ESTUDIO SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES DEL ÁREA METROPOLITANA DE MEDELLÍN

LILIANA CASAS JIMÉNEZ

UNIVERSIDAD EAFIT
INGENIERÍA DE SISTEMAS
DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS
MEDELLÍN
2006

ESTUDIO SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES DEL ÁREA METROPOLITANA DE MEDELLÍN

LILIANA CASAS JIMÉNEZ

Trabajo de Grado para optar al
Título de Ingeniero Sistemas

ASESOR
RAFAEL DAVID RINCÓN
PROFESOR
DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS
UNIVERSIDAD EAFIT

UNIVERSIDAD EAFIT
INGENIERÍA DE SISTEMAS
DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS
MEDELLÍN
2006

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

DEDICATORIA

"A mis padres y familiares que siempre estuvieron apoyándome en todas las situaciones y por ser mi soporte constante, por vivir y sufrir conmigo, cada día de este proceso y proyecto, pues sin ellos hubiese sido imposible alcanzar este logro"

AGRADECIMIENTOS

El autor expresa sus agradecimientos:

A Rafael David Rincón, Profesor del Departamento de Informática y Sistemas de la Universidad Eafit, por el constante acompañamiento para la consecución de este trabajo.

A todas las empresas encuestadas por su apoyo a este proyecto, a los encuestados por su tiempo y disposición en la realización de todas las actividades y a las personas que facilitaron la comunicación con muchas de las personas pertenecientes a las empresas encuestadas.

A nuestras familias y seres queridos por su apoyo incondicional y su comprensión en todo momento.

A la Universidad Eafit, por habernos dado la oportunidad de tenernos en las aulas de tan magna institución.

Finalmente, a todas aquellas personas y amigos que me brindaron su apoyo, tiempo e información para el logro de mis objetivos.

A todos, muchas gracias.

TABLA DE CONTENIDO

ABREVIATURAS…….……10

GLOSARIO…….…….…… 11

1. INTRODUCCIÓN GENERAL…….....14

2. OBJETIVOS GENERALES Y ESPECÍFICOS.....16

2.1. Objetivo General……..16

2.2. Objetivos Específicos……..16

3. SEGURIDAD INFORMÁTICA……..17

3.1. Definición de Seguridad……..17

3.2. Análisis de la importancia de la seguridad informática…..…….18

3.3. De quién se debe proteger……..…….24

3.3.1. AMENAZAS HUMANAS EXTERNAS…..……..25

3.3.1.1. Hackers……..…..…… 25

3.3.1.2. Crackers……..…… 27

3.3.1.3. Phreakers……..……...27

3.3.1.4. Phisher……..……..……..……28

3.3.1.5. Ex - Empleado……..……... 28

3.3.1.6. Curiosos……..……..……..…… 28

3.3.1.7. Terroristas……..……..……29

3.3.1.8. Intrusos remunerados…..……..……. 29

3.3.2. AMENAZAS HUMANAS INTERNAS…..……..…… 29

3.3.2.1. Personal Interno……..…….30

3.4. Qué se debe proteger……..…….30

4. SEGURIDAD LÓGICA……...32

4.1. CONTROLES DE ACCESO…….33

4.1.1. Identificación y Autentificación……..……..…….. 33

4.1.2. Roles……..……..…….36

4.1.3. Limitaciones a los servicios…..……..……..……36

4.1.4. CONTROL DE ACCESO INTERNO…..……..……..……36
4.1.4.1. Palabras claves (Password)……..……...36
4.1.4.2. Encriptación……..……...37
4.1.4.3. Etiquetas de seguridad……..……...38
4.1.5. CONTROL DE ACCESO EXTERNO…..……..……..…...…38
4.1.5.1. Dispositivos de control de puertos……..…….38
4.1.5.2. Firewalls o puertas de seguridad…….…….38
4.1.5.3. Acceso de personal contratado o consultores……..……38
4.1.5.4. Accesos públicos……...……..……38
5. NORMA ISO 17799…….…….39
5.1. Historia de la norma ISO 17799……...……..39
5.2. Qué es la norma ISO 17799……...….40
5.3. Objetivos de la norma ISO 17799……...40
5.4. Diez áreas de control de ISO 17799……41
5.5. Ventajas del uso de la norma ISO 17799……44
5.6. Factores críticos de despliegue de las buenas prácticas recogidas en la norma ISO 17799……45
5.7. Antecedentes……..……..46
6. SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES……47
7. SEGURIDAD INFORMÁTICA EN COLOMBIA……..……...49
8. INVERSIONES EN TECNOLOGÍAS DE SEGURIDAD…….…51
9. ANÁLISIS DE CAMPO SOBRE LA SEGURIDAD INFORMÁTICA EN ALGUNAS EMPRESAS DE MEDELLÍN…….…….54
9.1. Consideraciones……...……54
9.2. Metodología utilizada para la investigación práctica……..…...55
9.3. Encuesta realizada……...……56
9.4. Situación Actual de las empresas del Área Metropolitana de Medellín...…..58
9.5. Estadísticas generales……...……...60
9.5.1.Certificaciones del personal interno…..……..……..…….61
9.5.2.Elementos y soluciones tecnológicas de seguridad……..……..…...62

9.5.3.Presupuesto de seguridad…..……..……..…….63
9.5.4.Confianza en la protección…..……..……..……...63
9.5.5.Incidentes de seguridad…..……..……..…….64
9.5.6.Retos de seguridad…..……..……..……65
9.5.7.Revisiones de seguridad en los activos de la información..……..……66
9.5.8.Obstáculos en la seguridad informática…..……..……..……66
9.5.9.Medidas de seguridad implementadas por las organizaciones..……67
9.5.1.0.Gestión del riesgo del proveedor…..……..……..……...68
9.5.1.1. Tecnologías de mayor preocupación en el área de seguridad……..…..68
10. RECOMENDACIONES DE LA NORMA ISO/IEC 17799……...…….70
10.1. Política de seguridad de la información……...……..70
10.2.Organización de la seguridad…..……..……..…….71
10.3.Seguridad de los accesos de terceras partes…..……..……..……...72
10.4.Outsourcing…..……..……..……72
10.5.Clasificación y control de activos…..……..……..……..73
10.6.Seguridad ligada al personal…..……..……..……..74
10.7.Seguridad física y del entorno…..……..……..……...76
10.8.Controles generales…..……..……..……....76
11. CONCLUSIONES……...78
12. BIBLIOGRAFÍA…….83
13. ANEXO 1 – ESTUDIO DE SEGURIDAD INFORMÁTICA DE EMPRESAS LATINOAMERICANAS……..87
ANEXO 2 - ENCUESTA DE LA SEGURIDAD DE LA INFORMACIÓN...92

LISTA DE FIGURAS

Figura 1: Certificaciones Personal Interno…….61
Figura 2: Herramientas de Seguridad empleadas……...62
Figura 3: Presupuesto Seguridad Informática año 2006……63
Figura 4: Nivel confianza amenazas internas……63
Figura 5: Nivel confianza amenazas externas……...64
Figura 6: Intrusiones de seguridad en el año 2006……64
Figura 7: Limitaciones presupuesto……...65
Figura 8: Concienciar del valor de la seguridad TI a los Directivos…….65
Figura 9: Revisiones de seguridad…….66
Figura 10: Obstáculos en la seguridad……...67
Figura 11: Medidas de seguridad implementadas…….67
Figura 12: Gestión del riesgo del proveedor…….68
Figura 13: Tecnologías de mayor preocupación……...69

ABREVIATURAS

BS	British Standard.
BSI	British Standard Institute.
CD-ROM	CD - read-only memory.
CPU	Central Processing Unit.
DNI	Documento Nacional de Identidad-Españoles.
ISO	International Organization for Standardization.
PC	Personal Computer.
TI	Tecnología Informática.
WEB	World Wide Web.
PDA	Personal Digital Assistant.
NIST	National Institute of Standards and Technology.
RBAC	Role Based Access Control.

GLOSARIO

CD-ROM: Un CD-ROM es un disco compacto utilizado para almacenar información.

CPU: Se denomina CPU o Unidad Central de Proceso (UCP) a la unidad donde se ejecutan las instrucciones de los programas y se controla el funcionamiento de los distintos componentes del ordenador. Suele estar integrada en un chip denominado microprocesador.

DNI: Tarjeta que contiene una firma electrónica y que sirve para identificarse ante cualquier aplicación por Internet u otro tipo de gestiones que requieran certificar la titularidad.

Downsizing: Es la migración de aplicaciones a plataformas de cómputo menores, con la intención de obtener mayor flexibilidad, eficiencia, reducción de costos y autosuficiencia para los usuarios.

Encriptar: Alterar información digital inteligible utilizando códigos secretos para que la información sea ininteligible para partes no autorizadas.

Firewall: Un cortafuegos o firewall en inglés, es un equipo de hardware o software utilizado en las redes para prevenir algunos tipos de comunicaciones prohibidos por las políticas de red, las cuales se fundamentan en las necesidades del usuario.

Hardware: Se denomina hardware o soporte físico al conjunto de elementos materiales que componen un ordenador. En dicho conjunto se incluyen los

dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, periféricos de todo tipo y otros elementos físicos.

Internet: Es una red de redes a escala mundial de millones de computadoras interconectadas con el conjunto de protocolos TCP/IP. También se usa este nombre como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que la Internet, independientemente de su extensión o de que sea pública o privada.

MainFrames: Es un ordenador grande, potente y costoso, usado antiguamente para el procesamiento de una gran cantidad de datos

Outsourcing: Contratación de los servicios de un tercero, para la ejecución de algunos procesos que se realizaban dentro de la organización.

Password: Una contraseña (password en inglés) o clave, es una forma de autenticación que utiliza una información secreta para controlar el acceso hacia algún recurso.

PC: Término genérico utilizado para referirse a todos los microordenadores.

PDA: (Ayudante personal digital) es un ordenador de mano, originalmente diseñado como agenda electrónica. Hoy en día se puede usar como un ordenador doméstico (ver películas, crear documentos, navegar por internet).

PIN: Es el número secreto que se otorga a un propietario a fin de probar su identidad.

Software: también conocido como aplicación informática, es la parte lógica del ordenador; esto es, el conjunto de programas que puede ejecutar el hardware para la realización de las tareas de computación a las que se destina. Es el conjunto de instrucciones que permite la utilización del equipo.

Staff: Conjunto de recursos que asesoran y colaboran con un componente específico dentro de una organización.

Tester: Es la persona encargada de hacer pruebas a un software.

TI: Nombre del conjunto para todo el hardware y el software del campo de los ordenadores y las comunicaciones.

WEB: La Web o WWW, es un sistema de hipertexto que funciona sobre Internet. Para ver la información se utiliza una aplicación llamada navegador web para extraer elementos de información (llamados "documentos" o "páginas web") de los servidores web (o "sitios") y mostrarlos en la pantalla del usuario.

1. INTRODUCCIÓN GENERAL

Hoy en día la empresa depende absolutamente de su sistema informático, si éste colapsa, se detiene el negocio; además, la competencia no podría recibir mejor regalo que cierta información confidencial de la empresa, como su plan de negocio, la base de datos de clientes, etc.
Sumado ello a la exposición a la que se encuentra dicha información, consecuencia de los accesos y privilegios a las aplicaciones concedidos a los usuarios que las manejan, se evidencia la necesidad de asegurar la información que apoya el negocio y garantizar que ésta se encuentre siempre disponible, íntegra y confidencial, para las personas que la requieren.

Pero eso no es todo; las miles de amenazas que ponen en riesgo estos principios de la información, hacen que se manifieste por parte de las directivas de las organizaciones la necesidad de asegurar la información. Por eso es importante para las empresas contar con un buen modelo de seguridad informática, que permita garantizar la transparencia en los procesos involucrados en la cadena de valor de la organización, de manera que permita la continuidad del negocio.

Desde esta perspectiva, la seguridad de los sistemas de información es una necesidad ineludible para las empresas, y se necesita asegurar la información disponible en muchos medios para afrontar los retos de la competencia, el dinamismo de los negocios y la operación diaria de los procesos.

Las organizaciones en el mundo empiezan a preocuparse por la seguridad de su activo más valioso, la información. Por esto se hace indispensable asegurar la infraestructura tecnológica, física y humana que soportan dichos activos, con el objeto de garantizar la transparencia en los procesos involucrados en la cadena de valor de la

organización, y por ende, garantizar la integridad, la confidencialidad y la disponibilidad de la información relevante para la continuidad del negocio.

Por lo tanto, es importante para las empresas contar con un buen modelo de seguridad informática, dado que la información se encuentra sometida constantemente a riesgos de tipo humano, físicos y tecnológicos, sumado a las amenazas y vulnerabilidades que a diario frecuentan dichos entornos.

Con base en lo anteriormente expuesto, se ha querido dirigir una investigación estilo trabajo de campo, con el fin de evaluar en las empresas de la ciudad de Medellín, qué grado de seguridad de la información manejan, qué tan valioso es para ellas mantener segura la información, cómo están preparadas para los constantes ataques informáticos, conocer el estado actual de la seguridad de la información en las empresas de la ciudad y a su vez, mirar cuáles son las debilidades, fortalezas, oportunidades y amenazas a la hora de mantener segura la información de la organización.

También este análisis permite el intercambio de conocimiento, opiniones y experiencias alrededor del tema planteado, para proponer soluciones a problemas complejos de seguridad informática, con la ayuda de los conceptos teóricos vistos durante la carrera, que enriquezca a los estudiantes, docentes, profesionales y empresas involucradas con las seguridad informática, demostrando así la gran aplicabilidad de la carrera Ingeniería de Sistemas en las organizaciones de nuestro medio. Este diagnostico a su vez permite a una empresa orientar un plan de seguridad conducente a reducir sus niveles de riesgo y amenazas a la información.

2. OBJETIVOS GENERALES Y ESPECÍFICOS

2.1 Objetivo General

Realizar un análisis sobre la Seguridad de la información en algunas de las organizaciones del Área Metropolitana de Medellín, que permita ver cómo normalizan, regulan y guían los criterios de seguridad adoptados en los diferentes ámbitos: Tecnológico, de Procesos, Humano y físico, delimitando los temas que serán base en el conocimiento del entorno, la recopilación de las preocupaciones de los usuarios, administradores y ejecutivos en materia de seguridad.

A partir de sus principios, mirar cuáles son los procedimientos utilizados para marcar y tratar la información, de acuerdo con el esquema de clasificación adoptado por las organizaciones, para luego analizar qué tanto varían estos procedimientos entre ellas y saber qué tanto están preparados los individuos involucrados en la gestión de la seguridad de la información para las nuevas amenazas que cada vez son más potentes.

2.2 Objetivos Específicos

- Conocer la cultura de seguridad informática organizacional de las empresas que se analizarán en el Área Metropolitana de Medellín
- Identificar la información critica de las organizaciones encuestadas
- Identificar los mecanismos y modelos empleados por las empresas para asegurar su información
- Revisar qué controles de la Norma ISO 17799 aplican, de acuerdo con la identificación de los mecanismos y modelos empleados por las organizaciones.

3. SEGURIDAD INFORMÁTICA

3.1 DEFINICIÓN DE SEGURIDAD

Empecemos por hablar de conceptos como Seguridad, cuya definición se maneja con cierto grado de incertidumbre, teniendo distinto significando para distintas personas. Esto tiene la peligrosa consecuencia de que la función de seguridad puede ser frecuentemente etiquetada como inadecuada o negligente, haciendo imposible a los responsables justificar sus técnicas ante reclamos basados en ambigüedades de conceptos y definiciones.

"La Seguridad es hoy día una profesión compleja con funciones especializadas". [1]
Como se sabe, los problemas nunca se resuelven: la energía del problema no desaparece, sólo se transforma y la "solución" estará dada por su transformación en problemas diferentes, más pequeños y aceptables. Por ejemplo: la implementación de un sistema informático puede solucionar el problema de velocidad de procesamiento, pero abrirá problemas como el de personal sobrante. Estos, a su vez, descontentos, pueden generar un problema de seguridad interno.

En el problema planteado pueden apreciarse tres figuras: [2]

1. El poseedor del valor: Protector.
2. Un aspirante: Competidor-Agresor
3. Un elemento a proteger: Valor

Luego, la Seguridad se definirá como: "Lo que tiene carácter de seguro, que está libre y exento de todo peligro, daño o riesgo" ó "La utilización de un adecuado sistema de

1 "Seguridad una Introducción". Dr Manunta, Giovanni. Consultor y Profesor de Seguridad de la Universidad. Cranfield. Revista Seguridad Corporativa. http://www.seguridadcorporativa.org

2 WEBER, R. (1999) Information Systems Control and Audit. Prentice Hall.

protección enmarcado dentro de una legislación vigente, que se vale de aspectos tecnológicos para su realización".[3]

Los competidores se pueden subdividir en:

- Competidor Interno: es aquél que piensa que el interés de la organización está por encima de sus intereses y, por lo tanto, actúa para sobreponer su interés personal, provocando daños a la organización.
- Competidor Externo: es aquél que actúa para arrebatar al poseedor lo que para él significa un valor empresarial o personal (clientes, mercado, información, etc.).

