUMPLE	 NO CUMPLE	 MEDIO CUMPLE
• Protección de datos circulante (usuarios)	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Políticas de seguridad predeterminadas y modificables	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Administración, protección y monitoreo de los datos en tiempo real	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Fácil integración con herramientas de seguridad lógica y perimetral	 SI CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE
• Notificaciones automáticas al usuario final	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Detección activa de eventos de seguridad, como movimientos de información sensible y	 SI CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE

Análisis Comparativo Técnico para Soluciones DLP

Nombre del Proveedor	 The Security Division of EMC RSA Data Loss Prevention (DLP)	 ProvenSecurity™ McAfee Network DLP	 ESSENTIAL INFORMATION PROTECTION™ WebSense Data Security Suite
Detalles a Evaluar			
cambios de configuración			
<ul style="list-style-type: none"> • Consola de monitoreo para alertamiento de eventos detectados 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Platillas modificables para la reporte de incidentes 	 SI CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE
<ul style="list-style-type: none"> • Notificaciones vía SMTP y SMS al administrador sobre alertas detectadas 	 MEDIO CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE
Escenarios Controlados			
<ul style="list-style-type: none"> • Correo institucional. 	 SI CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE
<ul style="list-style-type: none"> • Correo público 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Compartición de archivo (P2P) 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Mensajería instantánea aplicativo 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Mensajería instantánea acceso web 	 MEDIO CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE
<ul style="list-style-type: none"> • Redes Sociales 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
Dispositivos Controlados			
<ul style="list-style-type: none"> • Computadoras de escritorio. 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Laptops, Ipad, Tablets 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Discos de almacenamiento masivo 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Dispositivos infrarrojos y bluetooth 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Teléfonos inteligentes (Smartphone) 	 MEDIO CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE
<ul style="list-style-type: none"> • Dispositivos infrarrojos y bluetooth 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • USB, DVD y Blue-ray 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
Protocolos de Análisis mas comunes			
<ul style="list-style-type: none"> • HTTP/HTTPS. 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • FTP 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • SMTP 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • POP 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • IMAP 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • TELNET 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
Acciones de Control de Datos			
<ul style="list-style-type: none"> • Monitoreo. 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Preventivo 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Cuarentena 	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
<ul style="list-style-type: none"> • Justificación 	 SI CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE
<ul style="list-style-type: none"> • Bloqueo 	 SI CUMPLE	 MEDIO CUMPLE	 MEDIO CUMPLE


































Análisis Comparativo Técnico para Soluciones DLP			
Nombre del Proveedor	 The Security Division of EMC RSA Data Loss Prevention (DLP)	 ProvenSecurity™ McAfee Network DLP McAfee Host Data Loss Prevention	 ESSENTIAL INFORMATION PROTECTION™ Websense Data Security Suite
Detalles a Evaluar			
Medios para la Administración			
• Consola Administrativa web.	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Control de Usuarios por perfiles	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Control de Usuarios administradores y finales	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
Herramientas de Reporte			
• Reportes en formato texto y gráficos.	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Reportes customizables a las necesidades de la organización	 SI CUMPLE	 MEDIO CUMPLE	 SI CUMPLE
• Generación de reportes programados y periódicos.	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Envío de Reportes y alertas al administrador vía Email, PDA, SNMP trap, Syslog.	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
Configuración regional de la Solución			
• Español	 SI CUMPLE	 NO CUMPLE	 SI CUMPLE
• Inglés	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE
• Otros	 SI CUMPLE	 SI CUMPLE	 SI CUMPLE

Tabla 3 Comparativo técnico proveedores DLP

Con base a la comparativa anterior, ver tabla 3, se elige al proveedor de RSA Data Loss Prevention (DLP), puesto que cumple satisfactoriamente con la mayor cantidad de lineamientos de evaluación técnicos establecidos por la SSP.

