Facultad de Ciencias Empresariales, Departamento de Auditoria e Informática
UBB sede Chillán.

"Perfil de la mediana y gran empresa de la Ciudad de Chillán, en Seguridad y Riesgo Informático en las Áreas de Acceso Físico y Lógico"

DAMIÁN TORO - GONZALO SEPÚLVEDA
UNIVERSIDAD DEL BIO-BIO, CHILLÁN-CHILE

INDICE

TEMA	Página
Acrónimos	06
Introducción	07
CAPITULO I	
Marco Teórico y Conceptual de la Seguridad Informática.	09
1. Diagnóstico de la Seguridad informática a nivel local e internacional.	09
1.1 Los niveles de Seguridad Informática en el mundo	10
1.2. Los niveles de Seguridad Informática en el País	15
2. Seguridad Informática	16
2.1. Seguridad Física	18
2.1.1. Medidas generales de prevención que se deben considerar para lograr un Ambiente de trabajo seguro, en el ámbito de seguridad física	20
2.1.1.1. Seguridad ambiental	20
a) Incendios	21
b) Inundaciones	21
c) Catástrofes Naturales	22
d) Suministro de energía y sus instalaciones	23
d.1) UPS (Sistema de Energía Ininterrumpida)	24
2.1.1.2. Control de Acceso a las áreas criticas	25
a) Control de las personas	26
b) Utilización de guardias	26

c) Utilización de sistemas de seguridad 26

2.1.1.3. Mantención, controles y reparaciones del equipamiento 27

a) Garantías y seguros 28

b) Plan de contingencia 28

2.2. Seguridad Lógica 30

2.2.1. Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados 31

2.2.1.1. Login 31

2.2.1.2. Password 32

a) Debilidades de una password 32

b) Recomendaciones generales a los usuarios para crear una password 33

c) Recomendaciones generales a los usuarios para proteger una password 34

d) Un buen sistema que controle el acceso vía password debiera considerar lo siguiente 35

2.2.1.3. Firewall 36

a) Firewall a nivel de red 37

b) Firewall a nivel de aplicación 38

2.2.2. ¿Genios y/o Delincuentes? Lo único claro es que pueden darle a cualquiera un gran dolor de cabeza 40

2.2.2.1. Hackers 41

2.2.2.2. Crackers 42

2.2.2.3. Lammers 44

2.2.2.4. Personal de la Empresa 45

2.2.3. Legislación Chilena en delitos informáticos 47

2.2.4. Medidas de Seguridad para respaldar la información 48

2.2.4.1. Backups (copias de seguridad) 49

2.2.4.2. Mirror (servidor espejo) 51

2.2.5. Programas que protegen la información para que no sea interceptada y/o modificada 52

2.2.5.1. Antivirus 54

2.2.5.2. Virus 55

2.2.5.3. Encriptación 58

3. Conceptos básicos que sustentan esta Memoria 60

3.1. Auditoría 60

3.2. Informática 62

3.3. Auditoría Informática 63

3.3.1. Evidencia 64

3.4. Control Interno 65

3.4.1. Objetivos de Control Interno 67

4. Organismos y Normas creadas para guiar a las empresas a mejorar su Seguridad Informática 68

4.1. ISACA 68

4.1.1. COBIT 69

4.2. ISO 70

4.2.1. ISO 17799 71

CAPITULO I I

Metodología a utilizar en la evaluación de la Seguridad Informática. 73

1. Metodología de la PYMES. 75

2. Metodología de la determinación de riegos en base a riesgos importantes. 79

2.a. Determinación de la criticidad de los items a Auditar 80

2.b. Determinación de los niveles de riesgos basados en riesgos importantes 81

3. Metodología a utilizar. 84

3.1. Estándares de evaluación. 97

3.2. Técnicas de Auditoria para recopilar evidencia. 100

3.3. Fuentes de donde emana la evidencia. 103

3.4. Interpretación de los resultados. 104

4. Selección de las empresas sometidas a examen. 104

CAPITULO I I I

Aplicación de la Metodología. 107

1. Conclusiones por Empresa. 108

1.1. Empresa A 108

1.2. Empresa B 109

1.3. Empresa C 111

1.4. Empresa D 113

1.5. Empresa E 115

1.6. Empresa F 116

1.7. Empresa G 118

1.8. Empresa H 119

1.9. Empresa I 121

1.10 Empresa J 123

2. Conclusiones por Ítems. 125

2.1. Ítem 1 125

2.2. Ítem 2 126

2.3. Ítem 3 128

2.4. Ítem 4 129

2.5. Ítem 5 131

2.6. Ítem 6 132

2.7. Ítem 7 134

3. Conclusiones de una muestra de estándares claves. 136

3.1. U.P.S. 136

3.2. Firewall 137

3.3. Password 138

3.4. Copias de seguridad (Backups) 140

Conclusiones 142

Conclusiones Generales 144

Bibliografía 152

Anexos 155

ACRÓNIMOS

Con el objetivo de no repetir algunas palabras o términos nombrados en la memoria, se utilizarán para el desarrollo de esta última, algunos acrónimos, los cuales a continuación se describen:

Seg .Inf.: Seguridad Informática

S.F. : Seguridad física

S.L. : Seguridad lógica

R.I. : Riesgo informático

PCs : Computadores

A. : Auditoría

I. : Informática

A.I. : Auditoría informática

INTRODUCCIÓN

Durante el transcurso de nuestro último año en la carrera, estuvimos en la búsqueda de un tema para nuestra Memoria, el cual, fuese de alta satisfacción en términos personales y a su vez un aporte para la Carrera, Universidad y Sociedad, cuyo objetivo principal era encontrar un tema innovador, de gran auge en la actualidad y con un alto grado de desarrollo en el futuro.

Luego de investigar el historial de los proyectos realizados en la carrera, nos dimos cuenta que la mayoría apuntaba a las áreas de finanzas y tributaría, pero el tema de la Auditoría Informática era poco abordado por los estudiantes tesistas de la carrera de Auditoría, esto nos motivo a enfocarnos en este ámbito escasamente explotado y de gran importancia en el presente.

Las organizaciones que utilicen y procesen información soportada por sistemas informáticos, necesitan en forma imperiosa proteger y asegurar sus recursos contra amenazas internas y externas que pueden provocar perdidas millonarias y/o daños irreparables. Es por ello, que el tema de nuestra memoria apunta a la seguridad informática, en la cual, abordaremos las áreas de seguridad física y acceso lógico, donde a través de una Metodología (*ver página 82*) se evaluará el nivel de riesgo en Seg. Inf. en la Ciudad de Chillán. Se realizará en primer lugar una selección de las empresas, con el fin de obtener una muestra representativa de la ciudad, es preciso mencionar que esta muestra contará de 10 organizaciones lo que será explicado en forma más detallada, en el capítulo II.

La Memoria contará de una primera parte, introductoria al área de seguridad informática, definiendo y analizando conceptos claves en cuanto al tema, con el objeto de conocer, recordar y comprender lo que se quiere abordar. Luego de todo esto, se procederá a evaluar y elegir la metodología más adecuada para realizar un

diagnóstico individual a las empresas, con el objetivo de analizar la consistencia de los Sistemas informáticos en Seg. Inf. Esta metodología tendrá el carácter de estándar, es decir, se aplicará la misma a todas las empresas (*ver Capítulo II, página 82*) Estos serán analizados de tal manera que revele la situación real de cada empresa, en cuanto a la Seg. Inf. en el área física y en la parte lógica, en lo que se refiere a su acceso, para de esta forma obtener las falencias y debilidades que poseen sus sistemas de seguridad, que nos permitirá sacar conclusiones sobre el nivel de Riesgo Informático presente en su organización. Estos resultados se obtendrán mediante algunas técnicas de Auditoría, como la observación física, revisión de las salas donde manejan equipos y/o dispositivos computacionales y entrevistas directas con el personal encargado, con el objetivo de aplicar la metodología escogida.

Después de haber realizado el diagnóstico real a cada empresa, mediante la metodológica basada en estándares, los resultados de estos últimos serán tabulados en escalas, con el objetivo de interpretar la situación que presenta cada organización.

Luego de conocer el nivel de Riesgo Informático que existe en cada empresa y conociendo sus debilidades importantes que estas presentan, se les entregará un informe a cada una que contendrá las recomendaciones concretas y factibles de acuerdo a las características de cada organización, que deben considerar para mejorar su seguridad informática en los aspectos evaluados.

Así finalmente conociendo la situación de cada empresa evaluada, podremos alcanzar el objetivo esencial de la memoria, llegando a una conclusión final sobre el perfil de la mediana empresa de la ciudad de Chillán en Seg. Inf. en las áreas de acceso físico y lógico.

CAPITULO I

MARCO ACTUAL Y TEÓRICO DE LA SEGURIDAD INFORMÁTICA

1. Diagnóstico de la Seguridad Informática a nivel local e internacional

En la actualidad para muchas organizaciones, los sistemas de información basados en computadores son el corazón de las actividades cotidianas y objeto de gran consideración en la toma de decisiones. Es por ello, que de una u otra forma estamos obligados a familiarizarlos con este tema, por lo tanto, las empresas han focalizado sus esfuerzos en la creación de sistemas capaces de manejar una gran cantidad de información, que sin la ayuda de la tecnología, es prácticamente imposible la manipulación del flujo de información existente. Por ende, en el presente las empresas están tomando una mayor conciencia de que la información es uno de los activos más preciados que tienen y en consecuencia de esto, el concepto de seguridad informática a cobrado una importancia significativa para resguardar la información manejada por las instituciones. Una prueba de ello es lo ocurrido el 25 de Agosto del 2003, donde se produjo el robo de 3 discos duros de las oficinas del 3er Juzgado del Crimen de Valparaíso, en los cuales se vieron afectado tres parlamentarios del Congreso Nacional, esto puso en evidencia la mala gestión en cuanto a seguridad, lo que ratifica que no hay controles efectivos y eficaces, para contar con buen sistema de seguridad, que sin duda hubiese evitado ese robo y no es suficiente contar con avanzados sistemas y protecciones sólo referente al acceso lógico, en cuanto al acceso físico, también deben tomarse las medidas necesarias para proteger las dependencias donde se encuentran los PCs.

En el mundo se han y se están produciendo un gran número de ataques de diferente índole a diversas empresas, que cuentan con sistemas computacionales, donde se atenta a la Seg. Inf. Son muy escasos los estudios que existen y que se han hecho en el pasado en este ámbito, con el objeto de poder cuantificar y así de alguna forma valorar el problema que existe en las organizaciones, en cuanto, a la vulnerabilidad de sus sistemas y a los problemas que pueden llevar consigo. Si no se trabaja en este punto, para controlar las debilidades y si estas son detectadas por personas equivocadas, pueden acarrear graves problemas que pueden amenazar la continuidad de cualquier entidad.

Lamentablemente en los libros que se refieren a esta materia no existen estudios hechos sobre la problemática que existe en la actualidad, en cuanto a la seguridad informática a nivel empresas, pero después de una larga y angustiosa búsqueda en Internet, hemos encontrado algunas encuestas y estudios sobre el riesgo en S.I, donde se analizan varias organizaciones de diferente tamaño y pertenecientes a diversos rubros.

A continuación se expondrá los estudios encontrados y explicará gráficamente la situación que estos presentan en los distintos lugares donde se realizaron tales encuestas. Es importante aclarar que los estudios encontrados apuntan a la Seg. Inf., pero sólo en lo que se refiere a la seguridad lógica.

1.1. Los Niveles de Seguridad Informática en el mundo.

En primer lugar expondremos un estudio hecho en México por la empresa SekurelT y luego uno hecho en España por Security Center de HP.

La empresa SekureIT, Consultora en Seguridad Informática de México [1]

Desarrolló un estudio sobre la situación actual de las entidades mexicanas sobre la seguridad de sus sitios Web, el cual se analizó con diferentes pruebas, en distintos horarios, la vulnerabilidad y riesgos presentes en tales sitios. De 242 empresas, donde cada una de las Páginas Web cumple con la condición de ser sitios públicos, de acceso no restringido y las pruebas fueros en los meses de Abril a Mayo del 2001.

Primero se muestra una tabla, en la que se clasifica a las empresas por sector industrial:

Sector	Número de Entidades
Agricultura	10
Comercio	5
Comunicaciones	11
Educación	102
Energía	10
Finanzas	17
Gobiernos Estatales y Municipales	57
Secretarías de Estado	14
Turismo	10
Otras	6
TOTAL	**242**

Tabla 1. Entidades por sector

En este estudio, la vulnerabilidad se clasifica en 3 grupos: Alto Riesgo, Medio Riesgo y Bajo Riesgo, y estos van a depender de la gravedad de las consecuencias que su utilización pudiera ocasionar.

Entre las vulnerabilidades de bajo riesgo se incluyeron a aquellas que permiten la obtención de información secundaria, etc. Entre las vulnerabilidades de medio riesgo se incluyen a aquellas que permiten extraer información más relevante

[1] http://www.alfa-redi.org/upload/revista/102401--19-57-estudio.pdf

acerca del objetivo, como pueden ser, nombres de cuentas de usuario, así como las que permiten ataques que pueden comprometer parcialmente el desempeño y/o buen funcionamiento de los sitios atacados.

Finalmente, entre las vulnerabilidades de alto riesgo contemplamos las que pueden representar un compromiso total del sistema, permitiendo al atacante el control total del objetivo o al menos, impedir completamente su funcionamiento.

Una vez aplicadas las pruebas se encontraron 436 vulnerabilidades distintas, las que se exponen en la tabla 2, correspondiendo la mayor parte de ellas a medio y alto riesgo.

Tipo de Vulnerabilidad	Cantidad Encontrada	Porcentaje
Alto Riesgo	176	40.37 %
Medio Riesgo	214	49.08 %
Bajo Riesgo	46	10.55 %
TOTAL	**436**	**100%**

Tabla 2. Vulnerabilidades Encontradas

Los resultados obtenidos por este estudio muestran que: se encontró que prácticamente el 100% presenta algún tipo de vulnerabilidad y más del 50% de los sitios está en el rango de alto riesgo, mientras que apenas un 2% del total tiene bajo riesgo. A continuación, reproduciremos el gráfico que muestra con claridad los resultados.

Resultados Globales de Estudio de Vulnerabilidades

Para concluir con este estudio, se puede señalar que las cifras son categóricas, al indicar que la mayoría de las empresas sometidas a análisis tienen un alto riesgo en seguridad informática.

Volvemos a recalcar que este análisis apunta a la seguridad lógica, en cuanto al acceso vía Internet.

La empresa Security Center de HP de España. [2]

Hizo un estudio para evaluar la seguridad informática empresarial de las grandes corporaciones y la Administración Pública, tomando como referencia los entornos más críticos.

Lamentablemente él articulo donde se publica el estudio hecho por HP, no indica cuantas fueron las empresas sometidas a examen, pero lo que podemos rescatar es lo siguiente:

Fue realizado el 03 de Julio del 2003 en Madrid, tuvo una duración de una semana y la empresa firmó un contrato de confidencialidad para proteger la imagen de las empresas que se prestaron para llevar a cabo este estudio.

HP hace una clasificación de las corporaciones y las divide por sectores:

▪ Financieros	23%
▪ Telecomunicaciones	36%
▪ Industria	26%
▪ Públicos	15%
Total	100%

[2] http://www.hp.es/noticias/julio2003/noticia05.htm

Además HP definió los diferentes niveles de protección en función de los privilegios de acceso obtenidos y tiempo necesario para vulnerar los sistemas. Los dividió en:

1. Alto
2. Medio
3. Bajo

Las pruebas para penetrar en los sistemas se hicieron con un PC conectado a la Red (Internet), donde se obtuvieron los siguientes resultados:

Niveles de protección de las empresas frente a posibles ataques informáticos

- Altos 13%
- Medios 19%
- Bajos 68%

100%

Indica HP en su estudio que estas cifras ponen de manifiesto una escasa conciencia de los peligros que provoca la falta de Seg. Inf. en las compañías, con el impacto y repercusión que tiene en los negocios.