Por lo tanto, la seguridad es un problema de antagonismo y competencia. Si no existe un competidor–amenaza, el problema no es de seguridad.

3.2 ANÁLISIS DE LA IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA

Para comenzar el análisis de la Seguridad Informática, se deberá conocer un poco más a fondo lo que se pretende proteger: la Información

La palabra Información hace referencia a un conjunto ordenado de datos que es procesada por un Sistema Informático; mientras que un sistema informático se define como el "conjunto formado por las personas, computadoras (hardware y software), documentos, medios de almacenamiento digital, el entorno donde actúan y sus interacciones."[4].

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. La

3 TORRES DÍAZ, GERMAN AUGUSTO . A.B.C DE LA SEGURIDAD FÍSICA. MEDELLÍN : EDICIONES GATD, 1997. 168p. (PAPELES DE TRABAJO).

4 ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. Argentina. 1997. Página 22.

seguridad informática protege la información de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades del negocio.

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debe protegerse adecuadamente, cualquiera que sea la forma que tome o los medios por los que se comparta o almacene. La seguridad de la información se caracteriza aquí como la preservación de:

a. Su confidencialidad

La Privacidad o Confidencialidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

b. Su integridad

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que acceden al sistema sin estar autorizados.

c. Su disponibilidad

La Disponibilidad u Operatividad de la Información asegura que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo

requieran. Esto implica que la información se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria. También se debe tener implantado un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles deben establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la organización.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.
Existe información que debe o puede ser pública: puede ser visualizada por cualquier persona (por ejemplo, índice de analfabetismo en un país); y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo, antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo, reconociendo las características en la información, ya descritas.

La información también debe cumplir con las siguientes propiedades:
Tener *Control* sobre ella, que permita asegurar que sólo usuarios autorizados puedan tener acceso a la información.
La *Autenticidad* permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Cabe definir Amenaza en el entorno informático, como cualquier elemento que comprometa al sistema.

Gráfico 1 – Amenazas para la Seguridad[5]

Las amenazas pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo. Estos análisis de las amenazas ayudan a conformar políticas que garantizarán la seguridad de un sistema informático.

a. ***La Prevención (antes):*** mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal.

b. ***La Detección (durante):*** mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

c. ***La Recuperación (después):*** mecanismos que se aplican cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo, la recuperación desde las copias de seguridad (backup) realizadas.

Hay que tener presente que todas estas amenazas conllevan a un riesgo, y definiremos Riesgo como "la proximidad o posibilidad de daño sobre un bien". El riesgo puede ser aceptado, mitigado o desplazado.

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

5 HOWARD, John D. Thesis: An Analysis of security on the Internet 1989–1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995.

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

Luego, el daño es el resultado de la amenaza; aunque esto es sólo la mitad del axioma. El daño también es el resultado de la no–acción, o acción defectuosa del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza (por supuesto) pero también para la figura del protector.

Luego, el protector será el encargado de detectar cada una de las *Vulnerabilidades* (debilidades) del sistema, que pueden ser explotadas y empleadas por la amenaza para comprometerlo. También será el encargado de aplicar las contramedidas (técnicas de protección) adecuadas.

El riesgo solamente puede existir al concurrir tanto una amenaza, como determinadas condiciones de vulnerabilidad. El riesgo se crea en la interacción de amenaza con vulnerabilidad, en un espacio y tiempo particular, por lo tanto se puede decir que:

RIESGO = VULNERABILIDAD + AMENAZA

La Seguridad medirá el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir, según los especialistas, en un 100%, por lo que sólo se habla de *Fiabilidad* y se la define como

"la probabilidad de que un sistema se comporte tal y como se espera de él"[6], y se habla de Sistema Fiable en lugar de Sistema Seguro.

Luego, para garantizar que un sistema sea fiable se deberá reconocer las características ya mencionadas de Integridad, Operatividad, Privacidad, Control y Autenticidad. Se deberá conocer "qué es lo que queremos proteger", "de quién lo queremos proteger", "cómo se puede lograr esto legislativa y técnicamente", para luego concluir con la formulación de estrategias adecuadas de seguridad, tendientes a la disminución de los riesgos.
Comprender y conocer acerca de seguridad ayudará a:

- Llevar a cabo análisis sobre los Riesgos, las Vulnerabilidades, las Amenazas y las Contramedidas
- Evaluar las ventajas o desventajas de la situación
- Decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, con base en las necesidades de seguridad

Es importante remarcar que cada unas de estas técnicas parten de la premisa que no existe el 100% de seguridad esperado o deseable en estas circunstancias. Y "El único sistema totalmente seguro es aquél que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias muy bien armados y pagados. Aún así, no apostaría mi vida por él"[7].

Por lo tanto, "El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de

6 HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital – Open Publication License v.10. 2 de octubre de 2000. http://www.kriptopolis.com

7 Eugene Spafford, Professor of Computer Sciences and leading computer security expert.

la información manejada por computadora"[8] que busca la protección contra los riesgos ligados a la informática.

Contrario a lo que se piensa, este concepto no es nuevo y nació con los grandes centros de cómputos. Con el pasar de los años, y como se sabe, las computadoras pasaron de ser grandes monstruos que ocupaban salas enteras, a pequeños elementos de trabajo perfectamente ubicables sobre un escritorio de oficina. En este proceso de digitalización y miniaturización llamado "downsizing", la característica más importante que se perdió fue la seguridad.

Los especialistas de Seguridad Informática de hoy se basan en principios de aquellos antiguos MainFrames (grandes computadoras).

3.3 DE QUIÉN SE DEBE PROTEGER

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 actualmente, Julio C. Ardita[9] contesta lo siguiente:

"Los tipos de Intrusos podríamos caracterizarlos desde el punto de vista del nivel de conocimiento.

1. **Clase A:** el 80% son los nuevos intrusos, que bajan programas de Internet y prueban, están jugando, son pequeños grupitos que se juntan y dicen vamos a probar.
2. **Clase B:** es el 12%, son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, conocen cómo detectar qué sistema operativo está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.

8 ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. Argentina. 1997. Página 22.

9 ARDITA, Julio César. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. http://www.cybsec.com

3. **Clase C:** es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.
4. **Clase D:** el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

Estos intrusos utilizan diversas técnicas para quebrar los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder colarse en ella. El trabajo de los Administradores y Testers no difiere mucho de esto. En lo que sí se diferencian, y por completo, es en los objetivos: mientras que un intruso penetra en las redes para distintos fines (investigación, daño, robo, etc.), un administrador lo hace para poder mejorar los sistemas de seguridad.

3.3.1 AMENAZAS HUMANAS EXTERNAS

Existen personajes que pueden ser potenciales atacantes de los sistemas, como el personal perteneciente a la organización o personas externas.

3.3.1.1 Hacker

Un Hacker es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información, distribución de software sin costo y la globalización de la comunicación.

El concepto de hacker generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

- Un hacker es pirata. Esto no es así, ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero hacker solo obtiene esa información para su uso personal.
- Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que quien destruye información y sistemas ajenos no es el hacker sino el Cracker.

Pero entonces veamos que sí es un Hacker[10]:

1. Un verdadero Hacker es curioso y paciente. Si no fuera así, terminarían por hartarse en el intento de entrar en el mismo sistema una y otra vez, abandonando el objetivo.

2. Un verdadero Hacker no entra a un sistema para borrarlo todo o para vender lo que consiga. Quiere aprender y satisfacer su curiosidad. Esa es la única finalidad de introducirse en el sistema. Buscan dentro de un lugar en el que nunca han estado, exploran todos los pequeños rincones de un mundo diferente del que ya conocen y que les aburre. ¿Por qué destruir algo y perderse el placer de decir a los demás que estuvo en un lugar donde ellos no han estado?

3. Un Hacker es inconformista.
4. Un Hacker es discreto, es decir, que cuando entra en un sistema es para su propia satisfacción, no van por ahí cantándolo a los cuatro vientos. La mayoría de los casos de "Hackers" escuchados son en realidad "Fantasming". Esto quiere decir que si un amigo se entera que se ha entrado en cierto sistema; "el ruido de los canales de comunicación" hará que se termine sabiendo que se ha entrado en un sistema cinco veces mayor, que había destruido miles de ficheros y que había inutilizado el sistema.
5. Un Hacker disfruta con la exploración de los detalles de los sistemas programables y aprovecha sus posibilidades; al contrario de la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible.
6. Un Hacker programa de forma entusiasta (incluso obsesiva), rápido y bien.
7. Un Hacker es experto en un programa en particular, o realiza trabajos frecuentemente usando cierto programa.

10 Definición extraída y traducida del Jergon File de Eric Raymond. http://murrow.journalism.wisc.edu/jargon/jargon.html

8. Un Hacker disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa.

Ninguna definición muestra al Hacker como un criminal. En el mejor de los casos, los Hackers alteran precisamente la información en la que se sustenta la sociedad y contribuyen al flujo de la tecnología. En el peor, los Hackers pueden ser traviesos perversos o exploradores curiosos. Los Hackers NO escriben dañinos virus de computadora. Quienes lo hacen son los programadores inseguros y mediocres. Los virus dañinos están completamente en contra de la ética de los Hackers.

3.3.1.2 Crackers

Los Crackers, son personas que tienen fines maliciosos o de venganza, quieren demostrar sus habilidades pero de la manera equivocada, o simplemente personas que hacen daño solo por diversión. Los hackers opinan de ellos que son "Hackers mediocres, no demasiados brillantes, que buscan violar (literalmente "break") un sistema".

Estas personas intentan descubrir información sensible: contraseñas, acceso a redes, etc.

3.3.1.3 Phreakers

Otro personaje es el conocido como Phreaker. El Phreaking, es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software, pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.

La realidad indica que los Phreakers son Cracker de las redes de comunicación. Personas con amplios conocimientos en telefonía (a veces mayor que el de los mismos empleados de las compañías telefónicas).

3.3.1.4 Phisher

Este tipo de personas dedicaban sus esfuerzos a romper la seguridad como reto intelectual (con no tan buenas intenciones), son conocidos como delincuentes informáticos que tratan de engañar a personas para obtener información bancaria o personal, con la que puedan hacer fraude de algún tipo; entre sus actividades más usuales son: Carding – Trashing.

1. **El Carding**, es el uso (o generación) ilegitimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener los bienes realizando fraude con ellas. Se relaciona mucho con el Hacking y el Cracking, mediante los cuales se consiguen los números de las tarjetas.
2. **El Trashing**, que consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.

3.3.1.5 Ex–Empleado

Este grupo puede estar especialmente interesado en violar la seguridad de la empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes; o bien aquellos que han renunciado para pasar a trabajar en la competencia. Generalmente se trata de personas descontentas con la organización, que conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño. También han existido casos donde el ex–empleado deja Bombas Lógicas que "explotan" tiempo después de marcharse.

3.3.1.6 Curiosos

Suelen ser los atacantes más habituales del sistema. Son personas que tienen un alto interés en las nuevas tecnologías, pero aún no tienen los conocimientos ni la experiencia, básicos para considerarlos hackers o crackers. En la mayoría de los casos son estudiantes intentando penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para ellos vedada. Generalmente

no se trata de ataques de daño, pero afectan el entorno de fiabilidad y confiabilidad generado en un sistema.

3.3.1.7 Terroristas

Bajo esta definición se engloba a cualquier persona que ataca el sistema para causar daño de cualquier índole en él, como ataque de modificación de los datos de clientes entre empresa competidoras, o de servidores que albergan páginas Web, bases de datos entre partidos políticos contrarios, etc.

3.3.1.8 Intrusos Remunerados

Este es, sin duda, el grupo de atacantes más peligroso, aunque también el menos habitual. Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar "secretos" (código fuente de programas, bases de datos de clientes, información confidencial de satélites, diseño de un nuevo producto, etc.) o simplemente para dañar, de alguna manera, la imagen de la entidad atacada.

Suele darse, en grandes multinacionales donde la competencia puede darse el lujo de un gran gasto para realizar este tipo de contratos y contar con los medios necesarios para realizar el ataque.

3.3.2 AMENAZAS HUMANAS INTERNAS

Existen también los robos, sabotajes o accidentes relacionados con los sistemas informáticos, de los cuales el 70%[11] son causados por el propio personal de la organización propietaria de dichos sistemas.

Esto es realmente preocupante, ya que una persona que trabaje con el administrador, el programador o el encargado de una máquina, conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esa persona podrá ser

11 Fuente: Cybsec S.A. http://www.cybsec.com

más directo, difícil de detectar y más efectivo que el que un atacante externo pueda realizar. Dentro de este espectro podemos encontrar:

3.3.2.1 Personal Interno

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional.

Es de destacar que un simple electricista puede ser más dañino que el más peligroso de los piratas informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema. Al evaluar la situación, se verá que aquí el daño no es intencionado pero ello no está en discusión; el daño existió y esto es lo que compete a la seguridad informática.

3.4 QUÉ SE DEBE PROTEGER

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

Por hardware entendemos el conjunto de todos los sistemas físicos del sistema informático: CPU, cableado, impresoras, CD–ROM, cintas, componentes de comunicación.

El software son todos los elementos lógicos que hacen funcional al hardware: sistema operativo, aplicaciones, utilidades.

Se entiende por datos al conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos.

De los tres, los datos que maneja el sistema serán los más importantes, ya que son el resultado del trabajo realizado. Si existiera daño del hardware o del software, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar: hemos de pasar

obligatoriamente por un sistema de copias de seguridad, y aún así es difícil devolver los datos a su forma anterior al daño.

Existen multitud de amenazas y ataques que se los puede clasificar en:

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 intercepción 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.

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 los puede subdividir en cuatro categorías:

- **Interrupción:** si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
- **Intercepción:** si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
- **Modificación:** si además de conseguir el acceso consigue modificar el objeto.

• **Fabricación:** se consigue un objeto similar al original atacado, de forma que es difícil distinguirlos entre sí.

• **Destrucción:** es una modificación que inutiliza el objeto.

4. SEGURIDAD LÓGICA

La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permite acceder a ellos a las personas autorizadas para hacerlo." [12]

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que plantea la seguridad lógica son:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

12 http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

4.1 CONTROLES DE ACCESO

Estos controles pueden implementarse en el sistema operativo sobre los sistemas de aplicación en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software, de la utilización o modificaciones no autorizadas, para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo, las relacionadas con el procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Los siguientes estándares de seguridad se refieren a los requisitos mínimos de seguridad en cualquier sistema:

4.1.1 IDENTIFICACIÓN Y AUTENTIFICACIÓN

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación, al momento en que el usuario se da a conocer en el sistema, y Autenticación, a la verificación que realiza el sistema sobre esta identificación.

El Instituto Nacional de Estándares y Tecnología (NIST) propone un estándar en el control de acceso basado en roles (RBAC), donde básicamente, un rol establece un nivel entre los usuarios y los derechos de acceso, a través de un par de relaciones: asignación de roles a usuarios, y asignación de permisos y privilegios a roles. Las políticas de control de accesos basado en roles regulan el acceso de los usuarios a la

información en términos de sus actividades y funciones de trabajo, modelando de forma natural la estructura de autorización en las organizaciones.

Existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce, por ejemplo, una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
2. Algo que la persona posee, por ejemplo, una tarjeta magnética.
3. Algo que el individuo es y que lo identifica unívocamente, por ejemplo, las huellas digitales o la voz.
4. Algo que el individuo es capaz de hacer, por ejemplo, los patrones de escritura.

Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan; mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también los más costosos por lo dificultosos de su implementación eficiente.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación, según corresponda.
2. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.

3. Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema, siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera, de acuerdo con sus funciones.
4. Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo, de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.
5. Detección de actividades no autorizadas. Además de realizar auditorías o efectuar el seguimiento de los registros de transacciones, existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas de las funciones asignadas a cada una.
6. Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
7. Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos, ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea

a las aplicaciones intencionalmente. Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

4.1.2 ROLES

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

4.1.3 LIMITACIONES A LOS SERVICIOS

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

4.1.4 CONTROL DE ACCESO INTERNO

4.1.4.1 Palabras Claves (Passwords)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo, cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas, encuentra dificultoso recordarlas y probablemente las escriba o elija

palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

- **Sincronización de passwords:** consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos, en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene permiso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.
- **Caducidad y control:** este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

4.1.4.2 Encriptación

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

4.1.4.3 Etiquetas de Seguridad

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

4.1.5 CONTROL DE ACCESO EXTERNO

4.1.5.1 Dispositivos de Control de Puertos

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

4.1.5.2 Firewalls o Puertas de Seguridad

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización.

4.1.5.3 Acceso de Personal Contratado o Consultores

Debido a que este tipo de personal en general presta servicios temporales, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

4.1.5.4 Accesos Públicos

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico), deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.