6.4.1 Cuadro de comparación resultados

	Cumple	Medio Cumple	No Cumple
RSA	93.8 %	6.2 %	0 %
McAfee	70.8 %	25 %	4.2 %
WebSense	77 %	23 %	0 %

Tabla 4 Comparación de cumplimiento proveedores DLP

Por lo antes expuesto se considera que la solución DLP que más se adecua a las necesidades de la SSP, es RSA Data Loss Prevention (DLP), ya que cumple en un 93.8% los requisitos establecidos por la SSP, ver tabla 4, por ello se recomienda la implementación y puesta a punto de la suite de RSA DLP, para cubrir con la necesidad de prevención de fuga de Información en la SSP.

6.5 Elementos de prueba para la evaluación del proveedor de DLP en la SSP

Para los productos DLP evaluados, se toma como referencia a la clasificación realizada por (Cano, 2011), en donde clasifica los datos en tres escenarios diferentes para su identificación, monitorización y protección estas son:

- Datos transmitidos en la red (*data in motion*¹⁶ o datos en movimiento)
- Datos almacenados (*data in rest* o datos en reposo)
- Datos en estaciones de trabajo (*data in use* o datos en uso)

El área de seguridad en la SSP encargada de la revisión sobre propuestas tiene la encomienda de generar una matriz de prueba para la evaluación de la solución que presenta cada uno de los tres proveedores seleccionados, ver anexo 1, así mismo se deben de considerar los siguientes puntos:

- Configuración del repositorio de documentos a probar, considerando varios formatos como: txt, word, pdf y entre otros.
- Se requiere que las maquetas realicen el monitoreo y control de documentos en base a información personal o de carácter interno que fluye dentro de la SSP, así como el envío de avisos sobre violaciones a las políticas implementadas

Cada proveedor debe de configurar su solución de DLP al nivel que sea necesario para implantar políticas de protección para la identificación de los diferentes documentos clasificados de acuerdo a su nivel de importancia establecido por la SSP y que fueron explicados en el punto 1.1.1.2 Valores de la Información.

¹⁶ Introducción a la tecnología Data Loss Prevention (DLP) disponible en <http://www.seinhe.com/blog/14-introduccion-a-la-tecnologia-data-loss-prevention-dlp>

6.5.1 Matriz de evaluación DLP.

Para este ejercicio se utilizó un documento para plasmar la calificación que obtiene cada uno de los proveedores, se les pide simular un escenario de riesgo, transfiriendo el set de documentos de prueba enunciados en el punto 6.5.3, y se evalúa la capacidad que presenta la solución en el monitoreo, la notificación y el bloqueo de dicha transferencia, el resultado obtenido en cada escenario será sumado permitiendo obtener el grado de cumplimiento y servir de base para la elección de la solución a implementar, ver anexo 1.

6.5.2 Requerimientos técnicos para la evaluación de las soluciones de DLP

Se le requirió a cada proveedor una maqueta con todos los dispositivos configurados que necesitaban y con los que actualmente cuenta para cubrir con la evaluación de seguridad de DLP.

Se les facilitó a los proveedores una pequeña red equipada con direccionamiento interno y un servidor que contenían algunos de los servicios que se corren comúnmente en una red corporativa, entre ellos: FTP, HTTP, HTTPS, Mail (POP, IMAP, & Exchange) y SSH.

Para efectos de la prueba se preparó un set de documentación de prueba con información clasificada en los diferentes niveles de sensibilidad.

Usando una máquina colocada al exterior de la red simulada, se intentó acceder a una serie de archivos a través de cada protocolo y de diferentes puertos de servicios LAN para extraer información de la red protegida.

Se evaluó cada producto analizando alrededor de cien archivos que se encontraban en un repositorio generado para esta prueba. Algunos de estos archivos contenían información sensible y otros eran inofensivos. Se registró qué archivos pasaron, cuáles fueron bloqueados y cuáles fueron marcados (pero no bloqueados).