Al ser una clasificación por sector, se obtuvo que:

- El 29% de las empresas del sector financieros tienen niveles altos de seguridad
- El 10% de las Instituciones Públicas tiene niveles altos de seguridad.

- El 8% de las empresas de Telecomunicaciones tiene niveles altos de seguridad.
- El 8% de las organizaciones del sector industrial tienen niveles altos de seguridad, pero el 75% de este sector tiene bajos niveles de seguridad.

En general, la falta de conciencia acerca de la importancia de las políticas de seguridad, es un serio problema en la sociedad de las tecnologías de la Información que afecta a empresas de todos los sectores, lo que significa que hay que reforzar las estrategias de seguridad corporativa y protegerse adecuadamente de los ataques y vulnerabilidad.

Las recomendaciones de HP pasan por establecer una estrategia global, que contemple medidas efectivas como el análisis de riesgos, Auditoría Técnica, para evaluar las vulnerabilidades y una revisión continua de las políticas de seguridad.

Cabe mencionar que el estudio realizado por HP de España y el de SekureIT de México, apuntan a la Seg. Inf. en cuanto al acceso lógico vía Internet.

1.2. Los niveles de Seguridad Informática en el país.

Señores(as) Lectores lamentamos profundamente comunicarles que no hemos encontrado estudios y/o encuestas relacionadas con el tema tocado por la Memoria, ya sean hechas en nuestra ciudad, región y país, esto nos indica que aún estamos en pañales y no hemos creado una real conciencia sobre la importancia y relevancia que tiene la seguridad informática. Con lo mencionado anteriormente, podríamos decir que seremos pioneros en dar a conocer un estudio hecho en una ciudad, donde esperamos con esto incentivar a empresas para que se involucren y asimilen con más propiedad la importancia que tiene en el presente y futuro la Seg. Inf.

Una vez expuestos los estudios y dada las excusas correspondientes, continuaremos con el Capítulo, explicando y definiendo el concepto de Seg. Inf.

2. La Seguridad Informática:

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no es posible la certeza absoluta o total, el elemento de riesgo siempre esta presente, independiente de las medidas que se tomen en una organización. Debido a esto, antes de desarrollar el concepto de Seg. Inf. es preciso definir lo que es riesgo y vulnerabilidad.

Riesgo: *La probabilidad de una amenaza llegue a acaecer por una vulnerabilidad. Ejemplo: los datos estadísticos de cada evento de una base de datos de incidentes.*

Vulnerabilidad: *La situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático. Ejemplos: falta de control de acceso lógico (ver página 50), falta de control de versiones, inexistencia de un control de soportes magnéticos, falta de separación de entornos en el sistema, falta de cifrado en las telecomunicaciones, etc.* [3]

Actualmente la Seg. Inf. es cada vez más importante, pero en realidad la gran mayoría de las organizaciones no son conscientes de su relevancia, debido a que no es mirada como inversión, además la mayor parte de sus recursos se destinan a comprar tecnología de punta, porque se cree erróneamente que esa es la solución a sus problemas y es ahí donde nacen nuevos conflictos, necesitando de mejor infraestructura y recursos humanos adecuados, para poder utilizarlos de manera más eficiente y eficaz.

[3] "Auditoría Informática, Un enfoque practico", Mario Piattini y Emilio Del Peso, (pag 50)

La Seguridad Informática es definida como:

"Son medidas necesarias para llevar a cabo una protección física de las instalaciones y de los elementos electrónicos del proceso, de Seguridad Lógica y de la protección de los datos, en definitiva, de la información". [4]

Ahora bien, como dice un viejo proverbio "más vale prevenir que curar", tomando como referencia este célebre refrán, podemos decir que la Seg. Inf. es fundamental para prevenir daños ocasionados en forma accidental o intencional, y para evitar costos innecesarios. Donde el objetivo principal de esta, es resguardar la información que fluye en una empresa, para garantizar su *confidencialidad, integridad y disponibilidad* de los datos almacenados *(Ver Pág. 51 y 52)* y para ello deben de tomarse todas las medidas necesarias para alcanzar tal objetivo. Ejemplo de esto, es el de contar con un excelente antivirus el cual debe ir actualizando constantemente, porque nos va a permitir controlar que la información sea alterada por un *virus*, *(ver página 54).* Esta junto con otras medidas permitirá lograr una seguridad razonable.

Según lo estipulado por Jorge R. Nardelli,[5] la seguridad absoluta es imposible, debido a dos grandes circunstancias, la primera, debido al alto costo que tendrían las entidades si fuese factible lograr la seguridad absoluta, porque el gasto en protección sería enormemente, superior a los daños posibles. El segundo, esta relacionado directamente con el sistema operativo utilizado para soportar y manipular la información, debido a que estos no son del todo confiables, producto de que en cualquier momento estos se caen o paralizan el sistema. Además se deben hacer constantes pruebas de penetración, para ver las posibles fallas o debilidades que existen. También es conveniente mencionar que si se llegará a lograr la seguridad absoluta, la operatividad de los sistemas se verían afectados, debido a que entre mayor sea la seguridad, más aumentan las limitaciones y restricciones que se deben hacer para alcanzar ese nivel de seguridad, por ejemplo: si se quiere evitar el ingreso

[4] "Protección de los activos informáticos", José A. Labodía Bonastre, 1994, (pag. 179)

[5] "Auditoría y Seguridad de los Sistemas de Computación", (pag 299)

vía Internet de intrusos externos como: los hackers, crakers y lammer, se debe quitar la conexión a esa red para lograr la seguridad absoluta, pero esto afectaría a la empresa si está tiene entre sus metas, internacionalizar su negocio, por que necesariamente debe estar presente con una página Web. en la Internet, además en el presente todas las empresas se han visto obligadas a usar tecnología para mantenerse en el tiempo.

La Seguridad Informática se puede dividir claramente en seguridad física y lógica, debido a esto se definirán estos conceptos.

2.1. Seguridad Física

"Garantiza la integridad de los activos humanos, lógicos y materiales de un CPD. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Fallo, local o general." [6]

"Aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante las constantes amenazas a los recursos e información confidencial". [7]

La seguridad física implica el asegurar que el hardware esté seguro de desastres naturales, de un error humano, y de hurto o de vandalismo. Inconscientemente estamos relacionados con el término de S.F., por ejemplo, la practicamos en un cierto grado en nuestros hogares, porque tomamos medidas preventivas tales como: asegurando nuestras puertas y ventanas, instalando alarmas de incendio y de construir nuestros hogares lejos de un plano de inundación para asegurar que nuestras posesiones estén seguras. Obviamente, también no permitimos que los extraños caminen en nuestros hogares y que vean o lean nuestras pertenencias.

[6] "Auditoría Informática, un enfoque práctico", Mario G. Piattini y Emilio Del Peso,2001 (pag.182)
[7] http://www.cprti.com/docs/segfisica.pdf

Cuando se habla de seguridad informática, se hace más conocido o se le otorga un mayor interés al concepto de S.L. y muchas veces la S.F. es una de las áreas más olvidadas a la hora de diseñar un sistema de seguridad informático, sino que se tiene una mayor preocupación por combatir y prevenir la vulnerabilidad de hacker, cracker y lammers, etc, es decir, ataques vía Internet. Si bien algunos de los aspectos básicos de seguridad se consideran, otros como detectar a un atacante interno de la empresa, que intenta acceder físicamente a la sala donde se encuentran los equipos computacionales, son difíciles de prevenir. Esto puede derivar en que para un atacante le sea más fácil tomar y copiar una cinta o un CD que tiene la información respaldada por la empresa, que intentar acceder vía lógica a los sistemas computacionales.

Un ataque lógico al sistema de información, puede dejarlo inutilizable o sin servicio por un determinado tiempo más o menos largo, pero un ataque físico al sistema puede provocarle en algunos casos un daño irremediable.

Un ladrón que roba un PC, un incendio o un pirata que accede sin problemas a la sala de operaciones, puede hacer mucho más daño que alguien que se intenta conectar a un PC de forma no autorizada, es por eso que no sirve de nada tener los mejores y más modernos sistemas de cifrado, firewall, antivirus, etc, sino no están protegidos de buena forma los factores físicos. Por ello, es fundamental tomar en consideración el acceso físico a los equipos computacionales, es decir, tener identificada a todas las personas que tienen acceso a estos equipos y si estas personas son realmente las que deberían acceder a ellas. Además es sumamente importante que el personal encargado del manejo de los PCs sea el adecuado y tenga conciencia de tomar las medidas necesarias para una buena seguridad física.

2.1.1. Medidas generales de prevención que se deben considerar para lograr un Ambiente de trabajo seguro, en el ámbito de la Seguridad Física.

Al hablar del ambiente de trabajo nos vamos a referir a la infraestructura tangible que debe contar una determinada organización. No a la parte intangible, es decir, lo psicológico y espiritual del ambiente de trabajo, en relación, a que debe existir un ambiente agradable y armonioso para que los trabajadores se sientan a gusto, porque es material para otro análisis.

Se analizarán a tres grandes aspectos, que sin duda, son fundamentales en una seguridad física como: la seguridad ambiental; control de acceso a las áreas críticas y mantención del equipamiento. Para lograr una eficiencia y eficacia en cada uno de ellos se deben tomar medidas y procedimientos que a continuación se detallarán.

Ahora se dará a conocer la seguridad ambiental, la que a su vez se subdividirá en cinco puntos a tratar.

2.1.1.1. Seguridad ambiental

En este punto, se analizarán las condiciones y medidas que se deben tomar en cuenta, a la hora de implementar o elegir una infraestructura adecuada, para proteger los equipos computacionales encargados de soportar la información de la empresa. Estos casos que se analizan a continuación pueden ser generados por desastres provocados casual o intencionalmente y por catástrofes naturales en la evolución de nuestras vidas.

A) Incendios

La sala donde se encuentran los PCs debe ser de materiales de construcción sólidos y resistentes, además de contar con cortafuegos, también el piso, techo, paredes y puertas, deben funcionar como aislante, en caso de que se produzca un incendio desde o hacia la empresa.

En caso de fuego debe contar con detectores de humo, de calor, alarmas y extintores, los cuales deben ser del tamaño adecuado para la capacidad de la sala y encontrarse en excelente estado para recurrir a ellos en cualquier momento. Para esto deben realizarse periódicamente pruebas a los detectores y cargas a los extintores. Existen empresas que internamente tienen personal que asisten a cursos de capacitación para actuar en caso de producirse un incendio, además tienen coordinación con bomberos, para ayudar a combatir un incendio con mayor rapidez. Son dos iniciativas para tomar en cuenta y empezar a poner en práctica.

b) Inundaciones

La palabra *inundación* es definida como concepto por la Real Academia Española como: *"Acción y efecto de inundar"; "Multitud excesiva de algo".* En esta oportunidad nos referiremos a la presencia excesiva de agua, en lugares donde no debe estar o llegar.

Es importante tomar medidas acorde a las características de las condiciones climáticas de la zona donde se encuentra ubicada la empresa, por ejemplo, si la organización está establecida en una zona climática lluviosa y la calle donde se ubica se inunda cada vez que llueve, por lógica, no es aconsejable poner el servidor en el subterráneo o sótano.

Otro caso, puede ser que la inundación provenga de adentro de la organización, por ejemplo, si en el piso de arriba están ubicados los baños, la mantención de estos o el mal estado del alcantarillado, podrían provocar una inundación en menor escala, pero igual de peligrosa y dañina que una gran inundación.

c) Catástrofes Naturales

El término *catástrofe* es definido por la Real Academia Española como *"Suceso infausto que altera gravemente el orden regular de las cosas"*, si estos son provocado por la madre naturaleza, podríamos estar frente a grandes y graves problemas.

Son considerados como catástrofes naturales las: tormentas, tifones, maremotos, terremotos, tempestades, etc. Si bien el concepto de incendio e inundación podrían haberse considerado dentro de esta clasificación, no quisimos dejarlo en este punto, porque estos desastres pueden ser totalmente naturales en algunos casos, pero en otros la intervención de la mano del hombre es decisiva. Es por ello, que en este punto existe un riesgo extra del cual hay que preocuparse, que es el descuido e imprudencia de las personas, además del constante riesgo inherente que siempre existe. La idea de esto es tomar las medidas y controles adecuados, para que estos riesgos disminuyan al mínimo posible.

Es fundamental considerar la probabilidad que pueda ocasionarse o provocarse un desastre de los nombrados anteriormente. Es por esto, que al momento de que se elija la ubicación de la empresa y se decidan los materiales que se ocuparán para la construcción del edificio es muy importante y necesario tener en cuenta estos puntos, más si la zona donde se ubicará es de gran alerta a desastres.

En algunas partes del mundo están más propensos a este tipo de eventualidades y al estudiar la historia se podrían determinar y hacer estadísticas

sobre los lugares con mayor probabilidad, pero nada asegura que estamos exentos de ser afectados por una catástrofe natural. Además según la O.N.E.M.I. (Oficina Nacional de Emergencia Ministerio del Interior) en Chile la zona de la octava región se encuentra catalogada como zona amarilla, es decir, zona de alerta, por lo que se recomienda evaluar la posibilidad de contratar seguros, para que en caso de ocurrir una catástrofe natural la empresa cuente con ayuda económica para volver a construir lo que se haya perdido y así asegurar la continuidad de la empresa.

d) Suministro de energía y sus instalaciones

Tomaremos este punto dentro de la seguridad física, debido a la importancia que es recibir energía. Pero, sin duda, el cableado y las conexiones por donde proviene esta energía deben ser adecuados y seguros. Estos deben encontrarse en lugares bien protegidos para evitar que cualquier persona pueda cortarlos o manipularlos con la intención de vulnerar los sistemas y robar información de la empresa.

Además una inadecuada energía o potencia de esta, para los equipos computacionales puede provocar bajas de voltajes y hasta cortes de energía causando pérdidas de información, que puede traer como consecuencia pérdidas de tiempo y a su vez detener la producción, siendo perjudicial para la organización.

Para que funcione los PCs es imprescindible contar con una fuente de alimentación de energía continua, con el objeto de evitar la interrupción del flujo de información que maneja la organización mediante sus sistemas informáticos.

En el pasado se vivieron desagradables situaciones, porque los PCs estaban expuesto a los problemas que puede ocasionar las bajas de voltaje y las interrupciones bruscas de este servicio, debido a esto en la actualidad existen mecanismos creados para controlar estos problemas y el sistema más utilizado por la empresa, hoy en día, es instalar una UPS (Sistema de Energía Ininterrumpida). El que será definido a continuación.

d.1) UPS: (Sistema de Energía Ininterrumpida)

"UPS viene de la sigla en Ingles (Uninterrumpible Power Supply) que significa Sistema de Energía Ininterrumpida, el cuál ha sido diseñado principalmente para proteger de cortes de energía a equipos de misión crítica. Asimismo este equipo ha sido diseñado para proteger a los equipos de los problemas eléctricos más comunes. Es por esto, que existen diversas tecnologías de UPS, las cuales se diferencian por su grado de protección que otorgan cada uno". [8]

El contar con una UPS, en el presente, tiene carácter de obligatorio dada la inestabilidad con que es entrega la energía, la cual, es indispensable para hacer funcionar los equipos computacionales. La inversión que se haga en la compra de una UPS dependerá del hardware que estemos protegiendo (información critica), por ejemplo; si queremos proteger a un PC de uso personal, no necesitaremos invertir mucho, pero si se protege un servidor de una empresa, es necesario hacer un esfuerzo y adquirir la UPS más adecuada.

Una UPS protegerá al hardware y software, cuando haya una descarga eléctrica o un corte. En caso de producirse lo anterior es la UPS, quién recibe la descarga y no los equipos, porque si los equipos recibieran en forma directa ese golpe energía, es muy probable que se quemen (por lo general, es la fuente de poder de los PCs la que se quema). Protege el software porque si mientras se está utilizando un programa y es interrumpido bruscamente pueden dañarse archivos que haría que en el futuro no funcione correctamente, en cambio, la UPS dará un tiempo determinado para guardar y cerrar todo antes de cortar la energía eléctrica.