5. NORMA ISO/IEC 17799

5.1 Historia de la norma ISO 17799

La norma ISO/IEC 17799 tiene su origen en una Norma Británica anterior, la BS7799, que fue elevada a estándar internacional en el año 2000.[13]

El origen del BS 7799 se remonta a la fundación del *Commercial Computer Security Center* (organismo dependiente del Departamento de Comercio e Industria del Reino Unido) en 1987.

Años más tarde fue publicada como *British Standard's guidance document, "A code of practice for information security management",* que tras un periodo de consulta pública dio forma al *British Standard Bs. 7799:1995.* Una segunda parte, *BS 7799-2:199*8, fue añadida en Febrero de 1998. Tras una extensiva revisión y otro periodo de consulta pública, que comenzó en Noviembre de 1997; la primera revisión de la norma, denominada *BS 7799: 199*9, fue publicada en Abril de 1999.

La parte 1 de la norma fue propuesta como un estándar ISO en octubre de 1999. La votación internacional fue cerrada en Agosto de 2000, y recibió la mayoría de votos requeridos. En Octubre de 2000, tras unos cambios menores, el estándar fue aprobado y publicado el 1 de Diciembre de 2000 como ISO/IEC *17799:2000*. Mientras tanto, el Comité responsable del desarrollo del BS 7799 está preparando la actualización de la Parte 2, con vistas a ser propuesta también como un estándar ISO.

13 Durante la realización del proyecto la norma ISO 17799 fue actualizada.

5.2 Qué es la Norma ISO 17799

Es la principal norma internacional de evaluación, implementación y certificación que ofrece recomendaciones de medidas de seguridad en Tecnologías de la información, para realizar la gestión de la seguridad de la información, dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización. Esta norma está basada en la norma Británica BS (British Standar 7799), que dio origen a la norma ISO/IEC 17799-1 y 17799-2.

La ISO/IEC 17799 es una guía de buenas prácticas de seguridad de la información, que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de la seguridad de la Tecnologías de la Información, sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja. Este concepto marca la diferencia con el de seguridad informática que, en la práctica, se vino convirtiendo en equivalente de seguridad de sistemas de Tecnologías Informáticas, mientras que la norma considera también los riesgos organizacionales, operacionales y físicos de una empresa, con todo lo que esto implica.

La aplicación de un marco de referencia de seguridad basado en el ISO 17799 proporciona beneficios a toda organización que lo implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la seguridad de la información.

5.3 Objetivos de la Norma ISO/IEC 17799

- Uno de los principales objetivos de la norma ISO/IEC 17799, es proteger la confidencialidad, integridad y disponibilidad de la información escrita, almacenada, y transferida.

- Otro objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.
- Otro objetivo es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad.

5.4 Diez áreas de control de ISO/IEC 17799

Estas diez áreas cubren por completo la Gestión de la Seguridad de la Información:

1. **Política de seguridad:** Se necesita una política que refleje las expectativas de la organización en materia de seguridad, a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación.
2. **Organización de la seguridad:** Sugiere diseñar una estructura de administración dentro la organización, que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes. Esta sección considera las políticas generales de la organización y detalla cómo se debe administrar la seguridad de la información dentro de la compañía. Asimismo, define cómo mantener la seguridad de las instalaciones de procesamiento de información y los activos informáticos accedidos por terceros, (proveedores, clientes, etc.).
3. **Control y clasificación de los recursos de información:** Detalla los elementos de la compañía (servidores, PCs, medios magnéticos, información impresa, documentos, etc.), que deben ser considerados para establecer un mecanismo de seguridad, manteniendo una protección adecuada, garantizando que reciban un nivel adecuado de protección. En este sentido, los activos deben ser clasificados en: confidenciales, privados, de uso interno y de uso

público. Para cada clasificación se debe implantar mecanismos adecuados de seguridad, de acuerdo con su importancia.

4. **Seguridad del personal:** Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad de la información que manejan. También determina cómo incide el papel que desempeñan los empleados como co-responsables de la seguridad de la información. En esta sección se busca minimizar los riesgos ocasionados por el personal, tales como hurto y manipulación de la información, fraudes y mal uso de la plataforma tecnológica. Su propósito es crear conciencia en los usuarios sobre los riesgos que pueden amenazar a la información, para lo cual considera mecanismos y medios para informar y capacitar periódicamente a todos los usuarios (personal interno de la compañía y personal que brinde servicios) de todas las políticas, y establecer mecanismos de prevención, identificación, notificación y corrección de posibles incidentes de seguridad.
5. **Seguridad física y ambiental:** Responde a la necesidad de proteger las áreas, los equipos y los controles generales. El objetivo principal es la prevención de accesos no autorizados a las instalaciones de la compañía, con especial atención a todos los sitios en los cuales se procesa información (centros de cómputo, PC de usuarios críticos, equipos de los proveedores de servicios, etc.), y áreas en las cuales se recibe o se almacena información (magnética o impresa) sensitiva (fax, áreas de envío y recepción de documentos, archivadores, etc.), minimizando riesgos por pérdidas de información, hurto, daño de equipos y evitando la interrupción de las actividades productivas.
6. **Manejo de las comunicaciones y las operaciones:** Define las políticas y procedimientos para asegurar la correcta operación de las instalaciones de procesamiento (servidores y equipos de comunicación). Los objetivos de esta sección se pueden enumerar como sigue:

   1. Asegurar la protección y el funcionamiento correcto de las instalaciones de procesamiento de la información.

2. Minimizar el riesgo de falla de los sistemas.

3. Proteger la integridad del software y la información.

4. Conservar la integridad y disponibilidad del procesamiento y transmisión de la información.

5. Garantizar la protección de la información en las redes y de la infraestructura de soporte.

6. Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.

7. **Control de acceso:** Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos. Asimismo, establece los diferentes tipos de accesos o privilegios a los recursos informáticos (sistema operativo, aplicaciones, correo electrónico, Internet, comunicaciones, conexiones remotas, etc.) que requiere cada empleado de la compañía y el personal externo que brinda servicios, en concordancia con sus responsabilidades. Esto permitirá identificar y evitar acciones o actividades no autorizadas, garantizando los servicios informáticos.
8. **Desarrollo y mantenimiento de los sistemas:** Establece la necesidad de implantar medidas de seguridad y aplicación de controles de seguridad en todas las etapas del proceso de desarrollo y mantenimiento de los sistemas de información. Además, considera los mecanismos de seguridad que deben implantarse en el proceso de adquisición de todos los sistemas o aplicaciones de la compañía (protección de archivos, programas, base de datos, políticas de cifrado, etc.), para prevenir pérdidas, modificaciones, o eliminación de los datos, asegurando así la confidencialidad e integridad de la información.
9. **Manejo de la continuidad del negocio:** Considera el análisis de todos los procesos y recursos críticos del negocio, y define las acciones y procedimientos a seguir en casos de fallas o interrupción de los mismos, evitando la pérdida de información y la cancelación de los procesos productivos del negocio, lo que podría provocar un deterioro de la imagen de

la compañía, una posible pérdida de clientes o incluso una dificultad severa que impida continuar operando.

10. **Cumplimiento:** Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 17799, concuerda con otras leyes, reglamentos, obligaciones contractuales o cualquier requerimiento de seguridad, tales como propiedad intelectual, auditorías, contrato de servicios, etc. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y a las consideraciones técnicas; asimismo, busca garantizar que las políticas de seguridad sean acordes con la infraestructura tecnológica de la compañía.

5.5 Ventajas del uso de la norma ISO/IEC 17799

En general, las mejores prácticas son simplemente la mejor manera de cumplir con un proceso de negocio; y a su vez, representan la manera como las compañías líderes han alcanzado ser exitosas, logrando obtener muchos beneficios y ventajas. Entre esas ventajas se tiene:

- **Aumento de los niveles de seguridad en las Organizaciones**

  La implementación de la norma permite a las Organizaciones una gestión efectiva de sus recursos de información críticos y los mecanismos de protección adecuados. Esto redundará en una reducción efectiva de los niveles de riesgo y vulnerabilidades, que en definitiva se traduce en ahorro de dinero, tiempo y en una mayor confianza y fortalecimiento de la imagen institucional.

- **Planificación de actividades**

  A través de las áreas propuestas en la norma, de los controles y subcontroles, las organizaciones pueden trazar una efectiva planificación de las actividades a desarrollar con el objetivo de hacer más seguros sus sistemas. Esto es importante pues asegura no sólo que se abarquen todas las áreas relevantes, sino también el cumplimiento de los objetivos.

- **Mejora continua**

La norma describe no solamente los aspectos necesarios a tener en cuenta en el proceso de alcance de los objetivos de seguridad esperados, sino también los criterios de revisión y mejora continua a ser utilizados para mantener los niveles de seguridad deseados.

- **Posicionamiento estratégico**

Implementar la norma permite a las organizaciones enfrentar nuevos desafíos y ampliar sus actividades y competencias de manera segura. Esto puede representar un cambio de relevancia en las perspectivas de crecimiento, en la eficiencia operativa y en la calidad de servicio brindado.

- **Cumplimiento de normativas y reglamentaciones**

En muchos sectores existen normativas y reglamentaciones respecto al tratamiento de la información, tales como las disposiciones referentes a la protección de los datos de personas. El estándar permite alinear los esfuerzos y recursos de la organización.

- **Posicionamiento en un esquema comparativo en materia de seguridad con otras organizaciones**

Permite crear un marco homogéneo para comparar con otras organizaciones el posicionamiento frente a la seguridad de la información.

5.6. Factores críticos de despliegue de las Buenas Prácticas Recogidas en la Norma ISO17799.

- La política de seguridad, objetivos y actividades que reflejen los objetivos de la organización.
- El enfoque de seguridad de la información debe ser coherente con la cultura de la organización, siendo necesarios el compromiso y el apoyo visible de la dirección. (Alta Gerencia).

5.7. Antecedentes

Según la Investigación Nacional sobre Seguridad de la Información del año 2003 en España, realizada anualmente por módulo, la política de seguridad es un punto de preocupación del mundo corporativo. Según un estudio realizado a diferentes empresas españolas de diversos sectores la gran mayoría (63%) de las empresas cuentan con una política de seguridad, en un 31% de los casos la política aún está siendo desarrollada y un 5% afirman que será elaborada en el año venidero. En el 2003, cerca del 99% de las empresas tendrían una política de seguridad implementada[14]. Algunos resultados mencionan además que:[15]

- *Las empresas de mayor capital y las de capital extranjero son las que se preocupan con el tema desde hace más tiempo.*

- *Apenas un 24% contestó que el nivel de adhesión a la política es alto, revelando que el desafío actual es aumentar la participación de los empleados.*

- *Cerca del 47% de los ejecutivos entrevistados afirman que el principal obstáculo en la implementación de la política de seguridad es la falta de conciencia de los empleados, porque con frecuencia presentan resistencia en adoptar esas prácticas."*

14 http://www.aat-ar.org/Revista_art.asp?iid=90

15 REVISTA Sistemas ACIS - Criminalidad Informática en Colombia Jul 05 2005, Jeimy José Cano Martínez

6. SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES

La seguridad informática es un área que toman en cuenta cada día más organizaciones. Actualmente el aspecto de seguridad informática es factor importante para el desarrollo y despliegue de aplicaciones, redes y plataformas tecnológicas.[16]

Cuando se habla de seguridad de la información, se asocia ésta a la implementación de soluciones tecnológicas, sin medir los costos que implica en muchas ocasiones la aplicabilidad innecesaria de las mismas, debido al desconocimiento gubernamental de los riesgos asociados a la protección de los activos críticos y necesarios.

Circunstancialmente, en el ámbito de la informática, la tecnología se encuentra muy relacionada con la protección de los sistemas de información y de las redes corporativas, consecuencia del efecto de las empresas que comercializan productos relacionados con la seguridad, con la falta de conciencia y desconocimiento de los distintos escenarios que permiten vulnerar los activos críticos de las entidades.

En la práctica, la seguridad de la información es una pieza esencial dentro del universo del gobierno de TI, por eso para pensar en adquirir seguridad efectiva, se debe lograr un equilibrio adecuado entre las áreas operativas del sector administrativo y seguridad y la tecnología asociada al entorno informático; lograr una conciencia corporativa sobre el valor de los activos y la importancia de la protección de los mismos.[17]

En la actualidad, diversas organizaciones están incrementando su éxito a partir de la comprensión de los riesgos y la explotación de los beneficios de la tecnología de la información.

16 http://cnsi.funmrd.gov.ve/cnsi/index.php

17 http://www.bsecure.com.mx/articulos.php?id_sec=58&id_art=6382

Si se considera el entorno económico como contexto primordial para las empresas y la dependencia hacia la TI como ventaja competitiva, podemos decir que ambos se encuentran directamente relacionados, por este motivo un ejecutivo no puede darse el lujo de no aplicar a la TI el nivel de compromiso que se aplica al manejo total de la empresa.

Como se ha comentado anteriormente, la TI se ha convertido en parte integral del negocio y es fundamental para apoyar, mantener y propiciar el crecimiento de las organizaciones. Consecuentemente, el manejo de la TI considera principalmente cómo las personas encargadas de dirigir una entidad, tomarán en cuenta esta actividad para la supervisión, inspección, control y dirección de la misma.

La manera de cómo se aplique la TI dentro de la entidad tendrá un alto impacto en la probabilidad de que la misma alcance su visión, misión y metas estratégicas.

Como consecuencia del ámbito de TI, la seguridad de la información, al igual que los procesos operativos del negocio, deben contar con una estrategia clara y aplicable en el mediano y largo plazo, normas y políticas que permitan gobernar sobre los recursos corporativos y procedimientos/estándares, donde los actores principales son los directivos y el escenario es la organización, sin importar su origen o posición en el mercado, dado que la materialización de un riesgo puede derivarse en un impacto significativo si el bien afectado es de gran valor para el negocio.

Por todo lo manifestado, se puede concluir que el manejo de la TI no debe ser una disciplina aislada, sino que debe convertirse en parte del manejo total de una organización, es decir, la TI necesita adoptarse como parte integral de la empresa, en lugar de convertirse como algo que se practica en un rincón aislado o como simple teoría.

Por esta razón, es necesario que el nivel Directivo / Ejecutivo de una organización promueva medidas efectivas y oportunas encaminadas a tratar estas cuestiones de alta gerencia. Por consiguiente, la dirección y la administración ejecutiva necesitan extender su manejo a la TI y proporcionar el liderazgo, procesos y estructuras de organización para asegurar que la TI sustente y amplíe los objetivos y las estrategias organizativas.

7. SEGURIDAD INFORMÁTICA EN COLOMBIA

La constante evolución de las tecnologías de cómputo y comunicaciones, acompañadas por la globalización de las economías internacionales, han llevado a las organizaciones a descubrir un sin número de oportunidades y nuevos métodos de comercialización. Con el propósito de mantenerse competitivos y de generar valores agregados en sus productos y servicios, los empresarios exigen más resultados de sus departamentos de informática y de las tecnologías disponibles a estos para así soportar nuevas y revolucionarias estrategias. Gran parte de estas estrategias se basan en la capacidad de implementar negocios electrónicos, motivo por el cual muchas empresas han desarrollado proyectos para presentar sus productos y servicios en páginas Web a través de la Internet. Esto ha generado como consecuencia la necesidad de exponer la información de una forma más abierta al público en general, generando nuevos riesgos de seguridad antes inexistentes.

El número de usuarios de la Internet, también llamados cibernautas, se continúan incrementando a pasos exponenciales, y Colombia no es la excepción. De acuerdo con estudios realizados en nuestro país, para 1998 ya contábamos con más de 130.000 cibernautas, para el año 2000 esta cifra por lo menos creció tres veces y el incremento para el 2003 era aún mayor. Hace sólo algunos pocos años, los negocios electrónicos eran un asunto prácticamente desconocido en nuestro país. Hoy en Colombia como en el resto del mundo, se han convertido en una nueva alternativa

para las empresas y han revolucionado las estrategias convencionales de mercadear e identificar nuevos clientes. Aun cuando las actividades principales de los usuarios de la Internet siguen concentradas en la búsqueda de información, las transacciones comerciales de manera electrónica han tenido un crecimiento vertiginoso, generando cambios profundos en el mercado de productos y servicios, y generando un universo de oportunidades para quienes entiendan cómo capitalizarlas a su favor. Sin embargo, y a pesar de lo expuesto anteriormente, muchos clientes, existentes y potenciales, aún no desean realizar transacciones por la Internet debido al sentimiento de inseguridad que tradicionalmente conlleva el uso de una red abierta y pública en la cual se deben enviar números de tarjeta de crédito, datos financieros, identificación y demás información personal.

Estos temores están fundamentados. La aparición de los nuevos delincuentes informáticos (hackers y crackers) y el permanente desarrollo y evolución de los virus (actualmente se tienen identificados más de 64.000 virus activos que no solo tienen la finalidad de destruir, también captan claves de acceso de las computadoras de sus víctimas y las envían al creador del virus), han generado una serie de amenazas permanentes al adecuado desempeño de las empresas que utilizan y se benefician de los avances tecnológicos en informática y de los clientes que desean hacer sus compras o negocios a través de Internet. “Internet es un barrio peligroso”.