6.5.3 Criterios de prueba sobre información sensible

Para continuar con el proceso de evaluación, se solicita a los proveedores de DLP que las maquetas realicen el monitoreo y control de documentos en base a información personal o de carácter interno que fluye dentro de la SSP, tomando en cuenta los siguientes criterios:

CRITERIOS DE PRUEBA SOBRE INFORMACIÓN SENSIBLE			
Documentación necesaria para evaluación	Sistemas operativos para la instalación de agentes de seguridad	Medios de transporte de evaluación	Requisitos para la consola de monitoreo
Documentos con RFC (Registro Federal de Contribuyentes)	Windows Vista, XP y 7. Windows 2003, 2008 Server. Mac OSX 10.6.	USB, DVD, Blu-ray Dispositivos Infrarrojos y bluetooth	Monitoreo de eventos e incidencias en tiempo real
Documentos con CURP (Clave Única de Registro de Población)	Linux Red Hat Enterprise 5. Iphone 3 y 4 Blackberry	Mensajería Instantánea Teléfonos Inteligente (SmartPhones)	Generación de reportes por eventos e incidencias.
Documento con CUIP o (Cédula Única de Identificación Policial)	Android 3 en adelante Otros ambientes	Tabletas Electrónicas (Tablets)	Respaldo de configuración general de la solución.
Documento con números de placa de automóvil		Email público e institucional Impresora / Fax	Respaldo y depuración de bitácoras generadas.
Documento con información de contratos y licitaciones		FTP, HTTP, HTTPS	Monitoreo de eventos en tiempo real
Documentos con números telefónicos locales y celulares.			
Documentos con identificadores de contrato			
Documentos con números de cuentas bancarias			

Tabla 5 Criterios de prueba sobre información sensible

Los criterios clasificados de la Tabla 5, sirven de base para la evaluación de los diferentes escenarios prueba establecidos por la SSP y que serán calificados mediante la matriz de evaluación, como se enuncia en el punto 6.5.1.

6.6 Resultado de la evaluación de proveedores de DLP

En relación a la evaluación de las maquetas de prueba presentadas por los tres proveedores se obtuvo los siguientes resultados:

- En base a los datos obtenidos en el análisis de proveedores planteados en el punto 6.4 y 6.4.1, el proveedor que mayor calificación obtuvo fue el proveedor de RSA con su solución identificada con el nombre RSA Data Loss Prevention (DLP)
- Las soluciones de DLP de los proveedores de RSA y Websense fueron las que detectaron eficientemente los archivos con información sensible utilizados para la prueba.
- Para el caso de la solución de DLP de McAfee, esta detecto correctamente los archivos sensibles pero fueron menos eficientes a la hora de bloquearlos.
- Cabe resaltar que de las tres soluciones de DLP evaluadas, ninguna pudo analizar ni bloquear información sensible de contenido encriptado, quedando pendiente para una próxima evaluación.
- El agente de seguridad con el que cuenta la solución de DLP RSA, alcanzó el puntaje más alto en lo referido a detección, y también obtuvo un buen resultado en la facilidad de configuración, así como el refuerzo de la seguridad fuera de la institución.
- En lo referente a la interfaz web, la ofrecida por la solución de DLP RSA es la más amigable ya que muestra a través de gráficos la cantidad de incidentes que están siendo obtenidos por la solución.

- En lo referente a la configuración de las políticas para el monitoreo, análisis y bloqueo de incidentes, la solución de DLP que obtuvo el mejor puntaje ya que cuenta con la flexibilidad de tener precargadas una serie de reglas, que permiten al usuario modificar estas políticas y que se ajusten a sus necesidades. En comparación con éste, McAfee y Websense quedaron un poco deslucidos pues exigen más esfuerzos para comprender la estructura de reglas y complican innecesariamente el proceso.
- La Suite de RSA DLP, tuvo el mejor desempeño con una capacidad de detección: del 90% de precisión sobre el set de prueba evaluado. El 10% restante no lo pudo manejar por falta de soporte para flujo de tráfico encriptado (sesiones SSH).
- La solución de Websense tuvo una tasa de éxito de 64% en la detección y el bloqueo sobre el set de prueba evaluado. Para el otro 36% corresponde a datos que no pudo detectar, ni bloquear y que constituyen a una cantidad considerable de información perdida.
- En lo relacionado a reportes la solución de RSA DLP y McAfee, generaron reportes apegados a lo requerido por la SSP, y que para el área de seguridad resulta sumamente valioso saber qué tipo de información está siendo consultada, monitoreada y bloqueada por la solución, y que sirva como un histórico de datos o para la toma de decisiones.