La *fuente de poder* es la pieza interna que recepciona la energía eléctrica y la distribuye a todos los componentes de un computador como el disco duro, lector de

[8] http://www.elevair.cl/potencia_resp1.htm

CD, disqueteras, etc. Por lo general se ubica en la parte posterior del CPU o también conocido como procesador.

En el mercado se venden tres tipos de UPS, dependiendo del modo de funcionamiento, si se quiere profundizar en como opera cada una de ellas se recomienda visitar la página Web. que se hace referencia en este párrafo y son las siguientes*:* [9]

1. UPS Off Line o Standby
2. UPS Interactiva
3. UPS On Line

El costo de una UPS dependerá del tiempo que dure entregando energía una vez interrumpida, así encontramos UPS que dan algunos minutos y otras hasta una o dos horas antes de que se corte la corriente.

2.1.1.2. Control de Acceso a las áreas críticas.

Es controlar el acceso de quienes ingresan a las salas en donde se encuentran los equipos y dispositivos computacionales, con el objetivo de proteger los activos de las organizaciones. Este control es muy importante en toda organización, puesto que cualquier ingreso de persona(s) no autorizadas puede provocar un daño muy costoso para la empresa y muchas veces este daño puede ser irreparable. Para controlar este acceso y con el fin de que ingresen sólo personas autorizadas, se utilizarán una serie de medidas y diversos procedimientos.

[9] http://www.avp-ar.com.ar/arqco055/derecho/consejos/derecho_consejos_ups02.htm

a) Control de las personas.

Debe existir un control de identificación y tiempo de las personas que ingresan a las salas de computación. Para ello, es fundamental un registro de visitas, las cuales deben ingresar previa autorización. Aquí la persona que ingresa a la sala en donde se encuentran los equipos debe estar autorizado o en caso de que esta persona ingrese ocasionalmente, esta última debe contar con una credencial para su autorización de ingresar.

b) Utilización de guardias.

Es conveniente considerar cuando se cuente con los medios económicos necesarios, la utilización de guardias de seguridad para la vigilancia de las áreas, porque éstos son de gran utilidad para controlar el acceso de personas a las salas de cómputo, debido a que se pueden ubicar en lugares estratégicos para cumplir sus objetivos. La principal desventaja que presenta esta técnica es que el guardia puede ser sobornado por una tercera persona para obtener información o acceso a lugares en donde no está autorizado.

En muchas organizaciones el costo de este elemento es demasiado elevado para sus características y el uso de guardias de seguridad no se hace necesario, puesto que el número de equipos que posee la empresa es pequeño.

c) Utilización de sistemas de seguridad.

En lo posible se debe contar con una cámara de vigilancia o circuitos cerrados de televisión. Las cámaras deben ubicarse en sectores estratégicos, que permitan tener vigiladas las áreas donde se encuentran los PCs, los que contienen la información más relevante de la empresa.

La información obtenida por las cámaras debe estar respaldadas en cassette u cualquier otro formato, y estos deben resguardarse en un lugar seguro. Lo ideal es que este lugar fuese una caja fuerte, a la cual, debe tener acceso sólo el encargado. Donde este debe tener la responsabilidad de que estas cámaras estén en normal y continuo funcionamiento, con el objeto de que en caso de ocurrir algún problema las grabaciones puedan ser revisadas, sirviendo así de evidencia de lo ocurrido.

2.1.1.3. Mantención, Controles y reparaciones del equipamiento.

Consiste en la mantención y protección del hardware, unidades de respaldo, dispositivos y otros, ante cualquier eventualidad que ocurra o pueda ocurrir en el transcurso del tiempo. El objetivo de este punto es que los equipos se encuentren en perfectas condiciones para el normal uso de ellos.

El no contar con los equipos computacionales en perfectas condiciones puede provocar un elevado costo para la empresa, siendo este en muchas ocasiones una perdida de tiempo importante en el desarrollo de las labores que se realizan dentro de la organización, por ejemplo: si en el registro civil de Chillán, utilizan computadores con un bajo nivel de rendimiento, es decir, un procesador lento, con poca memoria RAM, esto provoca demora en la atención y si se analiza este problema a una hora en la que se está con una gran afluencia de público, se podría observar que provoca estrés tanto a los funcionarios como a los clientes, además afecta a la eficiencia y crea una mala imagen de este servicio.

Deben realizarse controles periódicamente a los equipos y dispositivos computacionales, y estos controles dependerán específicamente de las políticas que tenga la empresa, es decir, si la entidad tiene estipulado realizar controles mensualmente, semestralmente, anualmente, etc. Además los controles no sólo deben realizarse en estos periodos, sino también en cualquier otro momento que se

requiera, debido a cualquier circunstancia anormal que afecte a los equipos computacionales

En caso de que los PCs no se encuentren en perfectas condiciones o tengan fallas, se deben reparar rápidamente para ponerlos nuevamente en funcionamiento, con el objeto de no interrumpir las labores que se desarrollan en la empresa, ya que, al encontrarse los PCs en malas condiciones puede provocar la pérdida de información o de trabajo realizado.

a) Garantías y Seguros.

Es necesario contar con garantías o seguros en caso de falla total de equipo o pérdida de alguno de ellos, debido a diferentes circunstancias. Además debe efectuarse la contratación de seguros, capaces de cubrir riesgos en algunas oportunidades como:

- Fuego.
- Actos de vandalismo.
- Fenómenos naturales: terremotos, huracanes, lluvia y rayos, etc.
- Inundaciones y goteras.
- Explosiones de gas.
- Delitos informáticos.

b) Plan de contingencia.

Debe existir un plan de contingencia adecuado a las necesidades de la entidad, aunque la probabilidad de que ocurra un desastre sea baja. Además este plan debe tener la capacidad de recuperación.

Un plan de contingencia es un conjunto de procedimientos alternativos a la operación normal, que permitirá a una determinada organización seguir funcionando

frente a un fallo. En el libro de Mario Piattini y Emilio del Peso señala que el un plan de contingencia inexcusablemente debe:

- Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas.

- Establecer un período crítico de recuperación en el cual los procesos deben ser reanudados antes de sufrir pérdidas significativas o irrecuperables.

- Realizar un análisis de aplicaciones críticas por el que se establecerán las prioridades de proceso.

- Determinar las prioridades de proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto.

- Establecer objetivos de recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de desastre y el momento en que el centro alternativo puede procesar las aplicaciones críticas.

- Designar, entre los distintos tipos existentes, un centro alternativo de proceso de datos.

- Asegurar la capacidad de las comunicaciones y
- Asegurar la capacidad de los servicios de back-up

La seguridad lógica es una de las áreas más importantes dentro de la seguridad informática. A continuación, se definirá este concepto, sin olvidar que nuestro alcance en esta área abarca solamente a lo que se refiere al acceso lógico.

2.2. Seguridad Lógica

La seguridad lógica consiste en la *"aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo".* [10]

La información pasa a ser uno de los activos más importantes que se posee y por lo tanto, deben existir técnicas, más allá de la S.F. que la aseguren. Estas técnicas las brinda la S.L.

La seguridad lógica hay que tenerla en cuenta, por que la mayoría de los ataques apuntan a este tipo de seguridad, debido a que están conectado con la Internet, lo cual provoca la constante búsqueda por parte de personas no autorizadas a vulnerar los sistemas que almacenan y procesan la información. Para esto debe existir una constante preocupación por la empresa en este ámbito y el administrador de los sistemas debe ser consiente de evaluar y probar permanentemente sus sistemas, ya sea mediante test, software de análisis de vulnerabilidad, etc, con el objetivo de mejorar su seguridad informática.

Lamentablemente sólo algunas organizaciones están realmente preocupadas en la protección de su Seg. Inf. y son conscientes de tomar las medidas y políticas necesarias para su presencia en la Internet. Es por ello, que existe un mal concepto de la S.L., porque al contar con un firewall *(ver página 35),* la mayoría piensa que está protegido contra todo y en la realidad no es así, porque intervienen muchas cosas más, de las que se nombrarán y expondrán a continuación, pero desde el punto de vista del acceso lógico, no analizando la efectividad de los programas que utilizan las diversas empresas, sino viendo las medidas de seguridad que tienen para

[10] http://www.segu-info.com.ar/logica.htm

acceder a la información que poseen los PCs, porque el objetivo es dar un diagnóstico de la seguridad que tienen las empresas.

2.2.1. Barreras de entrada, que impiden y controlan el acceso a los usuarios no autorizados.

Es de vital importancia tener controlado el acceso a los sistemas, aunque sabemos que es imposible hablar de un sistema 100% seguro, sencillamente porque el costo de una seguridad total es muy alto.

Se debe estar consiente de que siempre existen intrusos que sin permiso puedan entrar y perjudicar el normal funcionamiento de la empresa. Estos intrusos utilizan distintas técnicas para burlar los sistemas de seguridad y buscan básicamente los puntos débiles de los sistemas, es por ello, que no se debe facilitarle el trabajo a estos intrusos, exponiendo un fácil acceso a los sistemas mediante el uso de la red. Para ello, se deben tomar las medidas necesarias para impedir que ocurra la violación a los sistemas.

A continuación, analizaremos algunos mecanismos básicos de seguridad, que toda empresa debe tener en sus sistemas informáticos, y así de esta manera, podrá la empresa impedir el acceso a personas no autorizadas, generando barreras eficientes de protección, que dificulten vulnerar el acceso mediante la red.

2.2.1.1. **Login:** (nombre de usuario)

"El proceso de identificarse ante un PC usualmente por medio del uso de un apodo (name) y contraseña (password)". [11]

[11] http://www.alexandercastillo.net/diccionario/Login.html

En términos generales, este tipo de seguridad está presente en las empresas y no es común encontrar este control de acceso en PCs monousuarios.

Cuando se habla de PCs monousuarios es para ser referencia a los computadores de uso personal, que generalmente es utilizado en los hogares

2.2.1.2. **Password:** (contraseña)

"Secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema". [12]

En los sistemas informáticos, se debe mantener una buena política de seguridad, tanto de creación, mantención y recambio de claves, lo cual es un punto crítico para resguardar la seguridad y privacidad.

a) Debilidades de una password:

Estas van a depender y relacionarse en forma directa, con las políticas que maneje la empresa, en lo concerniente a las *password*. Con una buena política de seguridad se logrará minimizar los riesgos que involucra a estas claves. Este punto es crítico, debido a que estas permiten el libre acceso a los sistemas computacionales, donde cualquier persona que posea una clave puede hacerse pasar por el dueño de esa password y puede provocar daños e incluso en algunos casos paralizar el proceso productivo.

---

[12] http://comunidad.derecho.org/pantin/g37313.html

El problema de las password es que son creadas por las personas que van a utilizar los sistemas a los cuales van a estar autorizados, donde estos usuarios por la idiosincrasia del ser humano, en términos generales, tiende a ocupar la misma clave para todo proceso en que se le exija tener una password para entrar a un determinado sistema, además en la mayoría de los casos las anotan en lugares no seguros y el número de la password esta relacionada con datos personales, lo que facilita a las personas que se quieren apoderarse de estas clave, como los crackers, (Ver Pág. 41) los cuales se definirán más adelante, en esta memoria.

Actualmente existen "diccionarios" que contienen millones de posibles password, que en unos cuantos minutos pueden obtener una clave, estos programas son creados y utilizados por los Crackers, además, existen organizaciones que están conscientes de esta amenaza, por ende, contratan a crackers para probar la vulnerabilidad de la barrera de entrada creadas por sus ingenieros informáticos.

b) Recomendaciones generales a los usuarios para crear una Password:

- No utilizar contraseñas que sean palabras o nombres de miembros de la familia, mascotas, marcas, ciudades, lugares u otros relacionados.

- No usar contraseñas completamente numéricas con algún significado, como por ejemplo: su número telefónico, Cédula de Identidad, fecha de nacimiento, patente del automóvil, etc.

- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.

- Deben ser de 8 o más caracteres. Deben ser fáciles de recordar para no verse con la obligación de anotarlas.

- Elegir una palabra sin sentido, pero pronunciable: wewiya.

- Ejemplos para crear una contraseña:

- Combinar palabras cortas son algún número o carácter de puntuación: tú5_yo7.

- Usar un acrónimo de alguna frase fácil de recordar: Muere de viejo pero no de sapo, la clave sería: MdVpndS.

- Añadir números para el mismo ejemplo anterior: M1dV2pn3dS.

c) Recomendaciones generales a los usuarios para proteger una Password:

- Nunca compartir con alguien su contraseña y si lo hace cambiarla inmediatamente.

- No escribir la contraseña en ningún lugar.

- Si la empresa le asigna una contraseña cambiarla inmediatamente.

- No teclear la contraseña si hay alguien mirando.

- No enviarla por correo electrónico ni mencionarla en una conversación.

- No mantener una contraseña en forma indefinida, debe cambiarla periódicamente.

d) Un buen sistema que controle el acceso vía password debiera considerar lo siguiente:

- Debe tener un número limitado de intentos, pasado este número bloquear el acceso durante un tiempo y enviar un menaje al administrador del sistema, en el cual, se debe mantener un registro especial que indique la procedencia de ese mensaje en forma detallada.

- Debe tener una longitud mínima, se recomienda 8 caracteres. Debe exigir una formato que obligue a un mínimo de letras combinadas con números.

- El sistema debe exigirle a los usurarios que cada cierto tiempo renueven su contraseña.

Para concluir diremos que la seguridad en este punto crítico, va a depender de las políticas de seguridad que emplee la empresa y de la participación, además de la conciencia que tenga el personal, sobre la importancia que tienen sus respectivas claves, donde la A.I. cumplirá un papel fundamental, para ver si se está cumpliendo con lo establecido, para así mantener controlado y minimizar el riesgo.

Algo para reflexionar, una password es como un cepillo de dientes, el cual lo debes usar todos los días, cambiar constantemente y no se debe compartir con nadie. (Autor anónimo)

A continuación, veremos un ejemplo de un programa que exige que se le ingrese el Login y Password.

En la Universidad del Bio-Bio se utiliza un programa llamado Novell, el cual controla el acceso a los recursos que les están permitido utilizar a los alumnos de las diferentes Carreras, el cual posee una base de datos de todos los alumnos activos.

Se ha puesto énfasis en la definición de este concepto, porque en la realidad los usuarios no están conscientes de la importancia que tiene el ser responsable de una password y en términos generales, las personas no se preocupan por mantener seguras sus claves y lo único que le interesa, es que les permita entrar para seguir trabajando, por este motivo la exposición a sido un poco extensa, se ha hecho con el propósito de crear algo de consciencia.

Sin duda, la vía más ocupada por los intrusos es la Internet, porque el acceso se puede hacer desde cualquier punto del mundo, sólo basta contar con un PC que esté conectado a la red.

Firewall es el sistema más popular que poseen las empresas para tener las vías de entrada aseguradas de sus PCs conectados a la red, para bloquear el libre transito de personas no autorizadas.

2.2.1.3 **Firewall:** (Corta-Fuego)

Después de leer y analizar varios conceptos escritos en libros y en las páginas Web. *Firewall* se definirá como:

Es un sistema de seguridad que permite controlar el flujo de información que entra y sale de un PC que está conectado a la Red. El cual, se puede programar para que niegue o deje el libre acceso a los recursos de una corporación, los firewall pueden ser implementados vía Hardware o Software o una combinación de los dos.

Los beneficios entregados por un firewall dependerán de la creatividad, conocimiento y experiencia que tenga la persona encargada de configurarlo, para poder controlar, lo que puede y no debe, entrar o salir de la empresa. Por ejemplo; se puede configurar que los e-mails no salgan con archivos adjunto, para evitar que se fugue información.