Lamentablemente, en Colombia aún no contamos con estadísticas locales relacionadas con este tema, primordialmente porque no existe una organización que realice esta clase de estudios, y segundo porque normalmente los delitos informáticos y otras eventualidades relacionadas con la seguridad no son denunciados, debido a la posible pérdida de imagen y reputación de las empresas ante sus clientes

A pesar del crecimiento de los delitos cibernéticos, las acciones legales parecen marchar demasiado lento. En Colombia por ejemplo, el Fraude Informático no se encuentra tipificado en la ley como delito, a pesar de las últimas modificaciones al nuevo código penal. Sin embargo, paradójicamente Colombia, con la creación de La ley 527 de 1999 denominada “Ley de comercio electrónico” (que se estuvo gestando

durante casi 3 años), se ha colocado a la vanguardia de los países que han comenzado a legislar para abrir paso al desarrollo de nuevos negocios y tecnologías basadas en la Internet. Según esta ley, la legislación colombiana en materia de tecnología informática no está tan atrasada como muchos creen.[18]

De acuerdo con todo lo expuesto anteriormente y teniendo en cuenta el altísimo valor que presenta la Seguridad de Información para las organizaciones, de ser considerada un lujo, o un gasto innecesario, la Seguridad Informática se ha convertido en un eslabón vital en las estrategias del negocio. Las empresas han comenzado a entender y medir los potenciales riesgos inherentes de una débil y vulnerable estructura de seguridad. Ya entendemos que está en juego mucho más que pérdidas económicas: pérdida de confiabilidad y confidencialidad en la información por accesos no autorizados, pérdida de imagen y reputación de la empresa, responsabilidades legales, objetivos y planes futuros, posicionamiento desfavorable frente a la competencia. Todo esto puede poner en peligro la estabilidad y el futuro del negocio.

8. INVERSIONES EN TECNOLOGÍAS DE SEGURIDAD

Para combatir las implacables, cambiantes y sofisticadas amenazas, tanto internas como externas, las organizaciones invierten cada vez más en las diferentes tecnologías de seguridad informáticas. Esto no ha evitado sin embargo, que se hayan producido numerosos incidentes de seguridad informática en diferentes empresas mundiales. Las grandes organizaciones son más frecuentemente punto de mira para los atacantes, pero también disponen de mayor presupuesto para tecnologías de la información y mayor estandarización

18 REVISTA Sistemas ACIS – Aspectos legales del comercio electrónico, Marcela Álvarez, EDICIÓN No.78 JULIO - SEPTIEMBRE DE 2000

La tecnología, y en especial la seguridad informática, son como el progreso. Cuanto más avanzas, más lo anhelas y más inviertes en él. Año tras año vemos aumentar el presupuesto destinado a la seguridad, que diferentes estudios cifran en torno al 15-20% como el recomendado, en relación con la inversión total en Tecnología.

Este simple porcentaje serviría para orientar a empresas, grandes y pequeñas, sobre el volumen anual de inversión en productos de seguridad.

Nunca, tanto como ahora, se ha estimado como prioritaria la inversión en seguridad informática. Medidas al parecer tan sencillas como la autenticación segura (no compartir contraseñas y por supuesto no transmitirlas a través de medios no cifrados), o cifrado de disco duro y carpetas de red, no se encuentran establecidas más que en algunas compañías y organizaciones.

Muchas organizaciones grandes en España son pioneras en la adopción de elevadas medidas de seguridad. Además, el reciente lanzamiento del DNI electrónico coloca a este país en primera línea en cuanto a seguridad informática se refiere. El DNI electrónico como llave del PC y como motor de una relación fiable y segura con la Administración Pública, ofrece un panorama muy alentador para quienes piensan que la confianza es la clave de toda relación, ya sea a través de medios tecnológicos o no.

Se abre una nueva etapa para Internet, en la que todos sabremos quién es quién a la hora de navegar. Es el final del anonimato en la Red, ya que en un futuro muy próximo cuando alguien se conecte a su ordenador, utilizará su DNI como llave del PC y por lo tanto estaremos seguros de que esa persona es quien dice ser.

A este hecho hay que unir una mayor seguridad en las transacciones, ya que gracias al DNI electrónico podremos realizar de forma telemática muchas más gestiones que antes, como por ejemplo, solicitar una beca, presentar la Declaración de Renta, acceder a los datos de la Seguridad Social, etc.

Pero si hablamos de tema de inversión en seguridad de la información, se está hablando de inversión en seguridad de la gente y de la seguridad de la tecnología de información. Hoy día es importante saber quién es la persona que estoy contratando y

quién es la persona con quien trabajo. No solo en el momento de la contratación, sino durante su permanencia en la organización.

En la medida en que una persona crece dentro de una empresa, tiene acceso a información cada vez más sensible, y sus acciones, buenas o malas, tienen un mayor impacto dentro de la organización.

En este sentido, uno ve que las organizaciones más avanzadas en seguridad de la información claramente han enfocado esfuerzos y presupuesto en temas de seguridad de la información basada en personas, focalizando temas como conciencia de seguridad, sensibilización de la gente, que la gente esté convencida de que el tema de seguridad no es impuesto por la organización y responsabilidad sólo de unos pocos, sino que compete a todos los miembros de la organización. También es claro que las organizaciones están invirtiendo mucho más que antes en servicios y en consultoría de seguridad, y con un foco diferente, porque los firewalls u otras tecnologías, a pesar de ser una necesidad, en muchas ocasiones no dan valor agregado.

La tendencia de muchas organizaciones a comprar tecnologías de seguridad, simplemente por la buena labor comercial de los proveedores, más que por un valor para el negocio, hizo que muchos de los servicios profesionales fueran entregados de manera gratuita por proveedores de software o hardware, ya que su objetivo principal era vender tecnología.

Hoy en día las organizaciones empiezan a ser concientes de que el servicio que deben contratar debe ir más allá de la instalación de un equipo o de la misma evaluación puntual de vulnerabilidades. Aquellas organizaciones que no tienen internamente ciertos recursos especializados en seguridad, han identificado la necesidad de contar con un tercero que pueda suplir ese conocimiento para cumplir con funciones específicas de seguridad, y más importante aún, para ayudar con actividades como:

- El alineamiento de la seguridad en la organización con normas internacionales
- La definición y la asignación de roles.
- Sensibilización de personal en aspectos de seguridad.
- Obtención de información sobre la percepción de la gente de la organización sobre los temas relacionados con seguridad.

Claramente la tecnología sigue siendo más costosa que los servicios profesionales, pero también es claro que el impacto de no invertir en la gente o en servicios profesionales adecuados para gestionar la seguridad, puede revertirse después en un costo muy superior al de la tecnología misma.

Más allá del sector financiero, en las organizaciones del sector real uno ve que las prioridades de inversión tienen que ver más con volver más eficiente su producción, con mejorar la producción y sus costos asociados, y con el control de calidad del producto.

El perfil de la gente en estas organizaciones hace difícil incorporar la seguridad de la información de manera consistente, ya que sus prioridades apuntan a la productividad, lo cual puede reñir con temas como el cambio periódico de contraseñas o con cierre de sesión en los sistemas después de 30 minutos de inactividad. Igualmente, la gestión de la seguridad de la información no genera un impacto social tan alto como el que genera en organizaciones del sector financiero.

Hay que definir aspectos importantes, como educar a la alta gerencia en lo importante que es invertir en seguridad, que es un activo prácticamente intangible.

9. ANÁLISIS DE CAMPO SOBRE LA SEGURIDAD INFORMÁTICA EN ALGUNAS EMPRESAS DE MEDELLÍN

9.1 Consideraciones

Con el objetivo de obtener los datos que permitieran hacer un análisis sobre el grado de implantación de la seguridad de los sistemas de la información en las empresas entrevistadas, se preparó una encuesta, que se reproduce en los anexos de este trabajo.

Este análisis muestra de forma concreta los resultados obtenidos del estudio realizado a las empresas de distintos sectores de actividad mediante una encuesta de 40

entradas, en las que se solicitaba información sobre el nivel de implantación de las distintas recomendaciones de seguridad que hace la Norma ISO/IEC 17799.

Las preguntas de la encuesta se realizaron con ayuda del asesor del proyecto, de manera que fueran preguntas que permitieran obtener información estadística sobre el tema de seguridad dentro de las empresas, mas no información confidencial de las mismas y que en todo momento fueran preguntas íntegras que no afectaran los valores de la cultura organizacional.

Para poder llevarse a cabo la investigación de este trabajo, se hizo contacto con 10 empresas de diferentes sectores industriales, consideradas grandes, con suficiente madurez y tamaño como para disponer de un área encargada de velar por la seguridad. Para esto se realizó contacto con diferentes personas que pudieran de alguna manera facilitar un acercamiento del encuestador con las personas que tuvieran conocimiento sobre el tema de seguridad informática dentro de las mismas para diligenciar la encuesta. Con algunas empresas hubo comunicación en algún momento directamente con el encuestador y otras veces fue a través de personas colaboradoras y conocidas personalmente.
Cabe anotar que las empresas encuestadas tenían que estar dentro del Área Metropolitana de Medellín para así poder delimitar el alcance del análisis.
Las diez empresas con las que se estableció comunicación fueron: Almacenes Éxito, Empresas Publicas de Medellín, Familia Sancela S.A, Sofasa, Susalud S.A, Euroceramica S.A, Corantioquia, Orbitel, Sufinanciamiento y Vestimundo.

9.2 Metodología utilizada para la investigación práctica

El método utilizado para la realización de la investigación práctica fue realizar una encuesta predeterminada con pregunta cerradas a personas del área de seguridad de las principales organizaciones del área metropolitana. Dicha encuesta contenía temas relacionados con seguridad informática, que permitiría posteriormente hacer un

análisis para determinar cómo es el estado actual de las organizaciones del área Metropolitana en cuestión de seguridad.

Se escogió este método para la recolección de datos ya que por este medio se genera un flujo de información preciso y rápido. Además, debido a que el análisis estaba enfocado a organizaciones, este método nos permitía obtener información de una manera muy discreta, debido a que las empresas requirieren confidencialidad con la información suministrada y los participantes individuales nunca puedan ser identificados al reportar los datos. La confidencialidad de los datos suministrados por los entrevistados es una de las preocupaciones primordiales de las organizaciones. Por lo tanto, este método permitía que todos los resultados de la encuesta se presentaran en resúmenes completamente anónimos, tales como tablas y gráficas estadísticas.

La encuesta fue realizada en algunas organizaciones de forma presencial y en otras fue enviada por correo electrónico, debido a la falta de disponibilidad de tiempo por parte de los encuestados.

9.3 Encuesta realizada

Dentro de la encuesta se han incluido una seria de preguntas que son claves para conocer el estado de la seguridad de la información en las organizaciones encuestadas.

Una serie de las preguntas se refieren a aspectos generales de la organización, así como de la tecnología implantada, mecanismos que utilizan y a la situación con respecto a las recomendaciones de la Norma ISO/IEC 17799, así como los principales problemas con los que se encuentran las organizaciones para implantar dichas recomendaciones.

Es claro, que es difícil medir el estado de la seguridad de las organizaciones sólo basados en los reportes de ataques generados dentro de una infraestructura, sin

embargo éstos nos dan un buen parámetro de identificación de qué acciones hacen falta.

La encuesta está compuesta por 40 preguntas sobre los siguientes temas:

- Demografía
- Presupuestos
- Fallas de seguridad
- Herramientas y prácticas de seguridad
- Políticas de seguridad

Demografía: Esta área identifica los sectores que participan, el tamaño de la organización, el personal dedicado de tiempo completo a actividades de seguridad, la dependencia organizacional de la seguridad y los cargos de las personas que respondieron las preguntas.

Presupuestos: Esta parte muestra si las organizaciones han destinado un rubro para la seguridad informática. Permite revisar el tipo de tecnología en el que invierten y un estimado del monto de la inversión en seguridad informática.

Fallas de seguridad: Esta revisa los tipos de fallas de seguridad más frecuentes; cómo se enteran sobre ellas y a quién las notifican. Por otra parte, identificar las causas por las cuales no se denuncian y si existe la conciencia sobre la evidencia digital en la atención de incidentes de seguridad informática.

Herramientas y prácticas de seguridad informática: En este segmento de la encuesta, el objetivo es identificar las prácticas de las empresas sobre la seguridad, los dispositivos o herramientas que con más frecuencia utilizan para el desarrollo de la infraestructura tecnológica y las estrategias que utilizan las organizaciones para enterarse de las fallas de seguridad.

Políticas de seguridad: Finalmente, esta sección busca indagar sobre la formalidad de las políticas de seguridad en la organización; los principales obstáculos para lograr una adecuada seguridad; los contactos nacionales e internacionales para seguir posibles intrusos.

9.4 Situación actual de las empresas del Área Metropolitana de Medellín

Unas de las mayores preocupaciones sobre ataques informáticos que se observó en las organizaciones del área Metropolitana de Medellín fueron:

- El uso indebido del correo/Internet.
- Mensajería instantánea seguirá representando una de las mayores amenazas en la Internet.

Las empresas descuidan las medidas de protección frente a las cada vez más numerosas amenazas a sus sistemas de información, según el análisis hecho. El análisis, basado en la encuesta hecha a las empresas, revela que a pesar de que las organizaciones y sus directivos son conscientes del incremento de los riesgos a los que están expuestos sus sistemas de información que contienen información crítica para su negocio, la alta dirección no toma las medidas adecuadas para prevenirlo.

Los resultados de la encuesta muestran que la falta de concienciación en la materia por parte de los usuarios es el principal obstáculo para que la seguridad informática sea realmente eficaz.

Un 60% de los encuestados proporcionó a los empleados formación en seguridad y controles, y el 100 por ciento considera que la alta dirección en sus organizaciones percibe la seguridad informática como un tema prioritario.

Pero a pesar de la importancia de los usuarios en cuestiones relacionadas con la seguridad informática, no lo son menos los procesos y la tecnología. La encuesta también los analiza. En cuanto a los procesos, el 60 por ciento de los encuestados evalúa esporádicamente si los proveedores externos cumplen o no con los requerimientos normativos en seguridad informática.

Las organizaciones encuestadas son maduras y reconocen que el riesgo está en todas partes, dentro de la organización y en la red más extensa de empresas asociadas, proveedores, clientes y otros miembros de la línea de distribución. Estas organizaciones son líderes dentro del Área Metropolitana y reconocen su dependencia de terceras partes, sobre los que tienen menos control. Pero no le dan un alto grado de atención a la gestión del riesgo de proveedores, un proceso de asesoramiento y mitigación de los riesgos que incluye revisiones regulares de prácticas y procedimientos que apoyan los productos y servicios de los proveedores, el análisis muestra que el 50 por ciento no analiza regularmente si estos proveedores cumplen con la política de seguridad de la propia organización.

El otro aspecto evaluado en la encuesta se refiere a la tecnología. La necesidad de las empresas de aumentar la productividad y las formas competitivas de trabajar hace que proliferen tecnologías de rápido desarrollo, como por ejemplo la telefonía voz sobre IP, el código de libre distribución y los servidores virtuales. Estas tecnologías pueden incrementar potencialmente la ventaja competitiva de las empresas. Sin embargo, al mismo tiempo pueden suponer serias amenazas que deben resolverse. Las exigencias de negocio y el coste reducido de la conectividad inalámbrica están imponiendo una expansión rápida y generalizada de la tecnología móvil. Pero como estos instrumentos están fuera de la seguridad del entorno corporativo controlado, los activos informáticos y la propiedad intelectual que contienen se están convirtiendo cada vez más en la responsabilidad de unos pocos individuos, una responsabilidad que muchas empresas no han acabado aún de asumir o anticipar. Las tecnologías emergentes son una realidad muy presente en la vida de las empresas encuestadas que

compiten en un entorno de negocio sometido a cambios rápidos. De acuerdo con la encuesta, algunas empresas reconocen hasta qué punto los riesgos de la seguridad de la información son inherentes a tecnologías emergentes. Sin embargo, una de las tecnologías más preocupantes para las empresas es la memoria extraíble, la informática móvil y las redes inalámbricas.

También en cuanto a tecnología, se encontró que el 80% de las organizaciones utilizaron herramientas anti-virus para proteger sus sistemas informáticos y haber llevado a cabo pruebas de intrusiones y vulnerabilidad de forma regular.

Las organizaciones están viendo que los retos para lograr los niveles de seguridad requeridos son concienciar a los empleados, por lo tanto el 60% está implementando esta medida como seguridad de la información. Sólo el 20% de encuestados dice estar creando o actualizando las políticas de seguridad y procedimientos, mientras un 20 % hacen cambios en su arquitectura de seguridad.

Dentro del análisis se puede observar que el 100% de las organizaciones restringe el acceso a algunos sitios web por seguridad.