Conclusiones y Recomendaciones

Actualmente la SSP cuenta con medidas de seguridad defensivas como Firewall, Proxy, VPN y supervisores de red (IPS e IDS), que realizan auditorías y evitan el acceso externo no autorizado a su información, sin embargo para el escenario de pérdida de información interna requiere de una solución efectiva que detecte los posibles incidentes de fuga de datos de manera oportuna, es en este sentido que el trabajo que se entrega a dicha institución como propuesta de análisis, responde a sus necesidades y condiciones, tal como se planteo inicialmente en el objetivo:

- Análisis de una solución integral, que permita proteger los recursos (Aplicaciones y Bases de Datos, Accesos, Transacciones, Políticas, Protocolos de Transferencia, Hardware) dentro de las Secretaria de Seguridad Pública (SSP).

Para cumplir con el objetivo, el documento de tesina incluyo un análisis de mercado en relación a las principales tecnologías de seguridad de DLP que le permitan a la SSP en un futuro poder ser candidato a certificaciones de calidad sobre el uso de la información.

Un punto valioso del trabajo realizado es que permite a cualquier persona conocer los principales procesos para elegir una tecnología de DLP que se adapte a las necesidades de su organización como en el caso de la SSP, aquí revisado; debe de empezar por identificar sus activos principales y revisar las políticas definidas en relación a los eventos potencialmente vulneradores que impidan la funcionalidad de cada área.

Dicha propuesta adquiere relevancia, ya que; las entidades gubernamentales y privadas le están dando mayor importancia al manejo de la información con la que cuentan, estableciendo políticas, procedimientos, normas e inclusive leyes que la regulan. Por lo que una solución DLP puede cubrir necesidades de seguridad requeridas en las dependencias de gobierno.

Las organizaciones no se pueden permitir el privilegio de tener fugas no controladas, es por esto que la implementación de la solución de RSA, les permitirá reforzar las medidas de seguridad con las que cuentan.

El trabajo desarrollado en esta tesina, impacta fundamentalmente en el Data Center denominado “Constituyentes”, que es donde se concentra toda la información confidencial utilizada por la SSP.

Con la solución determinada en el trabajo de tesina, la SSP:

- Contará con una solución que se adecua a sus necesidades presupuestales, tecnológicas y de seguridad para la protección de sus recursos.
- En su Dirección de Seguridad Informática (DSI), contará con una herramienta que le permita descubrir, monitorear y proteger la información que fluye dentro y fuera de la red, ante cualquier uso indebido.
- Reforzará políticas de seguridad Interna.
- Administrará de manera sencilla la información durante todo su ciclo de vida.
- Regulará a los usuarios en el correcto uso de su información.
- Se encaminará a ser candidato a una certificación de procesos en el tratamiento de la información.

Y en general este trabajo servirá de modelo para la implementación en otras dependencias de gobierno que desean prevenir la fuga de información.

La solución de seguridad DLP, dentro de la SSP puede ir más allá de esta propuesta. Como se ha mencionado anteriormente, este modelo de análisis e implementación contempla otros temas relacionados a la prevención de pérdida de datos que pueden ser punto de partida para temas de investigación, como la Seguridad de la Información en la *Cloud Computing* (seguridad en la nube de

internet) ya que en este trabajo de tesina se abarco la prevención de perdida de datos por usuarios internos, por lo que se debería de buscar medidas para la seguridad de la información también en la nube de internet, como un tema de aspecto más administrativo y de normatividad es la Implantación de un Sistemas de Gestión de Seguridad de la Información (SGSI) basado en DLP, ya que contar con un SGSI permitiría a una organización gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información y minimizando a la vez los riesgos de seguridad de la información.