Hay varios tipos de firewall y los vamos clasificar según su manera de operar en dos grandes grupos: firewall de nivel de red, y firewall de nivel de aplicación.[13]:

a) Firewall a nivel de red:

También se conocen como Packet-Filtering-Gateways (Paquete que Filtra Entradas), estos firewall son los más económicos, sus capacidades de filtrar la información generalmente están en el software del router. Estos firewalls trabajan con paquetes en donde se encuentran un lote de direcciones, ya sean estas de origen o destino, en las cuales el filtro se puede hacer en la entrada, salida o en ambas, para permitir o denegar el acceso. El problema es que la mayoría de las políticas de seguridad necesitan de un control más fino que este. Es decir, no basta con bloquear el acceso a una determinada página, porque si se permite acceder a una página y esta tiene en su contenido información que puede de una u otra forma perjudicar a la organización, entonces lo ideal es que también se niegue la entrada o salida de archivos que puedan tener información valiosa.

[13] http://support.microsoft.com/?scid=kb;es-es;E10556

Router: *Un router es un dispositivo físico que une redes múltiples juntas. Técnicamente, un router es una "capa de 3 entradas", significa que se conectan redes (como entradas) también tienen la habilidad de filtrar tráfico, entrante o saliente, basada en las direcciones de IP de remitente y receptores.*

Protocolo Internet (IP): *El Protocolo Internet (IP) es un protocolo de conmutación de paquetes que realiza direccionamiento y encaminamiento. Cuando se transmite un paquete, este protocolo añade una cabecera al paquete, de forma que pueda enviarse a través de la red utilizando las tablas de encaminamiento dinámico. IP es el responsable del empaquetado y división de los paquetes requerido por los niveles físico y de enlace de datos del modelo OSI. Cada paquete IP está compuesto por una dirección de origen y una de destino*

Para mayor información sobre protocolo de transferencia de datos que existen en la red, se recomienda leer un artículo muy interesante, el cual se encuentra en la siguiente página Web: http://fmc.axarnet.es/redes/tema_06.htm

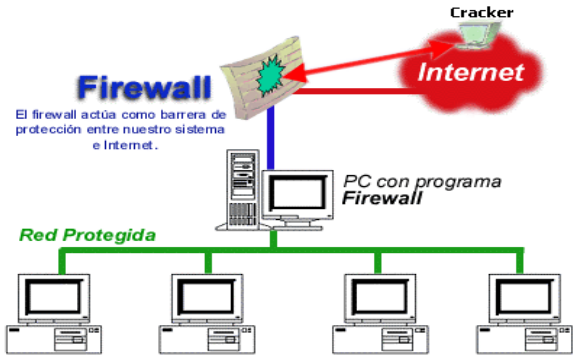
b) Firewall de nivel de aplicación:

Estos firewalls pueden registrar (log) y controlar todo el tráfico de entrada y salida. Además toman los paquetes, los abren, luego los examinan y una vez que se cercioren que no hay peligro, los trasladan a otra red, creando otro paquete con los mismos códigos, para después distribuirlos a sus destinos. En otras palabras este tipo de firewall analiza la información que entra y sale, verifica que no existe algún peligro para los sistemas de la empresa y después de efectuar este control, toma la información y la traslada a una red, para luego crear un nuevo archivo con los mismos códigos, el cual será distribuido a su destino.

Registro Log: Es un programa que registra las actividades ejecutadas por una determinada acción o persona, ejemplo: en este tipo de firewall queda registrada el tipo de información que envió el trabajador A al B.

Por ejemplo; si un archivo de Word está infectado con un virus, este firewall no permitirá su acceso, porque al analizar los códigos va a encontrar algunos que no corresponden.

A continuación, se mostrará en forma gráfica los firewall y donde estos encuentran ubicados.



(fuente:http://www.terra.es/personal2/pagina_de_fuika/tutoriales/puertos/firewall.htm)

Los principales agentes externos en probar la seguridad de acceso lógico son los Hackers, Crackers y Lammers. No importa el motivo que impulsa a estas personas a buscar las debilidades de los sistemas de seguridad, lo único que trasciende es que en muchas ocasiones, nos demuestran que tan vulnerables estamos frente a una amenaza real, que si se llegará a concretar puede provocar daños de imagen, económicos u otros muy importantes. El principal agente interno en buscar las debilidades de los sistemas, es el mismo personal de una empresa y es este el que tendría un mayor impacto sobre la seguridad informática *(ver Pág.15).*

En forma inmediata se hablará de estos agentes, dando una definición y exponiendo algunos ejemplos sobre los actos que han cometidos algunos de ellos.

2.2.2. ¿Genios y/o Delincuentes? Lo único claro es que pueden darle a cualquiera un gran dolor de cabeza.

Estos genios y/o delincuentes son personas amantes del conocimiento, con talento, inteligencia e ingenuidad, que buscan mostrar todas sus capacidades que poseen, vulnerando sistemas de información para disfrutar y lograr un ego personal, aprendiendo detalles de los sistemas.

Sólo necesitan, un PC y una conexión a Internet. No tienen rostro y son impredecibles. Socialmente son delincuentes informáticos que violan las leyes, intruseando en los sistemas privados, lo que provoca una verdadera pesadilla para los dueños de las empresas. Es por ello, que son conocidos como piratas informáticos, también llamados Hackers y Crakers. Pero no se debe calificar por igual a todos los delincuentes informáticos. La verdad es que a los hackers les molesta que los metan a todos en el mismo saco.

No obstante, las empresas chilenas aún no toman suficientes precauciones. Y muy lentamente se han visto más interesadas en invertir en seguridad informática, pero aún no se le da, la importancia que se merece, esta conclusión se obtuvo después de que se visitó a las diferentes empresas para pedir su autorización, para el desarrollo de la presente Memoria. Se conversó con el personal encargado del departamento de Informática y en todas ellas nos comentaban que todavía faltaba mucho camino por recorrer en este tema, pero reconocían que es indispensable para cualquier empresa que cuente con un sistema informático, del cual dependa su funcionamiento o que quiera participar y competir en la llamada "Nueva Economía".

Enseguida se definirán los principales agentes externos que están constantemente buscando la vulnerabilidad de los sistemas de una empresa y luego se expondrá el principal agente interno, que en determinadas condiciones busca las debilidades en Seg. Inf. para hacer algún daño.

2.2.2.1. Hacker:

La definición de un Hacker va de depender de quién lo defina, donde por facilidad de uso, este término es utilizado para referirse tanto al hacker y cracker, como a una persona que entra o intenta entrar en un PC o red sin autorización. Pero en la presente memoria se va a aclarar la diferencia que existe entre uno y otro.

Para ello se tomará como referencia la definición publicada por *Eric Raymond*, compilador de *The New Hacker's Dictionary,* el cual, "*indica que es un programador hábil. Un "buen hack" es una solución astuta a un problema de programación y "hacking" o "hackeo" es el acto de lograrla*" [14]. Raymond señala cinco características posibles que definen a un hacker y estas son las siguientes:

- Una persona que disfruta al aprender los detalles de un lenguaje o sistema de programación.

- Una persona que disfruta al hacer la programación real en vez de sólo teorizar sobre ella.

- Una persona capaz de apreciar el hackeo de otro.

- Una persona que aprende rápidamente a programar.

[14] http://www.geocities.com/mazatlanx/queesunhacker.htm

- Una persona que es experta en un lenguaje o sistema de programación específico como "un hacker de UNIX".

Es un término empleado por algunos para indicar a un "programador hábil" y por otros, sobre todo periodistas y personas ignorantes en el tema, que influenciados por una mala publicidad entregada, por los medios de televisión, radio, periódicos y otros para denotar a "alguien que trata de ingresar a un sistema informático y robar información".

Otra definición de *Hacker* es; una persona con elevados conocimientos de Informática, muchas veces adquiridos en forma autodidacta, que maneja sistemas operativos, lenguajes de programación, errores y fallas en los sistemas, entre otros. Su objetivo es indagar los sistemas informáticos y vulnerar aquellos que parecen más seguros, no necesariamente con una intención delictiva, sino más bien de enfrentar y sortear retos. En general, si descubre problemas de seguridad deja constancia de la vulnerabilidad para que los administradores la solucionen y sea un nuevo objetivo para él. Además muchas empresas multinacionales han contratado a un Hacker para que esté a cargo y sea responsable de la seguridad informática de su organización.

Por lo mencionado anteriormente, se tomarán a los hackers como personas que si bien pueden burlar los sistemas informáticos, estos no van a sacar provecho de estos, por ende, los que se van a mencionar más adelante serán considerados una verdadera amenaza para las organizaciones.

2.2.2.2 Cracker:

El término *Cracker* será utilizado para indicar y señalar a los “chicos malos” de los Hackers. Es el que entra subrepticiamente en el sistema de PCs de otra persona y con mayor frecuencia en una red y ocasiona un "crack" o brecha de seguridad, de

tal manera que se puede apropiar de información crítica de su víctima, como el número de una tarjeta de crédito o su password. Su motivación podría ser de origen ideológico, por el placer del desafío o en el peor de los casos, de carácter delictivo.

Por ende, al analizar bajo el prisma de Seg. Inf., cabe recomendar que los usuarios particulares y las grandes organizaciones deben tener ese tipo de información almacenada en otros medios extraibles (CD., disquette, Zip, etc), para que no esté siempre disponible en el equipo que se usa con frecuencia.

A continuación, se expondrán 3 casos que fueron mostrados a luz pública como los primeros delitos cometidos por los crackers y que tuvieron una gran connotación en su momento. [15]

Caso # 1

Víctima: Banco Security Pacific

Lugar: Los Ángeles, California

Autor: Stan Rifkin

Fecha: 1978

Hecho: Este cracker se robó 10,2 millones de dólares en diamantes al convertir una secuencia numérica por teléfono. Cayó a la semana por un error de tacto, porque ni el banco se había dado cuenta al hacer averiguaciones en el lugar del hecho.

Caso # 2

Víctima: Prue Bache, empresa de corredores de bolsa

Lugar: Londres

Autor: Lamberti

Fecha: 1986

[15] http://www.revistacambio.com/web/interior.php?idp=42&ids=45

Hecho: Se robó ocho millones de dólares y demostró la vulnerabilidad de los incipientes sistemas de acceso remoto.

Caso # 3

Víctima: Citibank

Lugar: New York

Autor: Wladimir Levin, un biotecnólogo ruso de 26 años que por aburrimiento se dedicó a programar PCs.

Fecha: 1994

Hecho: Se robó 10,7 millones de dólares en 1994 a lo largo de tres meses. La operación cayó al final de los tres meses cuando desde Colombia y otros países Suramericanos fueron transferidos tres millones de dólares hasta Holanda y así fue descubierta una conexión Rusa.

Resumiendo son *Cracker* los que se presentan como una gran amenaza para cualquier organización que maneje su información bajo una plataforma Informática, donde estos pueden provocar perdidas millonarias y daños irreparables.

Como podemos ver hay una diferencia clara entre un *Hacker* y un *Cracker*, el cual, podríamos resumir que si bien los dos son expertos fanáticos de los PCs, el primero, busca la vulnerabilidad de los sistemas computacionales para ingresar a ellos solo con el ánimo de alcanzar una satisfacción y reto personal a sus conocimientos en la materia y el segundo, busca el ingreso a estos sistemas para obtener beneficios personales.

2.2.2.3. Lammers

Es alguien que no tiene ninguna inquietud por aprender e investigar, sobre como se hizo un determinado programa y si este puede ser mejorado. Si no que lo

único que quiere es contar con programas, un nombre de usuario y una contraseña para entrar a un sistema y obtener información que pueda ser utilizada para el lucro y beneficio personal.

En otras palabras, un lammers no crea ni investiga nada, sólo busca programas hechos para utilizarlo de mala forma, porque este individuo quiere entrar a los sistemas para sacar provecho personal.

2.2.2.4. Personal de la empresa

Para efectos de esta memoria se definirá al personal de la empresa, como a toda aquella persona que trabaja físicamente dentro o fuera de ella, que tenga una obligación contractual, teniendo o no la facultad de acceder a los sistemas informáticos. Dentro de una entidad existen trabajadores que no tienen acceso a estos sistemas (personal de aseo, guardias), pero de todas maneras no se deben dejar de considerar, como una amenaza para la empresa.

En algunos casos se trabaja físicamente en un lugar distinto al de la organización, por ejemplo, el Gerente General que va otro país para negociar futuras transacciones con otras empresas y por problemas de distancia es necesario ausentarse algunos días, se le puede conceder una autorización para conectarse a los sistemas de la organización vía Internet. Esta situación se debe estudiar si realmente es productivo y beneficioso para la organización, porque el riesgo implícito en estos casos en enorme, debido a que el control del acceso a los sistemas informáticos se hace más difícil, porque no se tiene una certeza de que la persona que quiere entrar es la que fue autorizada por la empresa.

También se deben considerar a los asesores externos que contrata una empresa en un trabajo puntual, como por ejemplo un auditor externo, al cual necesariamente se le debe entregar una password, para que acceda y pueda realizar

su trabajo correctamente. En este caso la empresa debe de asignar una clave provisoria y luego de finalizado la asesoría esta debe proceder a eliminarla.

Sin duda, si el riesgo que corre la empresa con su personal se hiciera realidad, podría tener resultados catastróficos para la organización, producto de que los agentes externos (Hackers, Crackers y Lammers) pueden entrar vía lógica a los sistemas, para modificar y borrar la información, en cambio, el personal puede acceder en forma lógica y física. Por ende, puede modificar la información y también llevársela físicamente, al abrir un PC, sacar el disco duro y lo que es peor robar el respaldo diario que se hace en la empresa, es decir, el daño puede ser irreparable y muy costoso.

Se han dedicado varias páginas a la definición de estos agentes internos y externos, porque si llevamos la Seguridad Informática a un contexto bélico, siempre es conveniente tener el máximo de información posible del enemigo, para saber quienes son, como actúan y que tan peligrosos podrían resultar.

En nuestro país hace muy poco, en comparación con países más desarrollados, se dicto una ley en contra de los delitos informáticos, pero como dice un viejo proverbio *“más vale tarde que nunca”.*

Lamentablemente nuestra reacción es tardía, porque siempre se toma como ejemplos a otros países para tomar medidas o abordar algún problema de interés ciudadana, en muy pocos ámbitos podemos decir que somos los pioneros en impulsar una idea o tomar la iniciativa en algún proyecto innovador, en consecuencia, la Tecnología de la Información no es la excepción, pero bueno dejaremos las críticas y ahora se dará a conocer la Legislación Chilena promulgada en contra de los delincuentes informáticos.

2.2.3. Legislación Chilena en delitos informáticos.

En Chile no habían leyes en esta área, pero el 28 de Mayo de 1993, Enrique Krauss Rusque, Vicepresidente de la República y Francisco Cumplido Cereceda, promulgaron la Ley Nº 19223 relativa a delitos informático, la que contiene los siguientes artículos:

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

"Los ataques a los sistemas informáticos por vía electrónica se han vuelto cada vez más comunes. Chile es el primer país de Sudamérica que cuenta con una Brigada para el Ciber Crimen (adscrita a la Policía de Investigaciones)". [16]

La información como se ha dicho anteriormente es un activo con mucho valor y en algunos casos solo se le da la importancia que se merece cuando se ha perdido, por ende, es de vital importancia tenerla respaldada en caso de ocurrir cualquier eventualidad, reponerse lo más rápido que sea posible. Enseguida se darán a conocer algunas medidas que se utilizan para resguardar la información.

2.2.4. Medidas de seguridad para respaldar la información

Es fundamental, tener respaldada la información en caso de alguna falla fortuita o intencional que comprometa a todo el sistema de una organización en particular.

Que repercusión puede ocasionar si por error se borra toda la información de los clientes y proveedores de una empresa, en forma instantánea se formularían algunas de las siguientes preguntas: ¿Quién me debe y cuánto me han pagado mis clientes?, ¿A quién le debo y cuánto le he pagado a mis proveedores?. El no contar con una respuesta a estas interrogantes podría ocasionar un verdadero caos y por supuesto dañaría la imagen a cualquier empresa que sufra este tipo de problemas. Para solucionar este tipo de problemas, se debe contar con un respaldo que permita restaurar y recuperar esa información.