En general, los resultados obtenidos a través del análisis ponen de manifiesto que en un porcentaje muy elevado, las empresas del sector disponen de unos niveles de seguridad bajos.

Más adelante se presentan los resultados (en gráficas) de la encuesta por temas y algunos comentarios relacionados con los datos obtenidos.

9.5 Estadísticas Generales

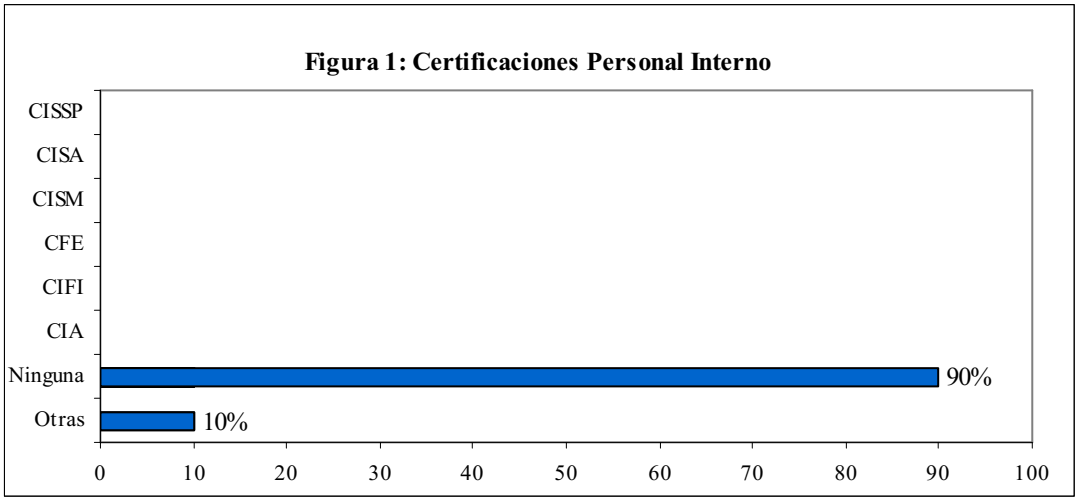
El objetivo de la parte general de la encuesta era conocer el nivel de implantación de los elementos de seguridad, los mecanismos y sistemas más habituales. En el numeral anterior se pudo apreciar algunos porcentajes generales del estado actual de las

empresas, ahora se representarán esos porcentajes en gráficas y por temas evaluados en la encuesta, para una mayor apreciación.

9.5.1 Certificaciones del Personal interno

Se ha buscado conocer el nivel de especialización que tienen las personas internas de las organizaciones que trabajan en seguridad informática con referencia a algunas de las certificaciones más importantes a nivel mundial en cuestión de la seguridad de la información como:

1. Certificado para el Profesional de la Seguridad de Sistemas de Información (CISSP)
2. Certificado de auditoría en los sistemas de información (CISA)
3. Certificación de Seguridad de la Información a Nivel Administrativo (CISM)
4. Certificado de examinador de fraude (CFE)
5. Certificado de investigador forense de la información (CIFI)



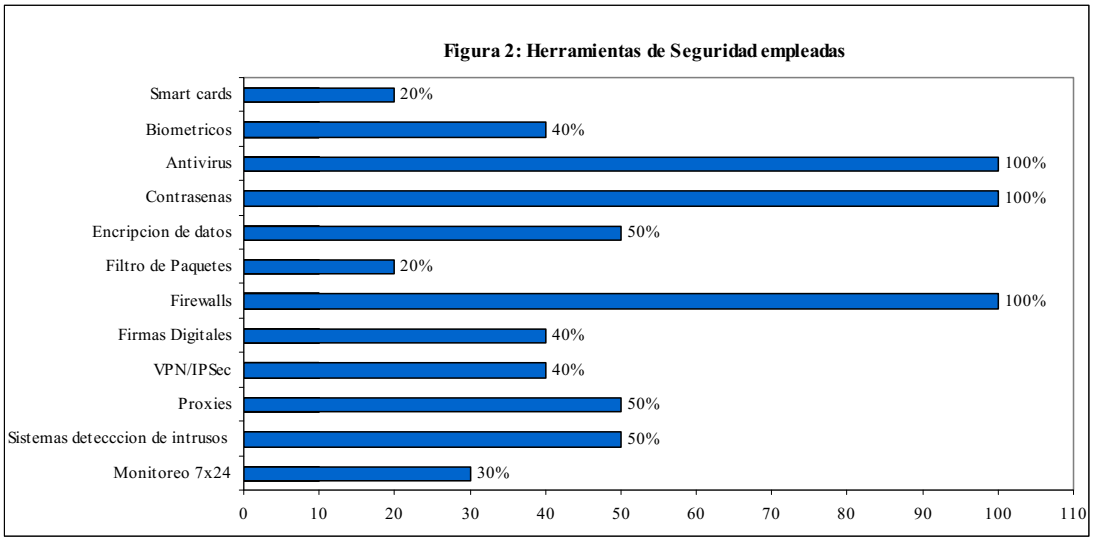
Los resultados demuestran que la situación es claramente deficiente, con un nivel de certificación inferior al 10% de las organizaciones encuestadas.

Pero vale rescatar que son concientes de la importancia y el reto que se tienen de incorporar especialistas en seguridad de la información cualificados y en adoptar y

obtener una certificación en seguridad de la información, ya que estas certificaciones ayudan a que las organizaciones tengan profesionales con habilidades necesarias para gestionar con éxito soluciones integrales, confirmando una gran experiencia y conocimiento en seguridad informática.

9.5.2 Elementos y soluciones tecnológicas de seguridad

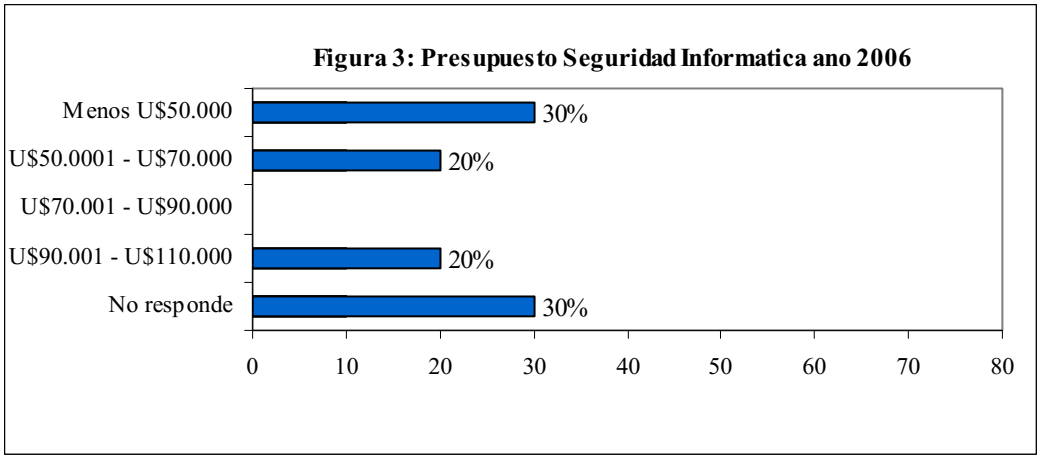
La encuesta también se ha realizado con el objeto de conocer las herramientas de seguridad que utilizan las organizaciones encuestadas, ya que esto nos da una idea de la concepción de la seguridad que tienen las mismas.



Los resultados obtenidos ponen de manifiesto, que como tecnologías de seguridad, las que más se han consolidado son los antivirus, los firewalls y las contraseñas y aunque menos, pero también, la autenticación. El resto de las soluciones de seguridad, aunque sean claramente necesarias para las organizaciones, su implantación aún no está extendida en alguna de ellas.

9.5.3 Presupuesto de Seguridad

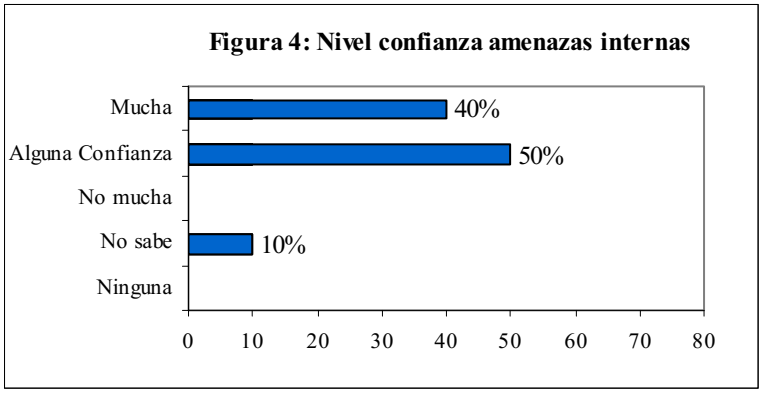
De acuerdo con el análisis, 30% de los encuestados aseguran que en el año se invierte menos de U$50.000, y manifiestan que en promedio un pequeño porcentaje del presupuesto de TI de las empresas es invertido en seguridad. Por el contrario, otros consideran prudente no contestar esta pregunta.

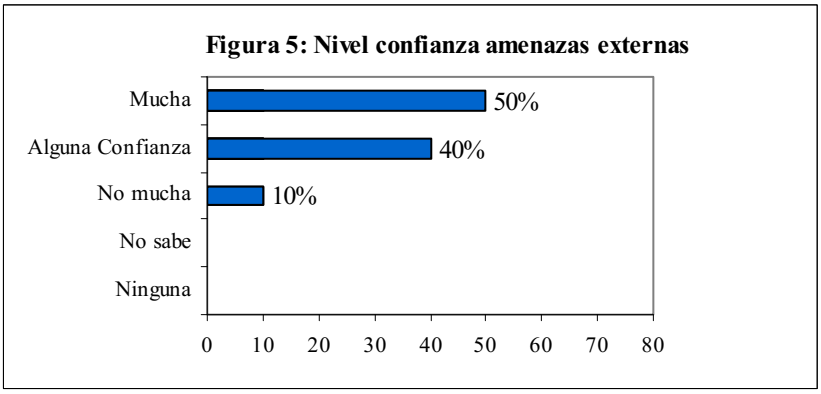


Sin embargo, es evidente que aún es necesario afinar el porcentaje destinado a estas actividades en la planificación del presupuesto, acorde con las estrategias de seguridad planteadas por las empresas.

9.5.4 Confianza en la protección

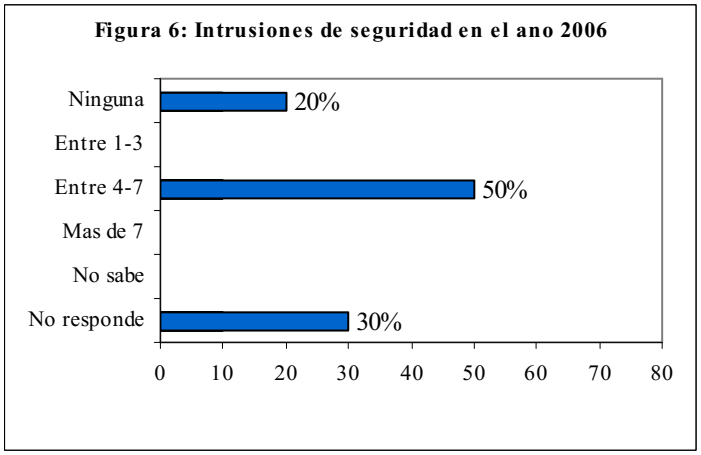
Gran porcentaje de los encuestados aseguran que los ejecutivos de TI están confiados de que sus empresas están protegidas ante las amenazas internas y externas a la seguridad. 50 % tienen “alguna confianza” de que sus empresas están protegidas ante las amenazas internas y sólo un 10 % no están muy confiados de que sus empresas están protegidas ante las amenazas externas.





9.5.5 Incidentes de seguridad

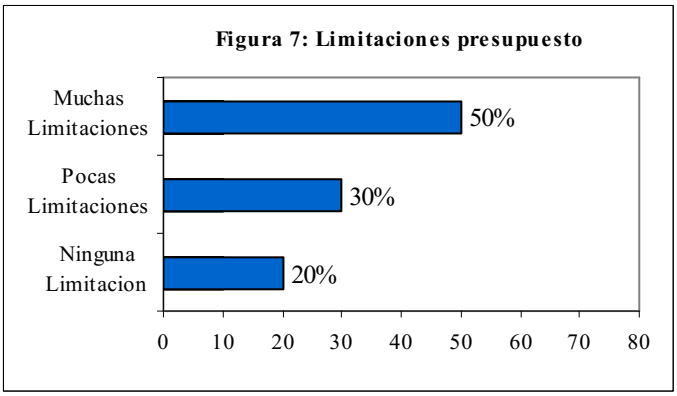
50 % de las personas encuestadas manifestaron haber sufrido un incidente o intrusión a la seguridad informática durante el último año. Entre mayor es el grado de prioridad puesto en la seguridad informática, menores posibilidades de un ataque externo, de acuerdo con las personas encuestadas.

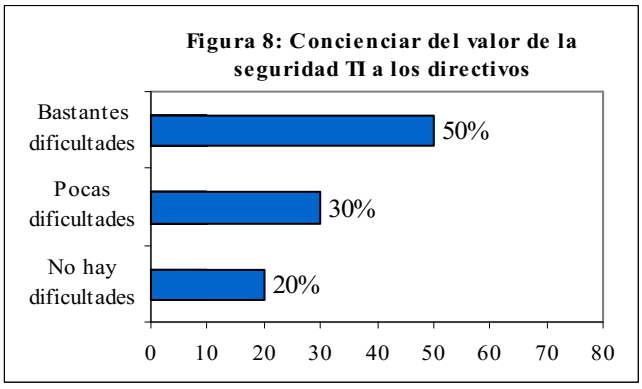


9.5.6 Retos de seguridad

Las limitaciones de presupuesto son el principal reto que enfrentan los ejecutivos de TI en materia de seguridad informática. Para el 50% de los encuestados, el presupuesto es un problema. Para el 30 % de los encuestados tienen pocas limitaciones en el presupuesto para invertir en la seguridad informática.

El segundo reto en importancia que enfrentan los ejecutivos de seguridad de sistemas, es concienciar del valor de la seguridad TI a los directivos de sus empresas. El 50% de los encuestados presenta bastantes dificultades para llevar a cabo este reto, pero sólo un 30% dice tener pocas dificultades.



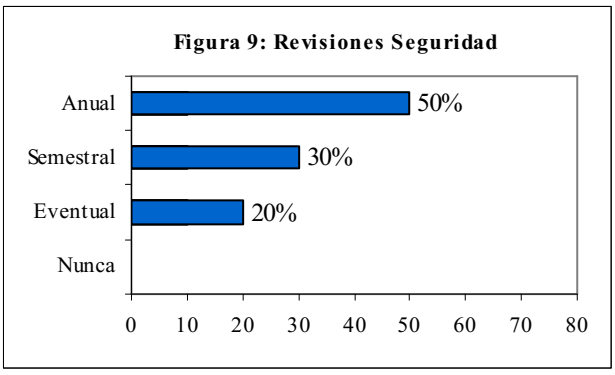


Los porcentajes muestran que la mayoría de las empresas encuestadas tienen grandes dificultades y esto es debido a que la seguridad de la información es vista muchas veces como un gasto y no como una inversión, y usualmente se aplica una vez que ya han ocurrido incidentes de cierta severidad. No obstante, la gran mayoría de las

empresas dice invertir en seguridad. El tema es en qué se invierte. Y parece ser que en ocasiones es más fácil convencer a los directivos de que se necesita adquirir tecnologías específicas de protección como firewalls y antivirus; pero no resulta tan sencillo conseguir presupuesto para invertir en consultoría, entrenamiento para el staff y servicios de soporte, y esto se debe a que no existe una real conciencia de los riesgos que implica la pérdida de la información por parte de los niveles directivos.

9.5.7 Revisiones de seguridad en los activos de la información

El panorama general ante el reto de la Seguridad de Activos de Información, indica que entre las actividades consideradas por la mayoría de las empresas se incluye la realización de evaluaciones de seguridad, al menos una vez al año. Esto da a conocer que la totalidad de empresas encuestadas están conscientes de la importancia que tiene el hecho de proteger de forma adecuada la información que poseen, y especialmente aquella que les sirve para realizar correctamente su actividad de negocio: el poder gestionar la seguridad de la información, no sólo permitirá garantizar a la propia organización que sus recursos están protegidos, sino que les aportará un grado de confianza superior al que puedan ofrecer sus competidores, convirtiéndose en un factor más de distinción en el competitivo mercado.