Bibliografía

A

Aguirre R. (2006), Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1, Sexta edición de 1 de Marzo de 2006. Disponible en http://www.criptored.upm.es/guiateoria/gt_m001a.htm

Alin, F. Lafont, D. y Macary, F. (1997). Trad. Amadeus Brugués. El proyecto intranet. Edit.Gestión 2000. Barcelona. ISBN: 84-8088-171-2.

Andrew S. Tanenbaum y Maarten van Steen. "Distributed systems: principles and paradigms". Prentice-Hall 2002. ISBN 0-13-088893-1.

Ardita, J. (2009), Director de Cybsec S.A. Security Systems y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2009 en instalaciones de Cybsec S.A. <http://www.cybsec.com>

B

C

Calvo, J. New Net S.A. Septiembre de 2009. Disponible en: <http://www.newnetsa.com/2009/08/fuga-de-informacion-en-las-organizaciones/>

Cámara de Diputados, "Ley Federal de Transparencia y acceso a la Información Pública Gubernamental" ultima reforma 05 de Julio de 2010, Disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf>

Campos, E. Líder empresarial. Octubre de 2009. Disponible en: <http://www.liderempresarial.com/num175/10.php>

Cano, J. (Junio de 2004) Inseguridad Informática: "Un concepto dual en Seguridad Informática". Disponible en: <http://www.acis.org.co/fileadmin/inseg-inf.pdf>.

Carbone, J.A. (2004). "IT architecture toolkit Enterprise computing series." Upper Saddle River, NJ, Prentice Hall PTR

Clinger-Cohen (1996) "What is the Clinger-Cohen Act, and how does it affect people with disabilities?" AccessIT University of Washington Disponible en: <http://www.washington.edu/accessit/articles?104>

Cook, M.A. (1996). "Building enterprise information architectures: reengineering information systems." Hewlett-Packard professional books. Upper Saddle River, NJ, Prentice Hall.

D

Default Password List, (2003) Portal de Seguridad Disponible en: <http://www.phenoelit-us.org/dpl/dpl.html>

Diccionario de la Real Academia de la Lengua Española, Disponible en: <http://buscon.rae.es/>

Diccionario Libre, disponible en: <http://es.thefreedictionary.com>

E

Enciclopedia Virtual Informática. "Arquitectura Informática", consultado por última vez agosto 2011, Disponible en: <http://www.terra.es/personal/lerrmon/cat/articles/evin0034.htm>

Enciclopedia libre "Wikipedia", "Informática", Disponible en: <http://es.wikipedia.org/wiki/Informática>, febrero de 2011.

Enciclopedia libre "Wikipedia", "Framework", Disponible en <http://es.wikipedia.org/wiki/Framework>, Septiembre de 2011

Escobar, B. (1997). "La evaluación económica de los sistemas de información." Edit. Universidad de Sevilla. Sevilla. ISBN: 84-472-0345-X.

F

Fehskens L (2008), "Re-thinking architecture. In: 20th enterprise architecture practitioner's conference." The Open Group, Reading

Fowler, M. (2003). "Patterns of enterprise application architecture". The Addison-Wesley signature series. Boston, Addison-Wesley.

Fuentes, M. (2008), Noticias, Sección Opinión: "Robo en CIMAC" Disponible en: <http://rotativo.com.mx/reginacantu/robo-en-cimac/7689/html/>

G

Gartner Consulting (2011), "Incorporating Security into the Enterprise Architecture Process." Whitepaper Disponible en: http://www.gartner.com/DisplayDocument?ref=g_search&id=488575.

George Coulouris, Jean Dollimore y Tim Kindberg. "Sistemas Distribuidos: conceptos y diseño". 3ª edición. Addison Wesley 2001. ISBN 84-7829-049-4

Global Knowledge. (2008), "Ten ways hackers breach security", Disponible en: <http://images.globalknowledge.com>

Graves K. (2010) "Etapas de un Ataque". Fuente, Certified Ethical Hacker Study Guide, 2010, by Wiley Publishing, Inc., Indianapolis, Indiana <http://www.eccouncil.org/>

Groot, R. Smits and. Kuipers, h. (2005). "A Method to Redesign the IS Portfolios in Large Organizations", Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05). Track 8, p. 223a. IEEE.