En esta Memoria se definirán los medios, en términos de respaldo, más utilizados por las empresas.

[16] http://www.uvirtual.cl/prensa/reportajes/hackers.htm

2.2.4.1 **Backup:** (Copias de Seguridad)

"Proceso para salvaguardar los datos de un medio distinto al disco que normalmente se está utilizando. Para microcomputadores podríamos considerar cuatro sistemas estándar: grabación en cintas (el más antiguo), sistemas Zip (grabadoras de discos especiales, con capacidad de unos 100 mb), grabadoras de disquette compatibles con los tradicionales de 3$^{1/2"}$ y con formatos nuevos de alta capacidad (sobre 120 mb) y grabadoras de CD-ROM (650-700 mb)". [17]

Los medios de almacenamiento para respaldar o salvaguardar la información de una empresa, dependerán de los recursos económicos con que cuente una entidad, también del volumen de la información que se quiere guardar.

Hoy en día, es básico hacer backup o copias de seguridad, para cualquier empresa que no quiera perder su información. Sin duda, una buena política de seguridad contempla la existencia de hacer backups, para permitir recuperarse en forma integra y oportuna, de una falla o perdida de los sistemas informáticos. A continuación, se reproducirá lo escrito por Cristian F. Borghello. [18]

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

- ✓ Se debe contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.

[17] http://www.elrinconcito.com/diccionario.php

[18] http://www.zonavirus.com/Detalle_Articulo.asp?Articulo=138

- ✓ Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.

- ✓ El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.

- ✓ Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.

- ✓ Se debe contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.

- ✓ Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se puede encriptar antes de respaldarse.

- ✓ Se debe contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.

- ✓ Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos. Puede optarse por:

Modalidad Externa: otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro producido.

Modalidad Interna: se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.

En todos los casos se debe asegurar reproducir toda la información necesaria para la posterior recuperación, sin pasos secundarios ni operación que dificulte o imposibilite la recuperación.

Uno de los mejores y más modernos sistemas para respaldar la información son los servidores espejo (Mirror), pero son los menos utilizados por el alto costo que tiene su implementación y mantención de este sistema.

2.2.4.2. Mirror: (espejo)

"Un mirror o espejo de cierto sitio web o archivos digitales, son estos mismos archivos, pero alojados en un servidor diferente". [19]

Si se cuenta con un servidor ubicado dentro de la empresa, esta debe tener otro instalado en un lugar geográfico distinto, para que trabaje en forma simultanea y en caso, que el servidor principal falle o presente algún problema, sea el servidor espejo quien asuma la responsabilidad de todas las tareas ejecutados por el principal.

Este tipo de seguridad tiene un costo elevado lo que para muchas empresas le es imposible implementarlos en sus sistemas, pero un ejemplo de este servidor espejo y la importancia que tiene el contar con uno de ellos, es lo que sucedió:

[19] http://www.lugcos.org.ar/mirrors.php

"El 11 de septiembre del año 2001, donde Estados Unidos sufrió el peor ataque terrorista de su historia. Dos aviones de pasajeros secuestrados fueron estrellados contra las Torres Gemelas del World Trade Center en Nueva York, provocando su derrumbe minutos después y la muerte de más de 3.000 personas. También fueron secuestradas otras dos aeronaves comerciales. Una fue estrellada contra un ala del Pentágono, causando la muerte de unas 200 personas". [20]

Lo acontecido en Estados Unidos es muy lamentable y ojalá Dios quiera que nunca más ocurra un desastre de esa naturaleza, ahora se enfocará al ámbito de esta Memoria, es decir, de Seguridad Informática. En esas torres habían varias empresas multinacionales que contaban con un Mirror, ya que estas en cuestión de horas y en algunos casos en minutos, reanudaron su normal funcionamiento y lo único que se perdió fue lo que no se había guardado antes del atentado a las torres, en otras palabras y considerando la magnitud del desastre, las empresas que contaban con un Mirror la sacaron barata, porque las perdidas pudieron haber sido mucho más elevadas de lo que fueron.

En el presente, existen programas que permiten proteger la información de intrusos indeseables como los virus, además cuando se transfiere la información, en ningún caso, debe ser interceptada por otras personas, que sólo buscan sacar provecho de esos datos, por ello, se han creado sistemas que permiten camuflar y hacer indescifrables la información, como es la encriptación. *(ver página 56)*

2.2.5. Programas que protegen la información para que no sea interceptada y/o modificada.

Es muy importante contar con programas que protejan los datos, que se encuentran almacenados en una empresa y aquellos que son transportados por la

[20] http://www.cnnenespanol.com/especial/2001/us.attack/index.eeuu.html

red a otras entidades, para mantener la confidencialidad, integridad y disponibilidad de la información.

A continuación, se dará una pequeña definición de las características que debe conservar la información para que sea confiable. [21]

*"La **confidencialidad** se cumple cuando solo personas autorizadas (en un sentido amplio podríamos referirnos también a sistemas) pueden conocer los datos o la información correspondiente".*

En la confidencialidad de la información, los valores de las personas cumplen un rol fundamental, ya que, la privacidad de esta es muy necesaria para llevarla a cabo.

*"La **integridad** consiste en que solo los usuarios autorizados puedan variar (modificar o borrar) los datos. Deben quedar pistas para control posterior y para auditoria".*

Es decir, que los elementos son modificados por personas autorizadas para ello y de una manera controlada. Cualquier variación de forma no autorizada que modifique la información pierde la integridad de ella.

*"La **disponibilidad** se alcanza si las personas autorizadas pueden acceder a tiempo a la información a la que estén autorizadas".*

En este punto, la información debe permanecer accesible en los momentos en que se requiera, el tema es disponer de ella en forma oportuna y no cuando sea demasiado tarde.

A continuación, se verán los conceptos de algunos programas como son los antivirus, virus y la encriptación.

2.2.5.1 Antivirus

"Es un programa informático específicamente diseñado para detectar y eliminar virus. Porque los conoce, sabe cómo actúan y también sabe cómo eliminarlos. La mejor manera de estar protegidos contra los virus es instalar en buen antivirus en tu PC. La efectividad de un programa antivirus reside, en gran medida, en su capacidad de actualización, preferentemente diaria" [22].

En el mercado existen varios antivirus que provienen de empresas de prestigio en esta área, a continuación se dará el nombre de algunos de ellos con sus respectivas páginas.

- Panda Antivirus (español) **http://www.pandasoftware.es**
- McAfee Viruscan **www.mcafee.com**
- Anyware **www.anyware.com**
- Thunderbyte **www.thunderbyte.com**
- Norton Antivirus **http://www.norton.com/region/es/**

De nada nos sirve tener un excelente antivirus, si dentro de nuestras políticas de seguridad no está contemplado una actualización periódica de ellos, debido a que los crackers están constantemente creando virus nuevos para hacer daño, por lo cual, estos programas deben ser actualizados para que detecten hasta los últimos virus.

Cualquier antivirus no importando su procedencia, cumple con los objetivos de controles informáticos y son los siguientes:

---

[21] "Auditoría Informática, un enfoque práctico", Mario G. Piattini y Emilio Del Peso,2001 (pag.398 y 399)
[22] http://www.sci.uma.es/proxy/stecnico/atdi/serviciotecnico/faq/index.php?idtema=1#89

- **Controles preventivos:** El antivirus impide el ingreso de un virus vía Internet, a demás en la actualidad existen programas capaces de detectar un virus cuando se está copiando información al disco duro del PC.

- **Controles detectivos:** Cuando falla el control preventivo, el antivirus puede detectar un virus cuando intenta activarse o cuando este empieza a producir daño. En esta etapa el virus se encuentra dentro del sistema. A veces es necesario ejecutar el antivirus, en busca de algún virus que se encuentre inactivo, porque hay cierta clase de virus que sólo se activan cuando se coloca en funcionamiento un determinado programa y en algunos casos hay virus que se activan en una fecha determinada.

- **Controles correctivos:** Una vez detectado el intruso indeseado, los antivirus ofrecen una serie de alternativas para controlar o eliminar el virus, para después limpiar los archivos infectados y en caso de no poder limpiarlos, este programa sugiere eliminar el archivo, para evitar problemas en el futuro.

Se han explicado en parte, cómo funciona un antivirus, ahora es el turno de explicar cuales son los tipos de Virus y cómo funcionan. Es necesario mencionar que a estos conceptos se les ha dedicado varias páginas, debido a la importancia que estos tienen en el ámbito de seguridad informática. Además es preciso aprender e ir actualizándose constantemente sobre este tema, lo cual permitirá sacar el máximo de provecho a un programa antivirus, logrando así poder combatir los virus, como los ejemplos que están a continuación.

2.2.5.2. Virus:

"Un virus informático es un programa que puede infectar a otros programas, modificándolos de tal manera que incluyan una copia suya, quizás desarrollada. Hay

que tener en cuenta que un programa no tiene porqué causar daño en el acto para ser considerado como un virus" [23].

Es un programa que se copia a sí mismo. También se podría decir que es un pequeño segmento de código ejecutable escrito en ensamblador o lenguaje de macro, capaz de tomar el control de la máquina o aplicación en algún momento y auto replicarse, alojándose en un soporte diferente al que se encontraba originalmente. Como soporte se entenderá el lugar donde el virus se oculta, ya sea un archivo ejecutable, sector de arranque o documento.

¿Qué hacen los virus?

"Cuando un virus lleva a cabo la acción para la que había sido creado, se dice que se ejecuta la carga. Cuando se inicia la carga, la mayoría de los virus son inofensivos, y no hacen más que mensajes de diferentes tipos. Otros pueden ser bastante maliciosos por naturaleza e intentan producir un daño irreparable al PC personal destrozando ficheros, desplazando o sobre escribiendo el sector de arranque principal, borrando los contenidos del disco duro o incluso escribiendo sobre la BIOS, dejándolo inutilizable". [24]

Los virus son una amenaza real para la información, debido al uso masivo de Internet, el cual ha derribado barreras geográficas, comunicándose e intercambiando información en forma muy sencilla. Esto aumenta el riesgo de infectarse con virus por lo que se hace necesario el incrementar la inversión en seguridad.

El virus es un cáncer electrónico, el cual ha provocado importantes pérdidas millonarias causando muchas veces daños de archivos sin remedio.

[23] http://www.alerta-antivirus.es/virus/ver_pag.html?tema=V&articulo=2&pagina=1
[24] http://www.alerta-antivirus.es/virus/ver_pag.html?tema=V&articulo=2&pagina=5

También ha arrasado con otros no tan costosos, pero de un valor especial para sus dueños como: tesis de grado, cartas de amor, tareas a entregar el día siguiente, novelas antes de ser enviadas a una editorial, etc.

Existen varios tipos de virus y diferentes clasificaciones, algunos de ellos son: [25]

- ***Virus residentes:*** *Se colocan automáticamente en la memoria del PC y desde ella esperan la ejecución de algún programa o la utilización de algún archivo.*

- ***Virus de acción directa:*** *Los virus que se pueden englobar en este grupo, realizan copias de sí mismos en el PC que infectan.*

- ***Virus de sobre escritura:*** *Sobre escriben en el interior de los archivos atacados, haciendo que se pierda el contenido de los mismos.*

- ***Virus de Boot:*** *Atacan a los disquetes y discos duros, haciendo imposible su utilización.*

- ***Virus de macro:*** *Estos virus infectan los archivos de texto, Bases de Datos, presentaciones, etc, que incluyen en ellos pequeños programas llamados macros, que permiten realizar algunas acciones de forma automática.*

- ***Virus de enlace o directorio:*** *Modifican las direcciones que permiten, a nivel interno, acceder a cada uno de los archivos existentes. El resultado es que posteriormente será imposible localizarlos y trabajar con ellos.*

[25] http://www.sinvirus.com/tipos.shtml

Algunos de los virus más conocidos son:

- **Creeper:** Año 1972. Emitía un mensaje que decía "soy una enredadera agárrenme si pueden".
- **Michelangelo:** 06/03/1992. Es un virus del sector de arranque. El nombre proviene por el día en que activa su carga dañina, día del nacimiento de Michelangelo.

- **I love you:** Mayo 2000. Se trataba de un gusano escrito que infectaba miles de PCs a través de un mensaje en el correo electrónico.

- **Anna kournikova:** 17/01/2001. Se trata de una imagen de la famosa tenista Rusa Anna Kournikova, simplemente pincharán en el adjunto, iniciando la infección.

2.2.5.3 Encriptación:

"Encriptar es hacer ilegible un escrito por medio de aplicar al texto un algoritmo. Por ejemplo, si yo a este escrito le aplico que cada vocal cambie por el número correspondiente, y cada consonante por... lo que sea, otro número, si se sabe lo que he hecho, el destinatario lo leerá, es decir, lo "desencriptará o descifrará". [26]

En otras palabras, el objetivo principal es hacer que la información que se está enviando o recibiendo sea ilegible, en caso de que sea interceptada por personas que no correspondan. Esto se logra con la aplicación de un algoritmo, el que consiste en asignar un valor distinto a cada letra o número del texto que se quiere encriptar. Es necesario contar con la llave o clave para desencriptar el documento encriptado.

[26] http://www.elrinconcito.com/diccionario.php

Un ejemplo de encriptación:

La palabra "***seguridad***", es igual a "***19c5v7v21c18c9v4c1v4c***" donde:

S = 19c
E = 5v
G = 7c
U = 21c
R = 18c
I = 9v
D = 4c
A = 1v
D = 4c

Para este ejemplo, el número representa el orden que ocupa la letra en el alfabeto y la letra que acompaña el número es "c" si es consonante y "v" si el vocal.

En la realidad una sola letra puede llegar a ser igual a 50 ó 100 caracteres, dependiendo de quien este encriptando y por supuesto, de que tan poderoso sea el programa utilizado.

La criptografía tiene una división básica que es: clave pública y privada, la primera es la utilizada por los emisores de la información para encriptarla y la segunda es utilizada por el destinatario para desencriptar la información.

Dato curioso:

- En Francia está restringido el uso de la Criptografía y si alguna empresa quiere utilizarla tiene que disponer de una licencia. [27]
- En Estados Unidos el uso de encriptación de mensajes está fuertemente controlada y también se prohibe la exportación de programas

[27] http://www.delitosinformaticos.com/especial/seguridad/legales.shtml

encriptadores, porque es considerado por el Acta de Control de Exportación de Armas (Arms Export Control Act), como incluida en su lista, junto a misiles, bombas y armamento diverso. [28]

Cabe mencionar, que este sistema de seguridad, en la antigüedad era utilizado solo por instituciones, del gobierno, específicamente por los militares, pero ahora cada vez se está haciendo más común, mandar información encriptada de una empresa a otra, a veces hay entidades que utilizan este mecanismo en forma interna.

Aclarar además que lo vertido anteriormente es una visión general de los componentes de la Seguridad Informática y principales elementos de riesgo. No obstante si es de su interés ahondar en la materia recomendamos los libros y páginas que se han citado a lo largo de la Memoria. En la bibliografía se unirán y enumerarán todo el material bibliográfico utilizado.

Antes de introducirse en la metodología de evaluación que se utilizará para realizar el diagnóstico de la realidad en Seg. Inf. de las empresas seleccionadas, es preciso manejar conceptos claves en forma teórica, es por ello, que es necesario abordar algunos términos que a continuación se definirá y explicará en detalle para el desarrollo de la Memoria.

3. Conceptos Básicos que sustentan esta memoria.

3.1 Auditoría:

"Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas". [29]

---

[28] http://www.delitosinformaticos.com/especial/seguridad/criptologia.shtml

Este concepto, generalmente no tiene la adecuada percepción e interpretación, porque una Auditoría es mirada por parte del usuario como un medio para descubrir fraudes, desfalcos, robos y detectar errores. Además, se espera que a través de este proceso se pueda identificar a los involucrados en las fallas, ya sean estas voluntarias e involuntarias.

El objetivo principal y real de esta ciencia, es analizar si lo estipulado explícitamente e implícitamente, está de acuerdo con evaluado en la Auditoría, es decir, la aplicación de este proceso no tiene como fin el descubrir fraudes, sino más bien emitir una opinión justificada y respaldada sobre la información analizada.