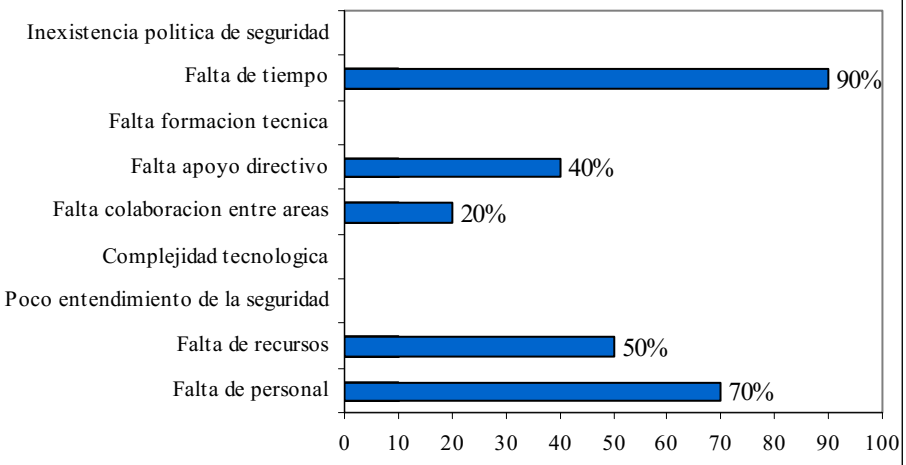


9.5.8 Obstáculos para la práctica de seguridad de informática

Existen varias barreras para la práctica de seguridad de la información, pero se observó que el 90% de las empresas bajo este análisis consideran que el mayor

obstáculo es la falta de tiempo y muy de cerca coincidieron con un 70% y 50% la falta de personal y recursos.

Figura 10: Obstaculos en la Seguridad

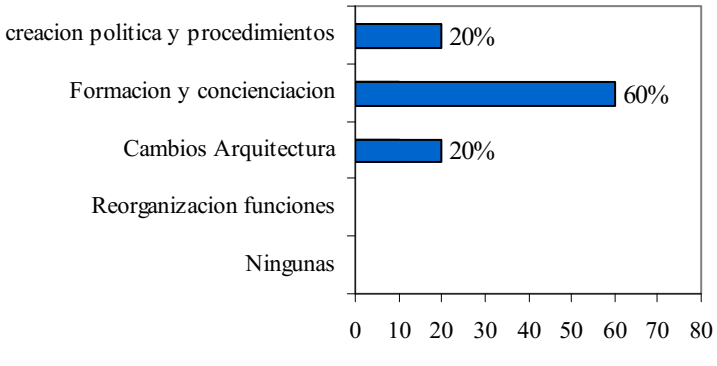


9.5.9 Medidas de seguridad implementadas por las organizaciones

Cerca del 20% de los encuestados que están implementando medidas de seguridad de la información, como resultado de tener que cumplir con regulaciones de control interno, se encaminan a la creación o actualización de políticas y procedimientos. Cerca de 60 % de estos llevan a cabo actividades de formación y concienciación.

En cambio, el 20% informa estar haciendo cambios en su arquitectura de seguridad.

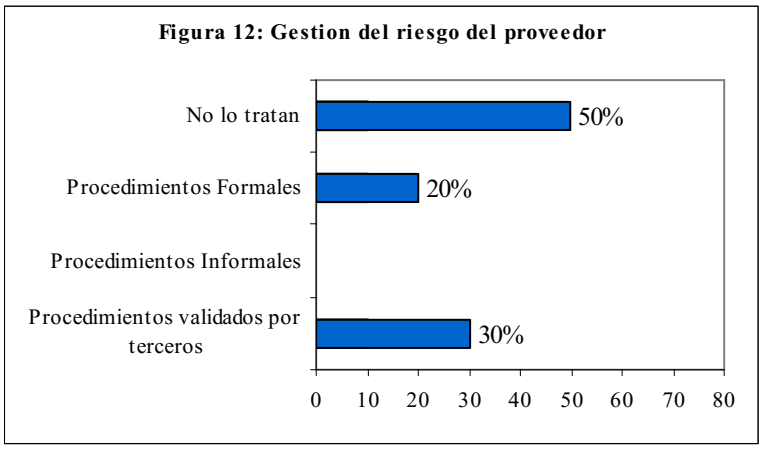
Figura 11: Medidas de Seguridad implementadas



9.5.1.0 Gestión del riesgo del proveedor

Durante el análisis se pudo observar que los procesos de la gestión del riesgo de proveedores son inmaduros e inadecuados.

Las organizaciones no exigen a terceras partes lo suficiente para que proporcionen una base viable de gestión de los riesgos en las relaciones. Un 50 % de los encuestados no nombran en absoluto el factor de la gestión del riesgo de proveedor; un 20 % informa que sólo tienen procedimientos formales para hacerlo. Y un 30% manejan procedimientos formales validados por un tercero. En el actual entorno de rápidos cambios en cuanto a riesgos, este acercamiento al contacto con terceros expone a las organizaciones a grandes riesgos que no deberían quedar sin gestionar.



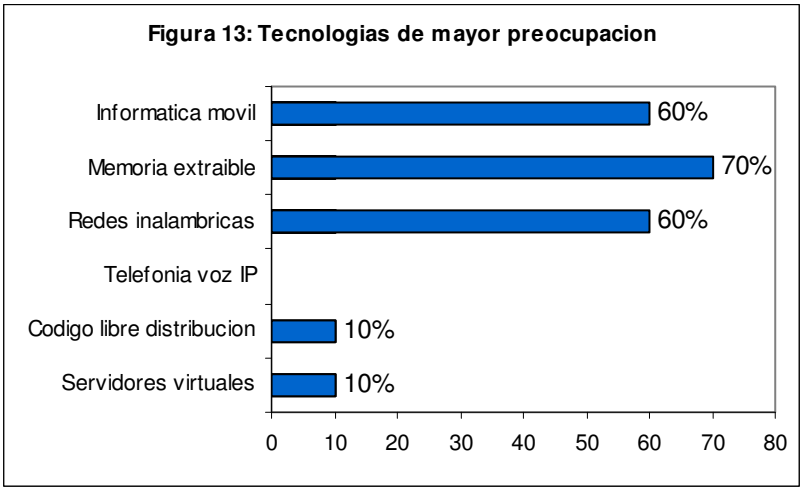
Los resultados muestran que la mayoría de las organizaciones no están dando una atención adecuada a la gestión del riesgo de proveedores.

9.5.1.1 Tecnologías de mayor preocupación en el Área de Seguridad

Más de la mitad de los encuestados reconocen los riesgos significativos en cuanto a seguridad de la información de las tecnologías móviles emergentes, incluyendo informática móvil, memoria extraíble y redes inalámbricas. Este reconocimiento sin duda refleja su extensa visibilidad y uso. Sin embargo, entre las tecnologías de rápido

desarrollo de telefonía voz sobre IP, código de libre distribución y servidores virtuales, el nivel de preocupación decae significativamente a un 0%, 10% y 10% respectivamente, a pesar de la seria amenaza que acarrean.

Figura 13: Tecnologias de mayor preocupacion



A medida que las organizaciones vayan adoptando tecnologías emergentes, necesitan ser conscientes de los riesgos asociados, como por ejemplo controles inmaduros, riesgo en la propiedad intelectual y temas de calidad. Además, deben poner en marcha en el momento adecuado las acciones para dar una solución a estos riesgos. En cuanto a tecnología móvil, aunque se reconoce por lo general como una preocupación de seguridad, no todas las empresas toman las medidas suficientes para gestionar los riesgos. Estas medidas deben empezar por reconocer que la seguridad de la información es responsabilidad de todo el mundo. Desde esta perspectiva, la comunicación de amenazas de seguridad debe fluir a la vez vertical y horizontalmente en la organización. Además, se necesitan nuevos tipos de activos y medidas distribuidas de protección. Actualmente, menos de la mitad de las organizaciones incorporan en sus planes sesiones sobre el impacto que tienen temas de seguridad de la información; menos usuarios aún reciben formación en cuanto a cómo hacer frente a incidentes de seguridad.

10. RECOMENDACIONES DE LA NORMA ISO/IEC 17799

Las recomendaciones de la norma técnica ISO/IEC 17799 son neutrales en cuanto a la tecnología. Así por ejemplo, la norma discute la necesidad de contar con firewalls, pero no profundiza sobre los tipos de firewalls y cómo se utilizan.

El enfoque está basado más en un método efectivo para diseñar, comunicar y mantener las políticas y procedimientos de seguridad, frente a las necesidades actuales como: Los usuarios necesitan políticas de seguridad claras y disponibles, los administradores necesitan técnicas de seguridad y control, los administradores de seguridad necesitan un entorno flexible para mantener y comunicar las políticas de seguridad, los recursos tecnológicos deben estar disponibles para todos los usuarios, se debe contar con métodos para garantizar la integridad, seguridad, validez y disponibilidad de la información.

En referencia a las áreas que cubre ISO/IEC 17799 se muestran algunas recomendaciones sobre las políticas de seguridad de la información propuestas por la norma ISO/IEC 17799.

10.1 Política de seguridad de la información

La gerencia de la organización debe establecer de forma clara las líneas de la política de la actuación y manifestar su apoyo y compromiso con la seguridad de la Información, publicando y manteniendo una política de seguridad en toda la organización.

- **Documento de política de seguridad de la información**

  La gerencia de las organizaciones, deben aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento que contenga la política de seguridad de la información.

- **Revisión y evaluación**

  En las organizaciones, la política de seguridad de la información debe tener un propietario que sea responsable de su mantenimiento y revisión, conforme a un proceso de revisión definido.

10.2 Organización de la Seguridad

Debe establecerse una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información.

- **Infraestructura de seguridad de la información**

  Comité de gestión de seguridad de la información

  En las organizaciones, se debe establecer o crear un Comité de Seguridad que vele por una dirección clara y el apoyo visible de la gerencia a las iniciativas de seguridad.

- **Asignación de responsabilidades para la seguridad de la información.**

  Las organizaciones deben definir claramente las responsabilidades para la protección de los activos individuales y para la ejecución de los procesos específicos de seguridad. Debe designar un propietario de cada activo de información, que se convierta así en responsable de su seguridad cotidiana.

- **Proceso de autorización de recursos para el tratamiento de la información.**

  En las organizaciones, se debe establecer un proceso de autorización para la gestión de cada nuevo recurso de tratamiento de la información que se requiera conectar a la red de la organización

- **Asesoramiento de especialista en seguridad de la información**

  En las organizaciones, se debe contar con el asesoramiento de especialistas en seguridad. Idealmente, un asesor interno experto en seguridad de la información debe proporcionar este soporte.

- **Cooperación entre organizaciones**

  En las organizaciones se deben mantener contactos con las autoridades encargadas de hacer cumplir la legislación, los organismos reguladores, los proveedores de servicios de información y los operadores de telecomunicaciones, para garantizar que se obtiene su asesoramiento y se adopta rápidamente la acción adecuada en caso de incidencia de seguridad.

10.3. Seguridad de los accesos de terceras partes

- **Identificación de riesgos por el acceso de terceros**

  Las organizaciones deben mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización cuando estos sean accedidos por terceros.

- **Requisitos de seguridad en contratos con terceros.**

  Los acuerdos que permiten el acceso de terceros a recursos de tratamiento de información en las organizaciones deben estar basados en un contrato formal que contenga o se refiera a todos los requisitos de seguridad que cumplan las políticas y normas de seguridad de la organización.

10.4. Outsourcing

- **Requisitos de seguridad en contratos de outsourcing**

Las organizaciones deben incluir en el contrato entre las partes, los requisitos de seguridad al externalizar la gestión y el control de parte o de todos sus sistemas de información, entornos de redes y terminales

10.5. Clasificación y control de activos

- **Responsabilidad sobre los activos**

  Las organizaciones deben identificar sus activos y su valor e importancia relativos, sobre la base de esta información podrán brindarse niveles de protección proporcionales a dicho valor e importancia.

  Debe establecerse y mantenerse el inventario de los activos importantes asociados con cada sistema de información.

- **Clasificación de la información**

  Guías de clasificación

  La información y los resultados de los sistemas que manejan datos clasificados de la organización deben catalogarse en relación con su valor e importancia.

  Las clasificaciones de información y otros controles de protección asociados deben tener en cuenta que el negocio necesita compartir o restringir la información, así como los impactos en la organización asociados con esas necesidades, por ejemplo, el acceso no autorizado o el daño a la información

- **Marcado y tratamiento de la información**

  La organización debe definir un conjunto adecuado de procedimientos para marcar y tratar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

10.6. Seguridad ligada al personal

- **Seguridad en la definición del trabajo y los recursos**

  Inclusión de la seguridad en las responsabilidades laborales

  Las funciones y responsabilidades sobre la seguridad de la información, de acuerdo con la política de seguridad de la organización, deben documentarse e incluirse en las responsabilidades laborales.

- **Selección y política de personal**

  La organización debe realizar comprobaciones al personal nuevo en el momento de la solicitud de trabajo de:

  - La disponibilidad de referencias satisfactorias sobre actitudes, por ejemplo, una personal y otra de la organización.
  - La comprobación (de los datos completos y precisos) de la hoja de vida del candidato.
  - La confirmación de las certificaciones académicas y profesionales.
  - Una comprobación independiente de la identificación (con pasaporte o documento similar).

- **Acuerdos de confidencialidad**

  La organización debe requerir la firma de un acuerdo de confidencialidad a los recursos humanos internos/externos o a los usuarios de terceros no cubiertos por un contrato de trabajo (que contiene cláusulas de confidencialidad) antes de su acceso a los recursos de tratamiento de información.

- **Términos y condiciones de la relación laboral**

  En la organización, los términos y las condiciones de empleo deben establecer la responsabilidad del empleado en materia de seguridad de la información.

- **Formación y capacitación en seguridad de la información**

  Todos los empleados de la organización y los usuarios de terceros, cuando corresponde, deben recibir la formación adecuada y actualizaciones regulares en las políticas y procedimientos de la organización.

- **Comunicación de las incidencias de seguridad**

  Todos los usuarios y contratados de la organización deben informar de las incidencias que afecten a la seguridad por los canales de gestión adecuados lo más rápidamente posible. Todos los empleados y contratados deben conocer el procedimiento para notificar las incidencias de seguridad e informar de ellas, tan rápido como sea posible.

- **Comunicación de las debilidades de seguridad**

  Se debe solicitar a los usuarios de los servicios de información de la organización que detecten e informen acerca de toda debilidad o amenaza observada o sospechada, respecto a la seguridad de los sistemas o servicios. Deben informar sobre estos asuntos lo más pronto posible a su propia gerencia o directamente al proveedor del servicio.

- **Comunicación de los fallos del software**

  En la organización se deben establecer procedimientos para comunicar los fallos del software.

- **Aprendiendo de las incidencias**

  En la organización se deben instalar mecanismos para cuantificar y monitorear los tipos, volúmenes y costos de las incidencias y malos funcionamientos.

- **Procedimiento disciplinario**

  En la organización, debe formalizarse un procedimiento disciplinario para los empleados que violen las políticas y procedimientos de seguridad de la organización para la retención de pruebas.

10.7. Seguridad Física y del entorno

- **Mantenimiento de equipos**

  Los equipos de la organización deben mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.

- **Seguridad de equipos fuera de los locales de la organización**

  En la organización, sólo la gerencia puede autorizar el uso de cualquier equipo para tratamiento de información fuera de los locales de la organización, sea quien sea su propietario.

- **Seguridad en la eliminación de la información**

  En la organización, la información sensible se debe destruir físicamente o sobrescribirse de manera segura y no simplemente usando la función normal de borrado.

10.8. Controles generales

- **Política de puesto de trabajo despejado y bloqueo de pantalla**

  Los usuarios de sistemas de información de la organización deben mantener siempre el puesto de trabajo libre y despejado de papeles y medios de almacenamiento removibles, para evitar el robo de información critica y la violación de la confidencialidad de la información que maneja, como información confidencial netamente laboral o claves de acceso a los sistemas a los que está autorizado. Debe bloquearse la estación y colocar un protector

de pantalla con contraseña de ser posible, con objeto de reducir los riesgos de acceso no autorizado, pérdidas o daños de la información dentro o fuera del horario normal de trabajo.

- **Extracción de pertenencias**

  En la organización, no se deben sacar de las instalaciones sin autorización los equipos, la información o el software. Cuando haya necesidad de sacar los equipos, se debe registrar su salida y su retorno. Se deben hacer controles puntuales de existencias para detectar sustracciones, de las que se advertirá al personal.

Estas fueron algunas de las recomendaciones propuestas por la norma técnica ISO/IEC 17799, teniendo en cuenta las áreas que cubre esta norma. Si una organización no ha adoptado un programa de protección definido de la información, esta norma técnica puede servir de parámetro para que lo defina, e incluso, puede servir de guía para configurar la política de seguridad de las empresas.

En general, al adoptar y mantener todas estas recomendaciones, ayudan a adquirir beneficios para las organizaciones como:

- Presentan una ventaja significativa desde la perspectiva de la seguridad y control.
- Si se utiliza un criterio estándar para la configuración y administración de los sistemas de la organización, se puede minimizar la posibilidad de que una debilidad en uno de ellos pueda comprometer los controles de acceso de los restantes, explotando sus vínculos habituales.
- Adoptando estándares, la organización puede construir una arquitectura de seguridad que permita minimizar las brechas que se puedan registrar entre las amenazas detectadas y los controles existentes, mitigando el riesgo asociado a una eventual ocurrencia de dicha amenaza.
- Se le facilita a la organización la simplificación, estandarización y automatización de los servicios de seguridad.