Groot, R., M. Smits and H. Kuipers (2005). "A Method to Redesign the IS Portfolios in Large Organizations." Disponible en: <http://csdl2.computer.org/persagen/DLAbsToc.jsp?>

Gómez, Á (2007). Enciclopedia de la Seguridad Informática. 1era Edición. México DF, AlfaOmega Grupo Editor S.A. de C.V. pp. 4, 7. ISBN: 978-970-15-1266-1

H

Hornos, M.; Araque, F. y Abad, M. (1998). "La gestión de la información como clave para adquirir ventaja competitiva: los MIS", en Alta Dirección. Número 199. Mayo. Barcelona. ISSN: 0002-6549.

Howard, J. (2005), "Thesis: An Analysis of security on the Internet 1989–1995." Carnegie Institute of Technology. Carnegie Mellon University. 1995. E.U. Disponible en: <http://www.cert.org/archive/pdf/JHThesis.pdf>. Capítulo 6 Página 59.

I

IETF "The Internet Engineering Task Force" en su RFC 2828 "Internet Security Glossary" (200), Disponible en: <http://www.ietf.org/rfc/rfc2828.txt>

ITIL (2006), Glosario de Términos, Definiciones y Acrónimos. Disponible en: http://www.google.com.mx/url?sa=t&source=web&cd=7&sqi=2&ved=0CG8QFjAG&url=http%3A%2F%2Fwww.itil-officialsite.com%2Ffmsruntime%2Fsaveasdialog.aspx%3FID%3D925%26SID%3D242&rct=j&q=confidencialidad%2Bitil&ei=1XeGT0-DOYvJsQK_x_2aDw&usg=AFQjCNHWwT7Rp8qQcKf0PEwCfmfHzq7UEQ&sig2=-E7ZRAxQLSjEbnFOUAKeA&cad=rja

ISO (Octubre de 2010), "Organización Internacional por la Normalización." " ISO/IEC 27002:2005", Disponible en: http://www.iso.org/iso/catalogue_detail?csnumber=50297

ISO (2005), "Organización Internacional por la Normalización." ISO/IEC 17799:2005 "Gestión de un incidente en la seguridad de la información" p (138), Disponible en: <https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf>

ISO (2004), Organización Internacional por la Normalización ISO/IEC 13888-1:2004, IT security techniques -- Non-repudiation -- Part 1: General

Cano, F (2011), "Introducción a la tecnología Data Loss Prevention (DLP)" disponible en <http://www.seinhe.com/blog/14-introduccion-a-la-tecnologia-data-loss-prevention-dlp>

J

James, J. (2003), Enterprise Risk Management, Wiley & Sons, Inc.

K

Kanagasingham, P. (2008) SANS Institute Reading Room "Data Loss Prevention." Disponible en: http://www.sans.org/reading_room/whitepapers/dlp/data_loss_prevention_32883

Killmeyer T. (2001). Information Security Architecture "An Integrated Approach to Security in the Organization", Auerbach, Washington, D.C.

Kurose, K. (2004), "Redes de Computadoras, Un enfoque descendente basado en Internet" 2da Edición ed. Pearson Addison-wesley. Disponible en: http://books.google.com.mx/books?id=Etb3tY4qXhgC&pg=PT9&lpg=PT9&dq=Redes+de+Computadoras,+Un+enfoque+descendente+basado+en+Internet%2Bbibliografia&source=bl&ots=kff8Tcx6mu&sig=Xc3IUwKxfPuAEc_Zb7rRj3x-OA&hl=es&sa=X&ei=78hrT_OcMMaP4gTA9sWABg&ved=0CC8Q6AEwAg#v=onepage&q=Redes%20de%20Computadoras%2C%20Un%20enfoque%20descendente%20basado%20en%20Internet%2Bbibliografia&f=false

L

Laboratorio ESET Latinoamérica (2008) "Informe sobre malware en América Latina", Disponible en: <http://www.eset-la.com/threat-center/1732-informe-malware-america-latina>

Ley Clinger-Cohen, Parlamento Europeo, Noviembre de 2006. Última consulta junio de 2010 Disponible en: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2006-5036+0+DOC+XML+V0//ES>

López, J. y Quezada, C. (2005) .Apuntes de Seguridad Informática, México Facultad de Ingeniería – UNAM.