Lo expresado anteriormente, está dirigido a comentar la apreciación que se tiene sobre la Auditoría como Contador Auditor, pero ahora se tomará la definición escrita por Enrique Hernández Hernández [30]

"La Auditoría es un proceso formal y necesario para las empresas con el fin de asegurar que todos sus activos sean protegidos en forma adecuada".

La presente Memoria, es su esencia se basa y utiliza procedimientos, técnicas y estándares de Auditoría, para evaluar el riesgo informático existente tanto en la seguridad física como en el área de acceso lógico en una determinada entidad, cuyo objetivo final es el de proteger los activos involucrados en sus sistemas informáticos.

Es de vital importancia contar con medidas de seguridad, que nos permitan resguardar los activos informáticos, las cuales se deben monitorear constantemente, para que se cumplan y sean aplicadas según lo que se ha estipulado por la organización.

---

[29] "Auditoría Informática un enfoque práctico" Mario Piattini,Emilio del Peso (Pag. 4)

[30] "Auditoría en Informática un enfoque Metodológico" (pag. 16)

A continuación, se verá y analizará el concepto de Informática, su impacto y repercusiones que ha tenido esta ciencia en la humanidad.

3.2. Informática:

"Es equivalente a computación. Se puede definir como la ciencia que trata la información (de ahí su nombre) por medios electrónicos. Teniendo en cuenta su ámbito de aplicación, y por lo tanto, sus distintos sistemas de trabajo, da lugar a ramas o especializaciones, tanto más amplias como que su irrupción masiva en la vida cotidiana la convierte en elemento indispensable, potenciándose principalmente lo que se refiere a su vertiente de I. aplicada".[31]

La Informática es una de las ciencias con mayor crecimiento y desarrollo, la cual, nunca se pensó que iba a influir de gran forma en la humanidad, a tal punto que ahora es imprescindible para nuestra vida cotidiana contar con el apoyo de tecnología, debido a que sin ella hubiese sido imposible alcanzar el avance que existe hoy en día, producto de que en la actualidad está presente desde la labor más sencilla a la más compleja, aún es más, es demasiado incierto pronosticar la evolución y el límite que tendrá en el futuro.

El impacto producido por la incorporación de los PCs a las organizaciones a sido de gran importancia, el cual, se ha transformado en una de las herramientas de vital trascendencia, ya que, esta proporciona un soporte para la información que genera y transita por la entidad, procesándola en forma rápida y oportuna para que los usuarios de esta, tomen decisiones objetivas, que sean un aporte para la organización.

Una buena gestión en el presente sobre la utilización de la tecnología, puede generar una ventaja competitiva frente a sus similares, pero a su vez, una mala

[31] http://www.elrinconcito.com/diccionario.php

administración puede producir costos innecesarios lo que puede entorpecer el cumplimiento de los objetivos organizacionales.

Otra definición del concepto Informática para tener en cuenta es la siguiente:

"Es el campo que se encarga del estudio y aplicación práctica de la tecnología, métodos, técnicas y herramientas relacionados con los PCs y el manejo de información por medios electrónicos, el cual comprende las áreas de la tecnología de la información orientadas al buen uso y aprovechamiento de los recursos computacionales para asegurar que la información de las organizaciones fluya de manera oportuna, veraz y confiable." [32]

La Auditoría Informática es una combinación de dos ciencias, la A. y la I., la cual, se desarrolla al igual que estas en base a normas, procedimientos y técnicas. Este proceso es realizado por personas especializadas en el área. Existen instituciones como la ISACA (Ver Pág. 61) que prepara a sus asociados y les otorga una certificación llamada CISA, los cuales son reconocidos por todo el mundo, estos Auditores Informáticos están capacitados para emprender una auditoría informática a cualquier tipo de empresa. A continuación, se analizará el concepto de A.I.

3.3. Auditoría Informática:

1. "Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización una utiliza eficientemente los recursos. De este modo la A.I. sustenta y confirma la consecución de los objetivos tradicionales de la A..": [33]

[32] "Auditoría en Informática un enfoque metodológico" Enrique Hernández (Pag. 12)
[33] "Auditoría Informática un enfoque práctico" Mario Piattini,Emilio del Peso (Pag.29)

- ✓ *Objetivos de protección de activos e integridad de datos.*
- ✓ *Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia.*

2. "Proceso metodológico que tiene el propósito principal de evaluar todos los recursos (humanos, materiales, financieros, tecnológicos, etc.) relacionados con la función de I. para garantizar al negocio que dicho conjunto opera con un criterio de integración y desempeño de niveles altamente satisfactorios para que apoyen la productividad y rentabilidad de la organización".[34]

Cabe mencionar que de los dos conceptos descritos anteriormente, se desarrollará y tomará como referencia más adelante el del primer párrafo, debido a que se enfoca más a los intereses sobre el tema en la Memoria.

El objetivo de la Auditoría Informática es principalmente evaluar y controlar de la mejor forma, el cumplimiento de las políticas y procedimientos para el uso de la tecnología, además que los recursos de I. se aprovechen de manera óptima y que el personal que utiliza tal tecnología sea la encargada y adecuada para ello. Con esto, es probable que haya un mejor desempeño organizacional, proporcionando una gran productividad y rentabilidad, logrando así resultados satisfactorios los que llevan al cumplimiento de las expectativas y objetivos planteados.

3.3.1. Evidencia

"*Durante el transcurso de una Auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la A. Los hallazgos y conclusiones de la A. se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia".* [35]

---

[34] "Auditoría en Informática, un enfoque metodológico", Enrique Hernández H. (pag 17)

ISACA establece 3 tipos de evidencia; la física, la documentada y la de representaciones. [36]

a. **Evidencia física:** Puede incluir observaciones de actividades, propiedad y funciones de los sistemas de información, como por ejemplo; Un inventario de medios magnéticos en una bodega externa.

b. **Evidencia documentada:** Puede incluir resultados de datos extraídos, registro de transacciones, programas registrados, la impresión de una factura, también puede ser utilizada como evidencia, en una A. hecha con anterioridad a la A. actual, siempre que haya sido documentada.

c. **Evidencia de representaciones:** Se refiere a representaciones orales, el cual indica que esta evidencia es crítica para la opinión o conclusión de A., donde se debe tener confirmación escrita de las afirmaciones.

En la obtención de la evidencia, el criterio o juicio y la experiencia del Auditor Informático es fundamental, porque esto le va a permitir reunir evidencia suficiente y competente, para formar una opinión que luego será plasmada en un informe.

Para lograr los objetivos expuesto en el concepto de A.I. es necesario, contar con un excelente sistema de control interno, por ende a continuación se definirá y analizará tal concepto, y posteriormente enfocarse bajo un prisma informático.

3.4. Control interno:

Control Interno *"es el conjunto de planes, métodos y procedimientos adoptados por una organización, con el fin de asegurar que los activos están*

[35] http://www.isaca.cl/standares.html
[36] http://www.isaca.cl/sisas3.html

debidamente protegidos, que los registros contables son fidedignos y que la actividad de la entidad se desarrolla eficazmente de acuerdo con las políticas trazadas por la gerencia, en atención a las metas y los objetivos previstos".[37]

El control interno ha sido diseñado y considerado como la herramienta más importante para el logro de los objetivos. No sólo tiene el objetivo de prevenir fraudes, errores cometidos por el personal, violación de principios y normas contables, fiscales y tributarias, sino que también apunta la eficiente utilización de los recursos y de esta manera poder obtener una gran productividad.

El control interno incentiva a las personas a que cumplan con las medidas y políticas adoptadas por la organización, además debe ser capaz de que el personal se sienta parte de empresa y de la importancia de la eficiencia y eficacia en las operaciones por parte de todos.

De esta manera, el control interno contribuye a que la entidad logre alcanzar sus metas institucionales, controlando el buen uso de los bienes, mediante una correcta evaluación y seguimiento de la gestión organizacional.

El control interno pasa a ser una responsabilidad de todos los integrantes de la organización empresarial, debido a que de esta manera se puede llegar a lograr la eficiencia total.

También se puede definir control interno como "*cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos".* [38]

[37] "Auditoria y Control Interno, Gustavo Cepeda Alonso, (pag 4)
[38] "Auditoría Informática un enfoque práctico" Mario Piattini,Emilio del Peso (Pag.*30)*

3.4.1. Objetivos del control interno: [39]

- *La obtención de la información financiera oportuna, confiable y suficiente como herramienta útil para la gestión y el control.*

- *Promover la obtención de la información técnica y otro tipo de información no financiera para utilizarla como elemento útil para la gestión y el control.*

- *Procurar adecuadas medidas para la protección, uso y conservación de los recursos financieros, materiales, técnicos y cualquier otro recurso de propiedad de la entidad.*

- *Promover la eficiencia organizacional de la entidad para el ogro de sus objetivos y misión.*

- *Asegurar que todas las acciones institucionales en la entidad se desarrollen en el marco de las normas constitucionales, legales y reglamentarias.*

El control interno informático controla que diariamente se realicen todas las actividades de los sistemas de información y que estas se realicen de acuerdo a procedimientos o normas fijadas por la dirección de la organización. Es decir, que las labores que realice cada responsable estén bien ejecutadas y sean validas.

El control interno informático pretende de que las medidas que se implantan sean las correctas y adecuadas para un mejor desempeño organizacional y de esta manera cumplir con los objetivos planteados.

[39] http://www.uch.edu.ar/rrhh/Temas%20Varios/Finanzas/Control%20Interno.doc

Históricamente los objetivos de los controles informáticos se han clasificado en las siguientes categorías: [40]

- ***Controles Preventivos:*** *para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.*

- ***Controles Detectivos:*** *cuando fallan los preventivos para tratar de conocer cuando antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.*
- ***Controles Correctivos:*** *facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un archivo dañado a partir de las copias de seguridad.*

4. Organismos y Normas creadas para guiar a las empresas a mejorar su Seguridad Informática.

4.1 ISACA: (Asociación de Auditoría y Control en Sistema de información).*

Fue fundada en 1969 y cuenta con más de 22.000 miembros en 100 países, auspicia conferencias nacionales e internacionales, administra globalmente la rendición del examen de certificación mundial CISA (Certified information Systems Auditor) y desarrolla globalmente estándares de Auditoría y Control en Sistemas de Información.

[40] "Auditoría Informática un enfoque práctico" Mario Piattini,Emilio del Peso (Pag.30)
* www.isaca.com

La Misión de ISACA Chile A.G. se basa en promover, mejorar y desarrollar las capacidades de los asociados y de la comunidad en lo relacionado con la A., seguridad, control y/o consultoría gerencial, en el campo de los sistemas y tecnologías de información.

4.1.1. COBIT: (Objetivos de control para las Tecnologías de la Información)

La misión y Objetivos de COBIT es Investigar, Desarrollar, Publicitar y promocionar Objetivos de Control de TI internacionales, actualizados a la realidad actual para ser usado por los Gerentes de Negocios y Auditores.

COBIT ha sido desarrollado como estándares generalmente aplicables y aceptados para mejorar las prácticas de control y seguridad de las tecnologías de información (TI) que provean un marco de referencia para la administración, usuarios y Auditores. Básicamente consta de 4 libros, a saber:

1. Resumen Ejecutivo
2. Antecedentes y Marco de Referencia
3. Guías de Auditoría
4. Herramientas de Implementación

(Mayor información del contenido de los libros en página Web www.isaca.cl)

Además de ISACA también existen otras organizaciones internacionales aceptadas globalmente, como la ISO las cuales con sus normas, principios, procedimientos y técnicas ayudan a una mejor regularización de las empresas. A continuación se explicará el significado de ISO.

4.2 ISO (Organización Internacional para la Normalización)

Los grandes volúmenes de datos que se manejan, son el principal activo de las empresas en la actualidad y es por esta razón que los dueños necesitan aumentar su seguridad en tecnologías de la información, para garantizar su identidad.

Por esto, las empresas quieren dar la máxima confianza a sus clientes, realizando efectivos controles y excelentes gestiones. Debido a ello las empresas recurren a las normas ISO.

El 23 de febrero de 1947 fue fundada en Ginebra, Suiza, una organización internacional, no gubernamental: International Organization for Standardization, que significa **Organización Internacional para la Normalización**. Esta organización es representa por la sigla ISO.

El objetivo del ISO es: "*crear parámetros y patrones de igualdad para productos y servicios facilitando con ello el intercambio internacional. Pero como cambian las exigencias de mercado y surgen cada vez nuevas tecnologías y procesos, las normas ISO también se modifican".* [41]

Debido a la necesidad de seguridad de la información que poseen las organizaciones, era preciso la existencia de alguna normativa estándar que agrupara todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente.

[41] http://www.asedie.es/prensa/Octu07_03.htm

La norma engloba todos los aspectos relacionados con la gestión de la seguridad de la información dentro de una organización, para ello se verá a continuación la norma ISO 17799.

4.2.1 ISO 17799:

Esta norma establece controles y medidas suficientes, tanto legales como prácticas, para mantener la confidencialidad, integridad y disponibilidad (*Ver Pág. 51 y 52)* de toda la información que es manejada dentro de la entidad.

Desde el punto de vista jurídico en el cumplimiento de la normativa sobre protección de datos de carácter personal, propiedad intelectual, regulación técnica de cifrado y seguridad a través del personal.

Desde un punto de vista práctico, la norma establece unos controles técnicos y organizativos para que la empresa utilice las herramientas adecuadas que le permitan gestionar de una forma segura la información que maneja, dando unas recomendaciones de buenas prácticas.

Esta norma se estructura en 10 dominios en los que cada uno de ellos hace referencia a un aspecto de la seguridad de la organización: [42]

- *Política de seguridad*
- *Aspectos organizativos para la seguridad*
- *Clasificación y control de activos*
- *Seguridad del personal*

[42] http://www.virusprot.com/art41.htm

- *Seguridad Física y del entorno*
- *Gestión de comunicaciones y operaciones*
- *Control de accesos*
- *Desarrollo y mantenimiento de sistemas*
- *Gestión de continuidad del negocio*
- *Conformidad legal*

CAPÍTULO II

METODOLOGÍA A UTILIZAR EN LA EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

Continuando con el desarrollo de la Memoria, el presente capítulo, dará a conocer en que consiste una metodología enfocada a la seguridad informática, además se analizarán detalladamente algunas de ellas, las cuales están directamente relacionadas con el tema abordado. Más adelante, ilustraremos con ejemplos bibliográficos, donde nos daremos cuenta que existe una gran variedad de ellas y dependerá de lo que se esté evaluando para utilizar o adaptar una metodología adecuada a las necesidades que se quieren evaluar.

Sin duda, es importante desarrollar y entender conceptos teóricos, pero además estos deben ser llevados a la práctica, para que cumplan cabalmente con los objetivos que se quieren alcanzar. Por ejemplo, cuando se realizan los pasos para construir un edificio, en donde se efectúan exhaustivos estudios del terreno, medio ambiente, condiciones climáticas, etc. y por supuesto una gran planificación, acompañada de una espectacular maqueta, pero finalmente este proyecto no se implementa, se puede concluir que no sirvió de nada el esfuerzo. Por eso, una vez finalizada la parte teórica desarrollada por la presente Memoria, se llevará a cabo la práctica, mediante la aplicación de la metodología escogida. Evaluando a una muestra de 10 empresas de la Ciudad de Chillán. (Ver Pág. 100). Para de esta forma, tener una visión general sobre los niveles de seguridad informática presentes en las distintas empresas, en las áreas de acceso físico y lógico

A continuación se verán algunas definiciones que, sin duda, son fundamentales para familiarizarse con el tema de Metodologías. [43]

Metodología*: "conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal."*

Método: *es el modo de decir o hacer con orden una cosa.*

Existen diversas clasificaciones de las metodologías de Seguridad Informática, pero según *Mario Piattini y Emilio del Peso*, autor del libro "Auditoría Informática, un enfoque integral", se pueden agrupar en dos grandes familias:

- **Cuantitativas:** basadas en un modelo matemático numérico que ayuda a la realización del trabajo.