11. CONCLUSIONES

La seguridad informática se ha vuelto cada día más compleja para las empresas. En el estudio presentado sobre la "La Seguridad de la Información en las organizaciones del Área Metropolitana de Medellín" se ha visto que el riesgo que corren las empresas relacionado con las amenazas a la seguridad es real. Estas amenazas tienen un importante impacto no solo en las empresas del área Metropolitana de Medellín sino también en empresas de todo el mundo. Cada año se contabilizan pérdidas millonarias en las empresas debido a los numerosos ataques de virus y violaciones a la seguridad informática que sufren dichas empresas.

Hoy en día las empresas deben enfocar parte de su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se puedan traducir en pérdidas cuantiosas de dinero. Pero para protegerse ante ciertas amenazas no vasta que las empresas posean dispositivos de protección informática como firewalls o cortafuegos, sistemas de detección de intrusos, antivirus de red, dispositivos antispam y VPN, que generalmente significan inversiones considerables de dinero, sino que el funcionamiento de los mismos ha de estar marcado por la implicación de todos los departamentos y personal de la empresa.

Pero no sólo se trata de tecnología sino que se debe tener en cuenta siempre tres variables de disminución de riesgo: Tecnología, Procesos y Gente. En cada uno de estos puntos hay mucho que hacer, también considerando los niveles de confidencialidad, disponibilidad e integridad que requiere cada uno de los elementos ponderados de las funciones básicas del negocio.

En cuanto a los procesos, es importante que las empresas comiencen a entender, planear, diseñar e implementar los procesos, mecanismos y métricas necesarias que le permitan realizar el cumplimiento de regulaciones y normas. Pero se debe tener cuidado al desarrollar los procesos de seguridad sin apoyarse en los existentes en la

empresa (gestión de proyectos, incidencias, gestión del cambio y de riesgos) y comités de gestión y decisión, ya que esto puede significar una redundancia de costes importante, difícilmente asumible por parte de la propia organización. “Lo difícil no es definir los procesos de una empresa, sino relacionarlos entre ellos”,

En cuanto a las personas, los atacantes están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, en este caso es la gente, se trata de uno de los factores que ha incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el éxito de un plan de disminución de riesgos queda en manos del usuario. El cambio en la tendencia de los ataques y la táctica que aprovecha el comportamiento humano frente a las lagunas tecnológicas y de seguridad, se debe, a un serio hueco en la concienciación de los empleados en lo que se refiere a la utilización de las tecnologías de seguridad de la información. Por tanto, es imperativo que se entiendan los diferentes mecanismos de concienciación de los usuarios del por qué de los procesos, de la tecnología, etc. Estos mecanismos de comunicación de seguridad deben ser un proceso continuo, basado en la renovación de las amenazas, tendencias, medición de la efectividad, y constante verificación de que la información está siendo aplicada.

Y es que no basta con tener los últimos adelantos de TI en cuanto a seguridad de las redes, sino de llevar a cabo iniciativas de formación y concienciación a todos los niveles, incluyendo a los que aparentemente no tienen injerencia en la seguridad de la información, para evitar que se de a conocer información confidencial, pues muchas veces de ahí dependerá que se lleve a cabo un ataque directo a la información crítica del negocio, y que pueda causarle pérdidas de las cuales no se pueda fácilmente recuperar.

Las organizaciones no pueden permitirse considerar la seguridad como un proceso o un producto aislado de los demás. La seguridad tiene que formar parte de la

organización y no debe basarse en el conocimiento de un conjunto de expertos en técnicas de ataques y defensas de los activos informáticos de cada entidad.
Cada información tiene unos atributos de confidencialidad, integridad y disponibilidad, que de forma dinámica les acompañan en su ciclo de vida. Preocuparse de la seguridad en momentos puntuales (desastres, robos, virus) es, un lujo que pocas empresas se pueden permitir.
La seguridad se gestiona de forma continuada, desde el momento de la creación de la información hasta el momento de su destrucción.
Del mismo modo, el proceso de inversión por parte de las organizaciones en diferentes elementos tecnológicos de seguridad, sin que la propia organización conozca claramente aspectos como lo que está protegiendo, quién tiene acceso, la forma de tratarlo o la criticidad de disponibilidad que tiene la información, puede ser otro lujo económico para las empresas encuestadas, según las estadísticas.

En la actualidad, las inversiones en seguridad que realizan las empresas se están destinando cada vez menos exclusivamente a la compra de productos, y comienzan a destinar parte de su presupuesto a la gestión de la seguridad de la información. Las medidas que comienzan a tomar las empresas giran en torno al nuevo concepto de gestión de la seguridad de la información, es decir, un planteamiento coherente de directrices, procedimientos y criterios que permiten desde la dirección de las empresas, asegurar la evolución eficiente de la seguridad de los sistemas de Información, la organización afín y sus infraestructuras.

Para gestionar la seguridad de la información de una entidad se debe partir de una premisa fundamental y es que la seguridad absoluta no existe. Tomando como referencia esta máxima, una entidad puede adoptar alguna de las normas existentes en el mercado que establecen determinadas reglas o estándares que sirven de guía para gestionar la seguridad de la información. En el transcurso del presente trabajo se centró en una de ellas, concretamente en la norma ISO 17799, donde se nombraron algunas de sus recomendaciones. Aunque las actividades que plantea la norma no

hacen parte de un proceso inherente a la creación de una organización, sin embargo, los controles planteados pueden ser implementados y alcanzar el nivel de seguridad esperado a partir de ellos, por medio del trabajo arduo y el mejoramiento día a día.

Es bueno que las organizaciones encuestadas tengan presente que los niveles mínimos adaptables de seguridad se pueden alcanzar en las organizaciones al implementar los controles estipulados en la norma, destacando la elaboración de un plan de seguridad, integración del personal, la gestión de los activos, la implantación de controles y el desarrollo de actividades que presenten un diagnostico interno y del entorno, a partir del cual se puedan afinar los aspectos y retroalimentar la organización de sus aciertos y falencias.

De acuerdo con el análisis hecho en el presente trabajo y comparándolo con el estudio realizado a varias empresas latinoamericanas, vemos que las empresas del área metropolitana no están muy atrasadas en cuestión de seguridad informática con respecto a diferentes empresas de otros países latinoamericanas. Aunque las estadísticas muestran que las empresas de Medellín presentan riesgos y amenazas en la seguridad informática debido a la falta de implementación de medidas; también se puede notar que los incidentes de seguridad informática en las empresas latinoamericanas son muy comunes y presentan igual riesgo de ataques.

Comparativamente los encuestados dicen tener mas ataques en el Área Metropolitana (50%) que en el consolidado de las empresas estudiadas en Latinoamérica (38%), sin embargo en los últimos dichos ataques han aumentado en el 63% de las empresas, es decir, que el porcentaje tiene una tendencia al alza. Las empresas del Área Metropolitana están mas confiadas en la seguridad (40%) que las empresas en Latinoamérica (23%), siendo las más vulnerables las mexicanas y las brasileras.

En cuanto a la prioridad que representa la seguridad informática en Latinoamérica es más alta que en el Área Metropolitana, 71% y 50% respectivamente, claro que la

concienciación que hay problemas en este aspecto existe al interior de las organizaciones. Es común para las empresas de Latinoamérica y el Área Metropolitana que el presupuesto sea un problema para la seguridad informática, en ambos estudios supero el 50%, también es un problema la falta de personal ya que el 63% de las empresas Latinoamericanas no tiene un gerente de Seguridad Informática y el 70% de las empresas del Área Metropolitana reporta falta de Personal.

En general se debe generar una sensibilización a las organizaciones del Área Metropolitana para que las directivas entiendan que la seguridad informática es un factor importante dentro de la empresa y como tal se deben crear estrategias para ponerlas en marcha. El 68% de las empresas Latinoamericanas deben concienciar a las directivas de la importancia de la seguridad informática.

12. BIBLIOGRAFÍA

[1] Aguirre, Jorge, Formación en seguridad Informática, Revista Sistemas de la ACIS, 0089, 2004.

[2] Tamayo Arias, Johnny; Tamayo Alzate, Alonso, Auditoria y Seguridad Informática, Revista NOOS, 0018, 2004.

[3] Cano, Jeimy, Estado Actual de la Seguridad Informática en Colombia, Revista Sistemas de la ACIS, 0085, 2005.

[4] Asociación Española de Normalización y Certificación, Código de buenas Prácticas para la Gestión de la Seguridad de la Información, UNE-ISO/IEC 17799:2002.

[5] Sierra Brochero, Maria Claudia, Análisis de las practicas de seguridad de tecnologías de información comúnmente aceptadas y su aplicación en las pymes de Medellín, Proyecto de Grado - Pregrado, Biblioteca Eafit , 2005.

[6] (Barrientos Arcila Andrea Marcela, Areiza Cordoba Karen Alexandra), Integración de un sistema de gestión de seguridad de la información con un sistema de gestión de la calidad, Proyecto de Grado - Pregrado, Biblioteca Eafit, 2005.

[7] CANO, J. (2001). Reflexiones acerca de Estándares de Seguridad Informática. *Computerworld*. Colombia. Noviembre.

[8] BARNETT, S. (1996). Computer Security Training and Education: A Needs Analysis. *IEEE Symposium on Security and Privacy 1980 – 1999*. pág 26-27.

[9] BIBA, K. J. (1977). Integrity Considerations for Secure Computer Systems, Hanscom Field, Bedford, Mass.

[10] Gonzalo Álvarez Marañón; Pedro Pablo Pérez García; Seguridad Informática para la Empresa y Particulares, (Editorial McGraw-Hill), 2004

[11] Cano, Jeimy J, Inseguridad Informática un Concepto dual en Seguridad Informática, Revista de Ingeniería Universidad de los Andes, 2004

[12] Juan José Nombela, Seguridad Informática, Editorial Ediciones Parainfo, 1997

[13] Téllez Valdés Julio, Implicaciones de la seguridad informática, 1990

[14] Consentino, Guillermo, Tras los pasos de la seguridad perdida. Delitos informáticos, Mérida, 1998

[15] Bernal, Hernán Darío, La seguridad de la informática, 1998, p. 34-36, Revista Sicurex no.29

[16] López Franco, Nelson de Jesús, La seguridad, más que un valor agregado en los sistemas de información, Rionegro, 2005, Revista Universidad Católica de Oriente no. 19

[17] Articulo: http://www.virusprot.com/Art47.htm, BISHOP, M. (2003), Revista Computer Security. Addison Wesley. Information Assurance Technical

[18] REVISTA Sistemas ACIS - Criminalidad Informática en Colombia Jul 05 2005, Jeimy José Cano Martínez

[19] CANO, J. (2002) *Conceptos y retos de la atención de incidentes y la evidencia digital*. Revista Electrónica de Derecho Informático. Junio 2002. http://www.alfa-redi.org

[20] Revista de Ingeniería Informática del CIIRM, Análisis y gestión de riesgos de la seguridad de los sistemas de la información, por Javier Cao Avellaneda. Consultor de Seguridad de la Información, Abril 2005, No 2

[21] WEBER, R. (1999) Information Systems Control and Audit. Prentice Hall

[22] Cacho Y. (2002), "Inerme la Red Cibernética; alerta máxima de empresarios", *El Financiero*, México, D.F., septiembre 13, primera plana.

[23] Redacción de El Financiero, (2005). "Aumentan pérdidas de empresas por ataques de *hackers*", *El Financiero*, México, D.F., septiembre 22, p. 19.

[24] Piattini M. y Del Peso E. (2001). *Auditoría Informática. Un enfoque práctico*. (2ª. ed.). México: Alfaomega, p.60.

[25] Libro Seguridad de la información: protegiendo la empresa global, editorial Mc Graw Hill 2001

[26] Libro en Formato HTML y PDF de seguridad informática realizado por Antonio Villalon Huerta. http://www.rediris.es/cert/doc/unixsec/node7.html

[27] R.J. Anderson, Security Engineering - a Guide to Building Dependable, Distributed Systems, Wiley (2001) ISBN 0-471-38922-6

[28] Arango, Jorge. Memorias del Seminario de Seguridad ofrecido por Getronics (ICT Solutions and services) (2004)

[29] Primer Módulo de la Academia Latinoamericana de Seguridad Informática Unidad 1: Introducción a la Seguridad Informática

[30] Diccionario de Informática e Internet.
http://www.alegsa.com.ar/Diccionario/diccionario.php

[31] Trusted Computing Group, <http://www. trusted computing group.org/>.

[32] http://www.segu-info.com.ar/articulos/articulo27.htm

[33] http://www.monografias.com/trabajos12/fichagr/fichagr.shtml

[34] http://www.iso27000.es

[35] http://www.acis.org.co

13. ANEXO 1

ESTUDIO DE SEGURIDAD INFORMÁTICA DE EMPRESAS LATINOAMERICANAS

Empresas en Latinoamérica sufren más ataques a la seguridad informática El estudio, realizado por Kaagan Research & Associates (NY) entrevistó a 203 directores de tecnología y jefes de seguridad de empresas latinoamericanas. [19]

En el marco de un estudio realizado por la firma de investigación independiente Kaagan Research and Associates, y patrocinado por Cisco Systems e IBM, el 38% de ejecutivos entrevistados manifestaron que sus compañías habían sufrido ataques a la seguridad en el último año. En tanto, el 63% de los ejecutivos manifestaron que los riesgos en seguridad informática habían experimentado un aumento en los últimos 3 años.

Los incidentes de seguridad informática en las empresas latinoamericanas continúan aumentando al igual que el riesgo de ataques futuros, mientras disminuye la confianza de los ejecutivos de poder enfrentarlos. Esto se desprende del estudio "ActTIudes de los gerentes de TI de Latinoamérica respecto a la seguridad" realizado por la firma de investigación independiente Kaagan Research and Associates, y patrocinado por Cisco Systems e IBM.

En este contexto, 38% de los ejecutivos entrevistados manifestaron haber sufrido un ataque a la seguridad informática durante el último año, siendo las compañías mexicanas y las brasileras las más afectadas (46 y 42% respectivamente). Paralelamente, 63% de los ejecutivos entrevistados manifestaron que los riesgos en seguridad informática habían experimentado un "aumento dramático" o habían "aumentado de alguna manera" en los últimos 3 años.

[19] https://www.ciscoredaccionvirtual.com/redaccion/documentos/encseguridad.pdf

Sólo un pequeño porcentaje de ejecutivos TI entrevistados están confiados de que sus empresas están protegidas ante las amenazas internas y externas a la seguridad. 18% están "muy confiados" de que sus empresas están protegidas ante las amenazas internas y 23% están "muy confiados" de que sus empresas están protegidas ante las amenazas externas.

"La encuesta reconfirma que la seguridad de los sistemas informáticos ocupa un primerísimo lugar en las prioridades de los ejecutivos de TI de Latinoamérica", dijo Gastón Tanoira, gerente de Sistemas de Seguridad de Cisco Systems en Latinoamérica. "Sin embargo, las acciones para enfrentar estas amenazas no se corresponden con los riesgos percibidos".

"En Cisco estamos trabajando en informar y educar sobre la necesidad de contar con una arquitectura de red que identifique, prevenga y se adapte de manera proactiva y automática a las amenazas de seguridad", dijo Tanoira. "La única defensa viable a los ataques modernos de seguridad, debido a su complejidad y rapidez de expansión, es mitigar estos riesgos en la propia red. No se puede depender de dispositivos puntuales que estén en la periferia sino que la red en sí misma debe defenderse".

"Para IBM, y conforme muestra el estudio, la seguridad no es más una opción: debe estar incorporada en todo lo que hacemos. Entendemos que, para el pleno desenvolvimiento y éxito de una empresa, la seguridad precisa permear en todos los sectores. Cada elemento de seguridad depende de una integración bien hecha con la infraestructura de TI existente. Por eso, entendemos que las soluciones, las capacidades de alcance y experiencia de IBM pueden atender de forma eficiente todas las necesidades de seguridad", destacó Roberto Cruz, IBM Global Services Latinoamérica.

El estudio, realizado por Kaagan Research & Associates, firma de investigación de mercados con sede en Nueva York, entrevistó a 203 directores de tecnología y jefes de seguridad de empresas latinoamericanas, por medio de entrevistas entre agosto y septiembre de 2005. Se realizaron entrevistas a ejecutivos de Argentina (26), Chile (25), Brasil (45), Colombia (26), Venezuela (25) y México (56).

Estos fueron los principales hallazgos del estudio:

Prioridad de la seguridad informática para directivos de empresas. De acuerdo con el estudio, 71% de los directivos altos de las empresas tienen como "prioridad muy alta" o "prioridad alta" la seguridad de los sistemas TI. Mientras que en Colombia y Venezuela más del 50 % de ejecutivos entrevistados tienen como "prioridad muy alta" a la seguridad informática, en Brasil menos del 30 % de los ejecutivos altos de las empresas lo tienen como "prioridad muy alta".