M

Mieres, J. (2009), "Ataques informáticos Debilidades de seguridad comúnmente explotadas" p (4), Disponible en: https://www.evilmfingers.com/publications/white_AR/01_Atques_informaticos.pdf

Mitnick, B. (2005), "The Art of Intrusion". John Wiley & Sons,

M. L. Liu. "Computación Distribuida: Fundamentos y Aplicaciones". Addison Wesley 2004. ISBN 84-7829-066-4.

N

Nichols. R (2002) Defending your digital assets. Primera edición. New York. McGraw-Hill. p (45).

Ñ

O

Ortega, F. (2003), Noticias, Sección Nacional: "Robo del registro nacional de población (RENAPO)", Disponible en: http://www.cronica.com.mx/nota.php?id_notas=65060

P

Peltier, T. (2001) "Information Security Risk Analysis." Auerbach 2001 Londres, Inglaterra.

Pfleeger (1997), Conferencia de Investigación sobre Seguridad, "La investigación en línea Información de Gestión de Seguridad de Australia". Disponible en <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1001&context=ism>

Portal de la Subdirección de Seguridad de la Información (2010), Información y servicios de seguridad en cómputo, "vulnerabilidades". Disponible en <http://www.seguridad.unam.mx/vulnerabilidadesDB/>

Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05). p. 223a. IEEE.

Q

Quinn, J. Anderson, P. y Finkelstein, S. (1996). "La gestión del intelecto profesional: sacar el máximo de los mejores." en Harvard Deusto Business Review. Número 75. Diciembre. Edic. Deusto. Bilbao. ISSN: 0210-900.

R

Reynolds, J. Holbrook, P. (1991, Julio) "Site Security Handbook".

S

Schmidt, D. (1995), "Object interconnections. Introduction to Distributed Object Computing", SIGS C++ Report Magazine, Vol 7, No 1.

Schneier, B. (2000), *Secrets & Lies. "Digital Security in a Networked World"*. John Wiley & Sons.

Senado de la Republica (2010), *Comunicación Social: "Ley de Federal de protección de datos personales"* Disponible en: http://comunicacion.senado.gob.mx/index.php?option=com_content&task=view&id=15767&Itemid=80

Securosis. (2009, Noviembre) "Understanding and Selecting a DLP Solution". Disponible en: http://www.websense.com/assets/white-papers/Understanding_and_selecting_a_DLP_solution_WP.pdf

Seguridad Informática, (2011, Septiembre) "Cuadrante Mágico sobre proveedores de DLP", Disponible en: <http://seguinfo.wordpress.com/2011/09/02/cuadrante-magico-sobre-proveedores-de-dlp/>

Solay, M. García, R (2011), "Seguridad en la información y Seguridad Informática" Portal de Seguridad: Disponible en: http://www.manualdeseguridad.com.mx/aprende_a_protegerte/seguridad_en_la_informacion/seguridad_en_la_informacion.asp

Spewak, S. H. and S. C. Hill (1993). "Enterprise architecture planning: developing a blueprint for data, applications, and technology". Boston, QED Pub. Group

Sybex. (2007), *Official Certified Ethical Hacker*,

T

Trevor.K (2003) *Security*. Primera edición. California. Mc.Graw-Hill. p. (203)

Tzu, S. (2006), "El arte de la guerra", Versión de Samuel Griffith. Editorial Taschen Benedikt.