- **Cualitativas:** basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada.

Tomando como referencia la clasificación anterior, se puede decir que la metodología que se va ha ocupar es cuantitativa y cualitativa, porque para realizar la evaluación a las empresas, se utilizará como base un modelo estándar, el cual proporcionará resultados cuantitativos, es decir, en cifras numéricas, los que serán analizados posteriormente según parámetros de medición y de acuerdo a una forma cualitativa se interpretarán los resultados, con el objeto de conocer la realidad de la situación de las empresas seleccionadas, en cuanto, al nivel de riesgo de Seguridad Informática.

[43] "Auditoría Informática, un enfoque integral", Mario Piattini y Emilio del Peso, (pag 51)

Existen diversos tipos de metodologías, las que se crean para evaluar distintas áreas En este estudio sobre la seguridad informática se explicarán dos ejemplos de metodologías. La primera metodología que se expondrá corresponde a las de las PYMES, que se encuentra en el libro de Mario Piattini y Emilio del Peso, en el Capítulo 25 página Nº 567. En segundo lugar se mostrará la metodología denominada "Determinación de riesgos en base a riesgos importantes", que se encuentra en Seminario "Auditoría a la Seguridad y control de la información en Ambiente Windows NT" de Don Pablo Ibarra, en el Capítulo 7 página Nº 91. Luego se procederá a hacer un paralelo que permitirá justificar y dar las razones de porqué se consideraron ambas metodologías y no se eligió una en particular, para alcanzar el objetivo que se quiere lograr en la presente Memoria.

1. METODOLOGIA DE LAS PYMES

Esta metodología tal como su nombre lo indica, esta dirigida a las pequeñas y medianas empresas. Es una guía de auto evaluación, mediante un sistema sencillo, capaz de conocer la situación general de los sistemas de información de una empresa. Tal metodología no pretende eliminar las funciones de un Auditor Informático, debido a que puede ser aplicada por una persona que no sea Auditor ni Informático y que sea o no responsable directo de los sistemas de información, para comprobar por si mismo la fiabilidad y consistencia de los sistemas mediante una metodología, que la puede utilizar cualquier persona especifica en la empresa, pero debe tener un mínimo de conocimientos como por ejemplo: PC, red local (topologías anillo, bus, estrella, etc), periféricos (impresoras, teclados, scanner, memorias, etc), software (sistema operativo), Seguridad Lógica, Seguridad Física, Seguridad Ambiental, aplicaciones utilizadas y eficacia de servicio informático, donde el entorno de aplicación de esta metodología es los mini computadores e informática distribuida, redes de áreas local y PCs.

Esta evaluación de riesgos se desarrolla sobre determinadas áreas de aplicación y bajo técnicas como checklist (lista de control) o cuestionarios, los cuales contienen estándares fijos preestablecidos. Estos estándares se pueden repetir en las diversas áreas de riesgo, debido a que se debe analizar cada área en forma independiente.

A continuación, se explicará cada una de las áreas en las cuales se divide esta metodología:

- ☑ **Riesgo en la continuidad del proceso:** El hacerse efectivo este tipo de riesgo puede afectar la realización del trabajo de informática e incluso en algunos casos puede llegar a paralizar el proceso y por ende perjudicar gravemente a la empresa.

- ☑ **Riesgos de la eficacia del servicio informática:** Se entiende por eficacia del servicio la realización de los trabajos encomendados. Por ende este riesgo es asociado a alteración de dicha realización y el efecto que pueda tener sobre los resultados ofrecidos por el servicio.

- ☑ **Riesgo en la eficiencia del servicio informático:** Se entiende por eficacia del servicio la mejor forma de realizar los procesos o trabajos, a nivel económico o técnico, para de esta forma mejorar la calidad del servicio.

- ☑ **Riesgos económicos directos:** Son aquellas posibilidades de desembolso directos inadecuadas, gastos varios que no deberían hacerse.

- ☑ **Riesgos de la seguridad lógica:** Se entiende por este tipo de riesgo, la posibilidad de ingresar vía lógica sin autorización y acceder a la información mecanizada mediante técnicas informáticas o de otro tipo

☑ **Riesgos de la seguridad física:** Este tipo de riesgo se refiere a la acción que se haga para el deterioro o apropiación de elementos de información de una forma meramente física.

Dada las áreas de esta metodología, el usuario podrá valorar cada una de ellas en forma independiente según las necesidades, que este estime conveniente. La metodología de las PYMES se compone de una serie de estándares fijos, los que podrán ser contestados mediante tres tipos de respuesta un SI, NO o N/A (no aplicable) si una pregunta no se pudiera realizar por cualquier causa.

Valorización de los resultados.

Existen dos sistemas de valorización para los resultados en la metodología de las PYMES:

- Primer Sistema: La respuesta directa tendrá un valor numérico de 1 a 10 que se pondrá en el lugar de la casilla SI o NO dependiendo de la circunstancia. Por ejemplo:

Controles	SÍ	NO	N/A
¿Posee la instalación equipos de continuidad en caso de cortes de energía como puede ser los sistemas de alimentación ininterrumpido (UPS)?	7	4	

En el caso de que se dispusiera de una UPS, se pondría en la casilla SI un valor 7 y en caso contrario se pondría un valor 4. La diferencia de valorización puede estar determinada por que la existencia se considera una mejora sustancial, sin embargo, la falta de existencia podría ser de escasa importancia.

- Segundo Sistema: Aquí para la respuesta no existirá un número guía de ponderación, sino que será el propio usuario quién deberá dar una valoración propia a la respuesta, con valores mínimos y máximos. Además esto debe ir anexo a la pregunta, donde también debe indicarse en el casillero donde debe ubicarse el resultado, es decir en el casillero SI o NO. (generalmente en estos casos el estándar empieza con la propuesta EVALÚE). Por ejemplo:

Controles	SÍ	NO	N/A
Evalúe la carga de trabajo en época de proceso (Ponga el resultado en la casilla NO) 1-30	7	4	

Una vez aplicado los estándares se sumará los valores de la casilla **SÍ** y se restarán los valores de la casilla **NO**, lo cual, dará un valor que se podrá comparar con los estándares, que el usuario habrá valorado en un principio.

Dentro de un estándar podrá estar acompañado de un asterisco, el cuál, se considera de alto riesgo y por lo tanto, indispensable para la seguridad.

Podemos señalar que al analizar los dos sistemas de valorización utilizados por la Metodología de las PYMES, donde el primer sistema se evalúa de 1 al 10, en el cual, no se indica desde que número es bueno o es malo y en el segundo sistema de valorización, se deja el resultado obtenido a criterio del usuario, lo que lo hace una valorización muy subjetiva. Por lo mencionado anteriormente, se puede concluir que es difícil de entender y se hace muy subjetiva la interpretación de los resultados obtenidos, por ende, nunca será igual el resultado si esta Metodología es aplicada por dos personas distintas a una misma empresa.

A continuación se expondrá la segunda metodología, la cual fue aplicada sobre la información que es administrada por el sistema operativo Windows NT, pero que como metodología es igualmente adaptable y aplicable a cualquier otro aspecto o entorno que se quiere evaluar.

2. METODOLOGÍA DE LA DETERMINACIÓN DE RIESGOS EN BASE A RIESGOS IMPORTANTES

La metodología fue creada en el año 2000 por Don Pablo Ibarra, Docente de la Facultad de Ciencias Empresariales de la Universidad del Bío-Bío de Chillán y funcionario del Hospital Herminda Martín de Chillán.

Este método se basa en la elaboración de estándares, los cuales aluden a buenas prácticas obtenidas en la aplicación de técnicas de Auditoría, conocimiento bibliográfico y criterios del Auditor, los cuales, los estándares se clasifican en distintas áreas o ítem, con el objeto de evaluar la situación. Cada ítem de esta metodología, se le asigna un nivel de criticidad, según criterio del profesional y dependiendo de lo que se quiere evaluar. Esto se explicará, después de definir los siguientes conceptos:

Ítem: Son las áreas en las cuales el Auditor divide su evaluación, con el objeto controlar la seguridad de cada área en forma independiente. Un ítem es una parte del alcance y la unión de todos los ítems, forman el alcance que cubre el desarrollo de la Metodología expuesta anteriormente.

Criticidad: Es la importancia que se le otorga a cada ítem o área especifica, lo cual, mostrará el orden de ejecución en el informe final.

Ejemplo:

Ítem: Seguridad de acceso a las áreas criticas

Nivel de Criticidad: Muy Crítico

2.a Determinación de la criticidad de los ítems a Auditar. [44]

La determinación de la criticidad de los ítems a Auditar, es primordialmente por el juicio Profesional del Auditor y antecedentes aportados por la organización, el que deberá ser aplicado de acuerdo a la importancia relativa que tengan estos ítems o áreas para la seguridad de la empresa que se quiere evaluar. (En el caso de esta metodología, se evaluó la seguridad del ambiente Windows NT).

El nivel de criticidad de los ítems puede ser:

Poco crítico: Un ítem será clasificado como poco crítico por el Auditor, cuando el posible mal manejo en aquella área por parte de la empresa Auditada**, no debiese afectar** la continuidad de procesos informáticos claves de la organización.

Crítico: Un ítem será clasificado como crítico por el Auditor, cuando el posible mal manejo en aquella área por parte de la empresa Auditada, pudiese afectar la continuidad de procesos informáticos claves de la organización.

Muy crítico: Un ítem será clasificado como muy crítico por el Auditor, cuando el posible mal manejo en aquella área por parte de la empresa Auditada, **afecte concretamente** la continuidad de procesos informáticos claves de la organización.

Luego de conocer los niveles de criticidad que pueden llegar a tener los distintos Ítem que conforman esta metodología, se procederá a clasificar los niveles

44 "Auditoría a la seguridad y Control de la información en ambiente Windows NT", Pablo Ibarra (pag 86-87)

de riesgo en seguridad, que puede otorgar cada área o ítem en la aplicación de esta metodología.

2.b Determinación de los niveles riesgos basados en riesgos importantes. [45]

Los estándares que componen cada ítem, se aplicarán en base a técnicas de Auditoría (Ver Pág. 96) y preguntas, las cuales serán cerradas, teniendo cada una ellas tres posibles alternativas de respuesta. Estas son **Sí**, **No** y **Parcialmente**, a continuación se explica su significado:

- **La respuesta Sí** será positiva para la empresa auditada, significando riesgos bajos.
- **La respuesta No** será negativa para la empresa auditada, significando riesgos altos.
- **La respuesta Parcialmente** significará riesgos medios.

Esta metodología tiene un puntaje asociado a cada respuesta Sí, No y Parcialmente, que serán **0, 2, 1** respectivamente. Para finalmente determinar el nivel de riesgo de cada ítem se deberá:

1. Sumar los resultados obtenidos en las preguntas que componen el ítem en particular.

2. La cifra resultante se dividirá por el número de preguntas que tiene el ítem.

3. Luego:
   Si el resultado está entre 0,00 y 0,25, el riesgo es **Prácticamente nulo**.
   Si el resultado está entre 0,26 y 0,75, el riesgo es **Poco importante**.

[45] "Auditoría a la seguridad y control de la información en ambiente windows NT," Pablo Ibarra, (pag 88)

Si el resultado está entre 0,76 y 1,25, el riesgo es **Importante**.

Si el resultado está entre 1,26 y 1,75, el riesgo es **Muy importante**.

Si el resultado está entre 1,76 y 2,00, el riesgo es **Máximo**.

Lo anterior se puede expresar en una tabla para que quede más claro, de la siguiente forma:

Resultado Entre	(0....0.25)	(0.26....0.75)	(0.76...1.25)	(1.26....1.75)	(1.76....2)
Riesgo	Prácticamente Nulo	Poco Importante	Importante	Muy Importante	Máximo

El significado del resultado del nivel de riesgo de cada ítem es el siguiente:

- **Prácticamente nulo**:

Que el resultado sea Prácticamente nulo, implica que **no existen riesgos potenciales** de seguridad del ítem Auditado.

- **Poco importante**:

Que el resultado sea Poco importante, implica que si bien, **existen bajos riesgos potenciales** de seguridad del ítem Auditado, estos no afectarán la operación informática de este ítem.

- **Importante**:

Que el resultado sea Importante, implica que **existen riesgos potenciales** de seguridad del ítem Auditado, pudiendo éstos afectar la operación informática de este ítem.

- **Muy importante**:

Que el resultado sea Muy importante, implica que **existen riesgos potenciales** de seguridad del ítem Auditado, pudiendo ítem ser el camino para afectar otras áreas informáticas de la organización.

- **Máximo**:

Que el resultado sea Máximo implica que **existen variados riesgos potenciales** de seguridad del ítem Auditado, corriéndose el riesgo de que el ítem colapse, o bien, que por medio de él se atente contra la seguridad de otras áreas informáticas de la organización.

Conocido ya los niveles de riesgo, cabe mencionar que existen estándares que están acompañados de un asterisco, los que se denominan preguntas claves, que son consideradas de gran importancia o imprescindibles para la seguridad de cada ítem.

Si el resultado de la aplicación de la metodología es clasificado dentro de un nivel **poco importante**, pero dentro del ítem evaluado existe una pregunta clave que fue respondida con un **2 (NO)**, automáticamente el riesgo asociado al ítem será evaluado como **Muy Importante** o **Máximo.** A continuación se ejemplificará cómo se llevará a cabo la aplicación de la metodología.

Ítem: Seguridad Ambiental
Nivel de Criticidad: Crítico

Nº	PREGUNTAS	SI	NO	PAR
1	EXISTE ACCESO RESTRICTIVO AL SERVIDOR	-	-	1
2	LA SALA DONDE SE UBICA ES ANTI-FUEGO	0	-	-
* 3	ESTA CONECTADO A LA UNIDAD ININTERRUMPIDO (UPS)	0	-	-
4	LA SALA DONDE SE UBICA, ESTA PROTEGIDA ANTE INUNDACIONES	-	2	-
5	EXISTEN EXTINTORES EN LA SALA	0		-
	SUMATORIA	0	2	1

* La pregunta 3 es clave.

Entonces, 0 + 2 + 1 = 3. Por lo tanto, en este ejemplo:

- La sumatoria = 3
- La cantidad de preguntas del ítem = 5

Finalmente: $\frac{3 \text{ (resultado)}}{5 \text{ (Nº preguntas)}} = \mathbf{0,6}$

El resultado final 0,6 se ubica entre el tramo de 0,26 y 0,75, por lo tanto, el riesgo de la seguridad física del servidor es Poco Importante, lo que implica que existen riesgos potenciales a la seguridad y control de la información contenida en el servidor, pero como se mencionó, al tener una pregunta con un NO como respuesta y si esta es considerada clave dentro del Ítems, entonces, automáticamente el riesgo asociado al ítems será considerado como muy importante.

Resultado Entre	(0....0.25)	(0.26....0.75)	(0.76...1.25)	(1.26....1.75)	(1.76....2)
Riesgo	Prácticamente Nulo	Poco Importante	Importante	Muy Importante	Máximo

Al tener una estructura ya definida de los posibles resultados, donde son encasillados, obteniendo de forma inmediata el nivel riesgo, lo que hace que sea más fácil la interpretación del resultado obtenido.

3. METODOLOGÍA A UTILIZAR

En este punto se explicará él porque se va a utilizar una fusión de las dos metodologías expuestas, debido a que se llego a la conclusión de que por si solas no cumplían en su totalidad con los objetivos que se quieren lograr en el presente estudio, es por ello, que se rescatará lo más importante y eficiente de cada una ellas,

proporcionado una metodología más clara y fácil de aplicar a los requerimientos de este estudio.