Director de Seguridad TI. De acuerdo con los ejecutivos entrevistados, el 63 % de las compañías no cuentan con un gerente o director de seguridad TI. De éstas, 33 % tienen planeado contratar uno en los próximos 2 años. La probabilidad de contar con un gerente o director de seguridad es proporcional al tamaño de la compañía. 50 % de las empresas de 1.000 o más empleados cuentan con un gerente o director de seguridad TI. 37 % de las empresas con 300-1000 empleados cuentan con un gerente o director de seguridad TI y 30 % de las empresas con menos de 300 empleados cuentan con un gerente o director de seguridad TI.

Presupuesto de Seguridad. De acuerdo con el estudio, en promedio un 15.4% del presupuesto de TI de las empresas latinoamericanas es invertido en seguridad. 66 % de los entrevistados manifestaron que el presupuesto aumentó en los últimos 2 años y solo un 3% manifestó que el presupuesto disminuyó en los últimos dos años. Del presupuesto de seguridad, 51% se invierte en hardware y 49% en software.

Incidentes de seguridad. 38 % de los ejecutivos entrevistados manifestaron haber sufrido un ataque a la seguridad informática durante el último año, siendo las compañías mexicanas y las brasileras las más afectadas (46 y 42% respectivamente). 61% de los incidentes de seguridad provinieron de una fuente externa. Entre mayor es el grado de prioridad puesto en la seguridad informática menores posibilidades de un ataque externo, de acuerdo con los ejecutivos entrevistados.

Riesgos en seguridad. 63% de los ejecutivos entrevistados manifestaron que los riesgos en seguridad informática habían experimentado un "aumento dramático" o habían "aumentado de alguna manera" en los últimos 3 años. Sin embargo, es Brasil donde más ejecutivos (47 %) perciben un "aumento dramático" en los riesgos a la seguridad informática.

Confianza en la protección. Sólo un pequeño porcentaje de ejecutivos entrevistados están confiados de que sus organizaciones están protegidas frente a las amenazas internas y externas a la seguridad. 18% de los ejecutivos están confiados de que sus organizaciones están protegidas frente a las amenazas internas. La confianza en la protección ante las amenazas de seguridad decrece con el tamaño de la empresa: 8% de las compañías con 1000 o más empleados están confiados de que sus organizaciones están protegidas frente a las amenazas internas; 16% en las compañías con entre 300 a 1000 empleados y 25% en las compañías con 300 o menos empleados.

Con respecto a las amenazas externas, 23% de los ejecutivos están confiados de que sus compañías están protegidas. La confianza en la protección ante las amenazas de seguridad decrece con el tamaño de la empresa. 16% de los ejecutivos en empresas con 1000 más empleados están confiados en que sus organizaciones están protegidas frente a las amenazas externas; 24% en las compañías entre 300 y 1.000 empleados y 26% en las compañías con 300 o menos empleados.

Hackers y otras amenazas. Los hackers son la principal amenaza a los sistemas de TI de acuerdo con la opinión de los ejecutivos entrevistados. 47% de los ejecutivos entrevistados están "muy preocupados" por los hackers. Los ejecutivos de grandes compañías (1000 o más empleados) son los más preocupados (61%). La segunda preocupación en materia de seguridad son las empresas competidoras. 39 % de los entrevistados manifestaron que sus competidores son una amenaza a la seguridad de sus sistemas de TI. Esta cifra es especialmente alta en México, donde el 52% de los entrevistados considera a la competencia como una amenaza a la seguridad.

Retos de seguridad

Las limitaciones de presupuesto son el principal reto que enfrentan los ejecutivos de TI en materia de seguridad informática. Para el 80% de los entrevistados el presupuesto es un problema. Para el 42% de los entrevistados en un "problema grande" y para el 32% de los entrevistados es un "problema menor".

El segundo reto en importancia que enfrentan los ejecutivos de sistemas de seguridad, es concienciar del valor de la seguridad TI a los directivos de sus empresas (68% de los entrevistados).

ANEXO 2

ENCUESTA DE SEGURIDAD DE INFORMACIÓN

NOMBRE: _____

ÁREA: _____

EMPRESA: _____

1. ¿Cuántos empleados existen en total en su organización?
   - ☐ 1 a 50
   - ☐ 51 a 100
   - ☐ 101 a 200
   - ☐ 201 a 300
   - ☐ 301 a 500
   - ☐ 501 a 1000
   - ☐ Más de 1000

2. ¿Cuántas personas de tiempo completo o equivalente se dedican a la seguridad informática?
   - ☐ Ninguna
   - ☐ 1 a 5
   - ☐ 6 a 10
   - ☐ 11 a 15
   - ☐ Más de 15

3. Basado en la respuesta anterior, marque las certificaciones relacionadas con seguridad de la información que poseen los profesionales dedicados a estos temas.
   - ☐ Ninguna
   - ☐ CISSP - Certified Information System Security Professional
   - ☐ CISA - Certified Information System Auditor
   - ☐ CISM - Certified Information Security Manager

- [ ] CFE - Certified Fraud Examiner
- [ ] CIFI - Certified Information Forensics Investigator
- [ ] CIA - Certified Internal Auditor

Otra:

¿Cuál?

4. ¿De quién depende la responsabilidad de la seguridad informática de su organización?
   - [ ] Auditoria interna
   - [ ] Director de Seguridad Informática
   - [ ] Director Departamento de Sistemas/Tecnología
   - [ ] Gerente Ejecutivo
   - [ ] Gerente de Finanzas
   - [ ] No se tiene especificado formalmente

   Otra:

   ¿Cuál?

5. ¿Cual es su cargo en la organización?
   - [ ] Presidente/Gerente General
   - [ ] Director Ejecutivo
   - [ ] Director/Vicepresidente
   - [ ] Director/Jefe de Seguridad Informática
   - [ ] Profesional del Departamento de Seguridad Informática
   - [ ] Profesional de Departamento de Sistemas/Tecnología
   - [ ] Auditor Interno

   Otra:

   ¿Cuál?

6. ¿El presupuesto global de informática de su organización, incluye aspectos de seguridad de la información?
   - [ ] Sí
   - [ ] No

7. ¿En qué se centra el gasto de seguridad de su organización? (Elige todas las que apliquen)
   - ☐ Protección de la red
   - ☐ Proteger los datos críticos de la organización
   - ☐ Proteger la propiedad intelectual
   - ☐ Proteger el almacenamiento de datos de clientes
   - ☐ Concientización / formación del usuario final
   - ☐ Comercio/negocios electrónicos
   - ☐ Desarrollo y afinamiento de seguridad de las aplicaciones
   - ☐ Asesores de seguridad informática
   - ☐ Contratación de personal más calificado
   - ☐ Evaluaciones de seguridad internas y externas

   Otra:

   ¿Cuál?

8. ¿Cuál es el presupuesto total previsto para seguridad informática durante el 2006: gastos, hardware, software, asesorías y sueldos? (Elija una. Valores en Dólares Americanos)
   - ○ Menos de USD$50.000
   - ○ Entre USD$50.001 y USD$70.000
   - ○ Entre USD$70.001 y USD$90.000
   - ○ Entre USD$90.001 y USD$110.000
   - ○ Entre USD$110.001 y USD$130.000
   - ○ Más de USD$130.000

9. ¿Cuál es la proyección del presupuesto total previsto para seguridad informática durante el 2006: gastos, hardware, software, asesorías y sueldos?
   - ○ Menos de USD$50.000
   - ○ Entre USD$50.001 y USD$70.000
   - ○ Entre USD$70.001 y USD$90.000
   - ○ Entre USD$90.001 y USD$110.000
   - ○ Entre USD$110.001 y USD$130.000
   - ○ Más de USD$130.000

10. Durante el año anterior ¿Qué casos de violaciones de seguridad tuvieron lugar en su organización? (Elija todas las respuestas aplicables)
    - ☐ Ninguno
    - ☐ Manipulación de aplicaciones de software
    - ☐ Accesos no autorizados a la Web
    - ☐ Fraude
    - ☐ Virus
    - ☐ Robo de datos
    - ☐ Caballos de Troya
    - ☐ Monitoreo no autorizado del tráfico
    - ☐ Negación del servicio
    - ☐ Pérdida de integridad
    - ☐ Pérdida de información
    - ☐ No sabe
    - ☐ Otros:

    ¿Cuáles? _____

11. ¿Cuántas intrusiones o incidentes de seguridad identificó en promedio durante el año anterior?
    - ○ Ninguna
    - ○ Entre 1-3
    - ○ Entre 4-7
    - ○ Más de 7
    - ○ No sabe
    - ○ No responde

12. ¿Cómo se enteró de estas violaciones de seguridad? (Elija todas las aplicables)
    - ☐ Material o datos alterados
    - ☐ Análisis de registros de auditoria/sistema de archivos/registros Firewall
    - ☐ Sistema de detección de intrusos
    - ☐ Alertado por un cliente/proveedor
    - ☐ Alertado por un colega

- [ ] Seminarios o conferencias Nacionales e internacionales

Otros:

¿Cuál?

13. Una vez ocurre la violación de seguridad, ésta se notifica a: (Elija todas las aplicables)
    - [ ] Asesor legal
    - [ ] Autoridades locales/regionales
    - [ ] Autoridades nacionales
    - [ ] Equipo de atención de incidentes
    - [ ] Ninguno: No se denuncian

    Otro:

    ¿Cuál?

14. Si se decide no denunciar el incidente de seguridad, ¿cuáles son los motivos o principales preocupaciones? (Elija todas las aplicables)
    - [ ] Pérdida de valor de accionistas
    - [ ] Publicación de noticias desfavorables en los medios/pérdida de imagen
    - [ ] Responsabilidad legal
    - [ ] Motivaciones personales
    - [ ] Vulnerabilidad ante la competencia

    Otro:

    ¿Cuál?

15. ¿Su organización es consciente de que existe evidencia digital que debe ser identificada, asegurada y analizada, como parte del proceso de atención de incidentes de seguridad informática?
    - ( ) Sí
    - ( ) No

16. Durante el año anterior, ¿Cuántas pruebas de seguridad realizó su organización para valorar el estado de seguridad informática? (Elija una)
    - ( ) Una al año
    - ( ) Entre 2 y 4 al año

- Más de 4 al año
- Ninguna

17. ¿Cuáles de los siguientes mecanismos utiliza actualmente su organización para proteger sus sistemas de información? (Elija todos los aplicables)
    - Smart Cards
    - Biométricos (huella digital, iris, entre otras)
    - Antivirus
    - Contraseñas
    - Encripción de datos
    - Filtro de paquetes
    - Firewalls Hardware
    - Firewalls Software
    - Firmas digitales/certificados digitales
    - VPN/IPSec
    - Proxies
    - Sistemas de detección de intrusos
    - Monitoreo 7x24
    - Otros:

    ¿Cuáles?

18. Usted permanece informado de las fallas de seguridad de sus sistemas a través de: (Elija todas las que aplique)
    - Notificaciones de proveedores
    - Notificaciones de colegas
    - Lectura de artículos en revistas especializadas
    - Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, entre otras)
    - No se tiene este hábito.

19. ¿Qué describe mejor la política de seguridad de su organización? (Elija una)
    - No se tienen políticas de seguridad definidas

- ☐ Actualmente se encuentran en desarrollo
- ☐ Política formal, escrita documentada e informada a todo el personal

20. ¿Cuál de los siguientes es el obstáculo principal para lograr una adecuada seguridad informática en su organización?
    - ☐ Inexistencia de política de seguridad
    - ☐ Falta de tiempo
    - ☐ Falta de formación técnica
    - ☐ Falta de apoyo directivo
    - ☐ Falta de colaboración entre áreas/departamentos
    - ☐ Complejidad tecnológica
    - ☐ Poco entendimiento de la seguridad informática
    - ☐ Falta de recursos
    - ☐ Falta de personal

21. ¿Su organización (Todo el personal), reconoce la información como un activo más a proteger?
    - ☐ Sí
    - ☐ No
    - ☐ No Sabe

22. ¿Actualmente la organización posee contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de persecuciones de intrusos?
    - ☐ Sí
    - ☐ No
    - ☐ No sabe

    ¿Cuáles?

23. ¿Cuál de estos incidentes son más usuales en su Organización?
    - ☐ Infección por virus
    - ☐ Fuga de Información
    - ☐ No disponibilidad de los sistemas
    - ☐ Violación de la seguridad física

- Uso de software ilegal
- Hurto de equipos periféricos
- Uso indebido del correo/Internet
- Violación de controles de acceso a sistema
- Fraudes

24. ¿Cuáles de estas actividades de seguridad son realizadas en su Organización? ¿y cuáles son realizadas por personal externo o interno?
    - Integración y prueba de los planes de recuperación del negocio
    - Concienciación y divulgación de aspectos relacionados con la seguridad
    - Manejo de Incidentes de seguridad y análisis de vulnerabilidades
    - Evaluaciones de Seguridad
    - Seguimiento y Monitoreo de actividades
    - Administración de la seguridad
    - Configuraciones Técnicas

25. ¿Con qué frecuencia se hacen las revisiones de seguridad de activos de información?
    - Anual
    - Semestral
    - Eventual
    - Nunca

26. ¿Qué percepción tienen de la seguridad de la información en su compañía?
    - Como una tendencia
    - Como una necesidad
    - Como un factor estratégico
    - Como una evaluación de vulnerabilidades
    - Como una practica a conducir para la protección de la información
    - Como una moda

27. ¿Qué tan concientizados y capacitados están los usuarios de los riesgos a los que están expuestos sus sistemas de información?

- ☐ Mucho
- ☐ Poco
- ☐ Nada

28. ¿Han proporcionado a los empleados de la organización formación en temas de seguridad y controles?
    - ☐ Sí
    - ☐ No

29. En cuanto a los procesos, ¿Ustedes evalúan regularmente si los proveedores externos cumplen o no con los requerimientos normativos en seguridad informática?
    - ☐ Sí
    - ☐ No
    - ☐ A veces

30. En cuanto a tecnología, ¿Utilizan herramientas antivirus para proteger sus sistemas informáticos y alguna vez han llevado a cabo pruebas de intrusiones y vulnerabilidades?
    - ☐ Sí
    - ☐ No
    - ☐ A veces

31. ¿Que medidas de seguridad de la información están siendo implementadas por la organización?
    - ☐ Creación o actualización de políticas y procedimientos
    - ☐ Formación y concienciación
    - ☐ Cambios en la arquitectura
    - ☐ Reorganización de las funciones de la seguridad de la información
    - ☐ Ningunas

32. ¿Cómo la organización da respuesta a la gestión del riesgo del proveedor?
    - ☐ No lo tratan
    - ☐ Procedimientos formales

- ☐ Procedimientos informales
- ☐ Procedimientos formales validados por un tercero

33. Dentro de la organización, ¿Cuáles de las siguientes tecnologías son de mayor preocupación en el área de seguridad?
    - ☐ Informática móvil
    - ☐ Memoria extraíble
    - ☐ Redes inalámbricas
    - ☐ Telefonía voz sobre IP
    - ☐ Código de libre distribución
    - ☐ Servidores virtuales
    - ☐ Otros

¿Cuáles?

34. ¿Cómo han cambiado el nivel de riesgos de los Sistemas de Información en los últimos tres anos en su organización?
    - ☐ Aumentaron mucho
    - ☐ Se mantuvieron igual
    - ☐ Aumentaron poco
    - ☐ Disminuyeron un poco
    - ☐ Disminuyeron mucho

35. ¿Cuál es el nivel de confianza en que la organización está protegida de amenazas internas?
    - ☐ Mucha
    - ☐ Alguna confianza
    - ☐ No mucha
    - ☐ No sabe
    - ☐ Ninguna

36. ¿Cuál es el nivel de confianza en que la organización está protegida de amenazas externas?
    - ☐ Mucha
    - ☐ Alguna confianza

- ☐ No mucha
- ☐ No sabe
- ☐ Ninguna

37. ¿Tienen limitaciones de presupuesto para invertir en la seguridad informática?
    - ☐ Muchas limitaciones
    - ☐ Pocas limitaciones
    - ☐ Ninguna limitación

38. ¿Ustedes enfrentan dificultades para demostrar el valor de la seguridad de la información a los directivos de su organización?
    - ☐ Bastantes dificultades
    - ☐ Pocas dificultades
    - ☐ No hay dificultades

39. ¿Por seguridad se tiene restringido el acceso a los usuarios a algunos sitios en la Web?
    - ☐ Sí
    - ☐ No

40. ¿Cuál es el porcentaje de usuarios con acceso a un computador o ha Internet?
    - ☐ Entre el 1% y 25%
    - ☐ Entre el 25% y 50%
    - ☐ Entre el 50% y 75%
    - ☐ Entre el 75% y 100%