U

Urrutia, A. (2003), *Noticias, Sección Política, "Identifica el IFE al presunto autor de la venta del padrón electoral"* Disponible en: <http://www.jornada.unam.mx/2003/05/16/016n1pol.php?origen=index.html&fly=2> (Última fecha de consulta día de agosto 2010)

Universidad Centroccidental Lisandro Alvarado. "UCLA", (2009. Septiembre), Disponible en: http://www.ucla.edu.ve/dac/Departamentos/coordinaciones/informaticai/documentos/resumen_tema3.pdf

V

W

Wikipedia (2010), "Seguridad de la Información", Disponible en: http://es.wikipedia.org/wiki/Seguridad_de_la_informacion

Wikipedia (2011), "Riesgo (Informática)", Disponible en: [http://es.wikipedia.org/wiki/Riesgo_\(informática\)](http://es.wikipedia.org/wiki/Riesgo_(informática))

Wikipedia (2011), "Interoperabilidad", Disponible en: <http://es.wikipedia.org/wiki/Interoperabilidad>

X

Y

Z

Zendejas, S. (2000), *Ciclo Anual de Conferencias 2000 de CCEA (6a), p (2)*. Disponible en http://www.grupoccea.info/Biblioteca/Memorias/C_Seguridad.pdf

Anexo 1

Secretaría de Seguridad Pública
Coordinación General de la Plataforma México
Dirección de Seguridad Informática



México D. F.; a ____ de _____ del 2011.

Proveedor a Evaluar: _____ Contacto (s): _____
 Lugar de Evaluación: _____

Objetivo. Evaluar las herramientas de DLP de los proveedores así como la capacidad técnica de los especialistas de la solución.

- Pruebas que se consideran en la evaluación:
1. Públicos
 2. Privados
3. Detección de información sensible
 4. Detección de patrones de tráfico (REGEXP)
 5. Cualquier documento con cualquier extensión
 Caso práctico 5. Pruebas de operación

		Monitor														
		USB	Impresoras	Bluetooth	MSG	MSG Web	Red Sociales	email institucional	email publico	TFTP	File Share	Otros medios				
Plataformas OS: PCs de escritorio, Laps y servidores	Inbound	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5
		Tat														
		Cifrado														
		Comprimido														
		Captura de pantalla														
		Cambios de extensión/sin extensión														
	Archivo codificado en 64bits															
	Archivo codificado en hexadecimal															
	Ponderación															
	Observaciones.															
Plataformas OS: PCs de escritorio, Laps y servidores	outbound	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win XP Win Server 2003 Win Server 2008 Win Server 2008 R2 Mac OS X 10.5 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5	Win Vsta Win 7 Win Server 2008 Win Server 2008 R2 Mac OS X 10.6 Linux Red Hat Enterprise Linux 5
		Tat														
		Cifrado														
		Comprimido														
		Captura de pantalla														
		Cambios de extensión/sin extensión														
	Archivo codificado en 64bits															
	Archivo codificado en hexadecimal															
	Ponderación															
	Observaciones.															

		Monitor														
		USB	Impresoras	Bluetooth	MSG	MSG Web	Red Sociales	email institucional	email publico	Otros medios						
Plataformas OS: Smart phones	Inbound	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6
		Tat														
		Cifrado														
		Comprimido														
		Captura de pantalla														
		Cambios de extensión/sin extensión														
	Archivo codificado en 64bits															
	Archivo codificado en hexadecimal															
	Ponderación															
	Observaciones.															

		Remediación														
		USB	Impresoras	Bluetooth	MSG	MSG Web	Red Sociales	email institucional	email publico	Otros medios						
Plataformas OS: Smart phones	Inbound	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6	iPhone 3 iPhone 4 BlackBerry Android Symbian Windows Mobile 6
		Tat														
		Cifrado														
		Comprimido														
		Captura de pantalla														
		Cambios de extensión/sin extensión														
	Archivo codificado en 64bits															
	Archivo codificado en hexadecimal															
	Ponderación															
	Observaciones.															

 Proveedor

 Evaluador

Figura 20 Matriz de Evaluación DLP