Es preciso aclarar, que en la confección de los estándares, son buenas prácticas que una empresa debiera cumplir para alcanzar una seguridad informática razonable. En la metodología a desarrollar, los estándares serán confeccionados por nuestro criterio, apoyados de las Normas ISO 17799, Cobit, y basados en las Metodologías expuestas en el punto 1 y 2 del **Capítulo II,** realizando los estándares que sean necesarias, hasta alcanzar los objetivos que se quieren alcanzar, entregando información suficiente y competente para formarse una opinión, que será plasmada en un informe final, analizando en forma general el nivel de riesgo de seguridad informático presente en la ciudad de Chillán.

Para justificar el porqué se adapto una metodología y no se utilizó una de las ya explicadas anteriormente, se analizarán las diferencias y semejanzas que existen entre ellas. Para ello, se mostrarán dos tablas, correspondiendo la metodología 1 a la “De las Pymes” y la metodología 2 a “Determinación de los niveles riesgo basados en riesgos importantes”.

DIFERENCIAS

METODO 1	METODO 2
1. Está dirigida a las PYMES (Pequeñas y Medianas Empresas).	**1. Está dirigida a un sistema operativo de la Microsoft Windows NT, pero esta metodología es adaptable a cualquier entorno que se quiera evaluar.**
2. Los estándares son fijos, es decir, están previamente estipulados y pueden ser aplicados a cualquier empresa, que su información sea soporta por sistemas informáticos.	**2. Los estándares se realizan en base a la criticidad, según las circunstancias que este quiere evaluar.**
3. Los estándares pueden tener tres tipos de respuesta; SI, NO o N/A (no aplicable), esta última en caso que el estándar (pregunta) no se pueda aplicar a la empresa.	**3. Los estándares pueden tener tres tipos de respuesta; SI, NO o PAR (parcialmente), esta última en caso de que la empresa no cumpliera cabalmente con lo que se pregunta.**
4. La valorización de los resultados, es subjetivo, debido a que debe asignarse un valor en cada casillero de respuesta (SI, NO o N/A) de acuerdo a un criterio.	**4. La valorización de los resultados, esta predeterminado, debido a que si la respuesta es** SI **el valor es 0; si es** NO **el valor es 2 y si es** PAR **el valor es 1.**
5. Tiene 2 sistemas de valorización: 1º Sistema; **la respuesta tendrá una valor numérico de 1 a10 que habrá que colocar en el lugar del casillero SI o NO.** 2º Sistema; **la respuesta no tendrá un valor numérico predeterminado, sino que será el propio usuario el que deberá dar una valorización.**	**5. Tiene un sólo sistema de valorización, el que se describió anteriormente (Ver Pág. 78)**

6. No asigna niveles de Criticidad a las diferentes áreas, por ende, no divide el alcance que abarca la metodología.	**6. Si asigna niveles de criticidad a las diferentes áreas o ítem y así de esta manera, otorga un grado de importancia a cada una de ellas, además divide el alcance que abarca la metodología.**
7. Para interpretar los resultados se deben sumar los valores asignados al casillero de respuesta SI y restar los valores del casillero NO, para luego comparar con los valores que el usuario valora en un principio, lo que hace que sea más difícil la interpretación de los resultados.	**7. Para interpretar los resultados se deben sumar los valores asignados a los casilleros de respuesta SI, NO y PAR, luego dividir el total de la suma por el número de preguntas realizadas, para finalmente comparar el resultado con los niveles de riesgos que vienen predeterminados, lo que hace que sea más fácil la interpretación de los resultados**

Una vez expuestas las diferencias más relevantes que poseen tales metodologías, se procederá a mostrar las semejanzas que tienen en común, en la siguiente tabla:

SEMEJANZAS

1. **El objetivo principal es minimizar el riesgo informático y mejorar la seguridad de las empresas.**
2. **Las metodologías se basan en estándares.**
3. **Ambos métodos componen su Metodología por estándares.**
4. **Existen Estándares que pueden tener un asterisco (imprescindibles), que la empresa debe cumplir y sino es así se asume que corre un gran riesgo su seguridad informática.**
5. **Se deben realizar cálculos matemáticos, para interpretarlos.**
6. **No requiere personas eruditas en el tema, pero si se debe tener conocimientos mínimos de que está evaluando.**

EN CONCLUSIÓN, SE UTILIZÓ LO SIGUIENTE DE LAS DOS METODOLOGÍAS:

- La Metodología que se utilizará en este trabajo, ira dirigida a un grupo determinado de empresas de la ciudad de Chillán, al igual que la metodología de las Pymes que tal como su nombre lo indica esta dirigida a las Pequeñas y Medianas Empresas.

- Como concepto, se usarán estándares fijos (método 1), técnicas de Auditoría, conocimiento bibliográfico y criterios del Auditor (método 2), esto con el objetivo de realizar un análisis estándar a toda la muestra de empresas a evaluar, es decir, se aplicarán los mismos estándares a todas las empresas.

- Los estándares tendrán 3 tipos de respuesta SI, NO y PAR (método 2) y además los estándares no aplicables (N/A, método 1), se dejarán en blanco, en caso de que no pueda ser aplicados a una determinada empresa. Por tanto, no se consideran al contar el número de estándares (preguntas), utilizados como divisor al calcular el nivel de riesgo.

- Se utilizará la valorización de los resultados (método 2), debido a su fácil utilización, es decir, le tomarán los siguientes valores en cada respuesta; SI=0; NO=2; PARCIALMENTE=1.

- Se dividirá en áreas o ítems para evaluar las distintas empresas (ambos métodos).
  Por ejemplo: Ítem: Seguridad Ambiental

- Se utilizarán los niveles de criticad (método 2) de acuerdo al criterio del Auditor, estos pueden ser; poco critico, critico, muy critico.

- Se usarán los niveles de riesgo (método 2)

Los estándares que se utilizarán en la presente metodología serán clasificados de la siguiente forma: un ítem para evaluar si las empresas cuentan con un organización que permita apoyar o desarrollar la seguridad informática. Tres ítems en lo que se refiere a la seguridad física y en tres ítems para evaluar la seguridad de acceso lógico.

Gestión Directiva:

Ítem 1: Objetivo de las Organizaciones en Informática

Nivel de Criticidad: Crítico.

Se definió como crítico, porque es importante que las empresas tengan una buena estructura organizativa, que asegure un crecimiento y desarrollo constante en Seguridad Informática.

Seguridad Física:

Ítem 1: Seguridad Ambiental

Nivel de Criticidad: Crítico.

Se definió como crítico, porque es importante que las empresas tengan una buena Seguridad Ambiental, que ayude a proteger los equipos tecnológicos.

Ítem 2: Seguridad de acceso a las áreas críticas

Nivel de Criticidad: Muy Crítico.

Se definió como Muy crítico, porque es necesario que las empresas restrinjan el Acceso a las áreas críticas, donde por lo general, se guarda la información más valiosa de la empresa, además por el alto costo que tienen los equipos.

Ítem 3: Mantención, controles y reparaciones del equipamiento

Nivel de Criticidad: Crítico.

Se definió como crítico, porque es importante que las empresas realicen mantenciones, controles y reparaciones a sus equipos en forma periódica, para minimizar el riego y evitar que se produzcan fallas.

Seguridad Lógica:

Ítem 1: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados.

Nivel de Criticidad: Muy Crítico.

Se definió como muy crítico, porque es importante que las empresas cuenten con barreras que impidan el libre acceso a usuarios no autorizados, que podrían dañar y producir pérdidas irreparables.

Ítem 2: Medidas de Seguridad para respaldar la información.

Nivel de Criticidad: Crítico.

Se definió como crítico, porque es importante que las empresas respalden uno de los activos más preciado que tienen, como lo es la información.

Ítem 3: Programas que protegen la información para que no sea interceptada y/o modificada.

Nivel de Criticidad: Crítico.

Se definió como crítico, porque es importante que las empresas protejan su información, cuando sea enviada por medios que no entreguen una seguridad absoluta.

A continuación se detallarán los estándares que se determinaron para evaluar a las empresas respecto a su nivel de riesgo en Seguridad Informática, es preciso mencionar que se aplicará la misma metodología a todas las empresas sometidas a análisis, para de esta forma tener un parámetro y poder comparar los resultados obtenidos por cada una de ellas.

GESTION DIRECTIVA

Ítem Nº1: Objetivo de las Organizaciones en Informática
Nivel de Criticidad: Crítico

Nº		Preguntas	SI	NO	PAR
1		Existen planes a largo plazo para el departamento de informática.			
2		Son adecuados los recursos asignados al departamento de informática para cumplir con los objetivos de la organización.			
3		Existen políticas para la planificación, control y evaluación del departamento de informática.			
4		Existe un comité de planificación o dirección del departamento de informática.			
5		La Gerencia le comunica los objetivos a corto y largo plazo que se quieren alcanzar con el Dpto. informática			
6		Es independiente la ubicación del departamento de informática de los otros departamentos de la empresa.			
7		Existe un método de evaluación para cubrir las vacantes del departamento de informática. (reclutamiento)			
8		Existe una descripción por escrito (manual de operaciones y procedimientos) de cada puesto de trabajo en las diferentes unidades del departamento de informática.			
	8A	Los manuales de operaciones procedimientos pasan por una revisión mínima anual			
9		Existe un plan de contingencia en la gerencia en caso de algún desastre.			
10		En el pasado y en el presente nunca ha sido vulnerada la seguridad informática en el acceso físico.			
11		En el pasado y en el presente nunca ha sido vulnerada la seguridad informática en el acceso lógico.			

SEGURIDAD FÍSICA

Ítem Nº2: Seguridad Ambiental

Nivel de Criticidad: Crítico

Nº		Preguntas	SI	NO	PAR
1		Existen políticas que consideren la Seguridad Ambiental.			
	1A	Estas políticas son conocidas por el personal informático.			
	1B	Estas políticas son acatadas y aplicadas por el personal informático.			
2		La sala donde se ubica el Servidor esta construida con materiales cortafuegos: murallas, techo o cielo y piso.			
3		Donde se ubican los computadores cuenta con detectores de humo y de calor en caso de incendio.			
4		Donde se ubican los computadores posee extintores en caso de incendios.			
	4A	Estos extintores son revisados y cargados periódicamente para que estén en perfectas condiciones al momento de utilizarlos			
5		La empresa tiene la coordinación con Bomberos en caso de incendios.			
6		La sala donde se ubican los computadores se encuentra en un lugar a prueba de inundaciones.			
7		La sala donde se ubican los computadores es de materiales de construcción sólidos en caso de movimientos sísmicos.			
8		Los muebles o mesas donde se ubican los computadores son apropiados para el tamaño y peso de estos.			
9	*[46]	La empresa cuenta con un Sistema de Alimentación Ininterrumpido (U.P.S).			
10		La sala en donde se ubican los computadores cuenta con la iluminación adecuada.			
11		El cableado está bien protegido y ubicado en lugares estratégicos para evitar cualquier daño.			
12		La sala en donde se ubican los computadores, cuenta con un sistema de aire acondicionado adecuado.			
13		Se toman las medidas necesarias para evitar que los computadores se expongan en forma directa a los rayos solares.			
14		Existen dentro de la organización letreros o afiches con mensajes que prohíban: fumar, ingerir líquidos y alimentos, en la sala donde se ubican los computadores.			

[46] Estándar clave, que al tener una repuesta "NO", automáticamente el riesgo asociado al ítem será evaluado como Muy importante o Máximo.

15		La empresa cuenta con seguros contra incendios u otros desastres posibles (terremotos, inundaciones, etc.)			

SEGURIDAD FISICA

Ítem Nº 3: Seguridad de acceso a las áreas criticas
Nivel de Criticidad: Muy Crítico

Nº		Preguntas	SI	NO	PAR
1		Existen políticas de acceso físico definidas para las áreas críticos.			
	1A	Estas políticas son conocidas por el personal informático.			
	1B	Estas políticas son acatadas y aplicadas por el personal informático.			
2		Existe un plan de contingencia en caso de que sea vulnerado el acceso a las áreas críticas.			
3	*	Donde se ubica el Servidor se restringe el acceso a personas no autorizadas.			
4		Existen avisos visuales que restrinjan el acceso a la sala donde se ubica el Servidor.			
5		La sala donde está instalado el Servidor tiene una puerta que impida el libre acceso.			
	5A	La puerta de la sala es transparente.			
67	*	Donde se ubican los computadores se restringe el acceso a personas no autorizadas.			
7		Existen avisos visuales que restrinjan el acceso a la sala donde se ubican los computadores.			
8		La empresa cuenta con cámaras de seguridad o circuitos cerrados de televisión para un mejor control.			
	8A	Las grabaciones de las cámaras de seguridad se realizan en forma ininterrumpida.			
	8B	Las grabaciones se guardan en lugares seguros y adecuados para mantenerlas en buen estado.			
9		La empresa cuenta con la utilización de guardias para la seguridad de las áreas de la organización.			
	9A	Existen personas responsables de supervisar a los guardias.			
10		La empresa cuenta con seguros contra robos.			

SEGURIDAD FÍSICA

Ítem Nº 4: Mantención, controles y reparaciones del equipamiento
Nivel de Criticidad: Crítico

Nº		Preguntas	SI	NO	PAR
1		La empresa posee políticas de mantenimiento, controles y reparaciones de los equipos.			
	1A	Estas políticas son revisadas y actualizadas según decisiones de los encargados de la administración de los equipos.			
2		La empresa cuenta con un plan de contingencia en caso de ocurrir algún tipo de fallo.			
3	*	La empresa en forma preventiva realiza constantes mantenciones, controles y reparaciones a los computadores.			
4		La empresa en caso de fallar un computador, lo repara rápidamente.			
5		La empresa realiza constantes labores de aseo alrededor de los equipos y a su alrededor (que no se encuentren con polvo u otra sustancia).			
6		Los computadores que posee la empresa son de una marca de confianza que entreguen soporte, calidad y garantía.			
7		El hardware que posee la empresa es el necesario, para cubrir las necesidades de estas.			
	7A	Existen políticas de actualizaciones del hardware.			
8		Se han contratado seguros para resguardar el equipamiento utilizado por la empresa.			

SEGURIDAD LOGICA

Ítem Nº 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados.

Nivel de Criticidad: Muy Crítico

Nº		Preguntas	SI	NO	PAR
1		Existen políticas tendientes a resguardar el acceso lógico al sistema			
	1A	Estas políticas están acordes con las necesidades de la empresa.			
	1B	El personal tiene conocimiento y cumple con las políticas establecidas.			
2		Existen actividades de monitoreo que supervisen el acceso al sistema computacional.			
3		Existe un plan de contingencia que permita controlar o restablecer el sistema en caso de ser vulnerada la seguridad Lógica.			
4	*	Existe una persona encargada de la administración y mantención del software que controla las cuentas.			
5		Al personal de la empresa se le asigna un Login, para ingresar a los sistemas.			
6	*	Al personal se le entrega una password, para acceder a los sistemas de la empresa			
	6A	La empresa le facilita material de apoyo, para orientar al personal en la creación de una nueva password.			
	6B	El programa que administra las password exige un mínimo de 6 caracteres.			
	6c	Las password contemplan la combinación de caracteres alfanuméricos.			
	6D	La empresa le exige a los responsable una password que la cambien en un periodo de tiempo determinado.			
*	6E	Cuando un trabajador es despedido, la empresa bloquea la password.			
*	6F	La empresa bloquea la password, después de concluido un servicio externo. Por ejemplo: una Auditoría.			
	6G	El programa que administra las password bloquea el acceso por un par de minutos, después que se haya intentado ingresar sin éxito 3 o 4 veces.			
7		Para cada usuario está asignado un perfil que corresponda a su función y responsabilidad.			
8		La empresa cuenta con normas que prohíban el acceso de disquete de mala reputación o que hayan sido utilizadas por personas ajenas a la organización.			

9		La empresa cuenta con un firewall.			
	9A	La configuración del firewall, permite el cumplimiento de los objetivos organizacionales.			
	9B	Existe personal capacitado para el correcto funcionamiento del firewall.			
	9C	El firewall funciona correctamente y forma continua.			

SEGURIDAD LÓGICA

Ítem Nº 6: Medidas de Seguridad para respaldar la información
Nivel de Criticidad: Crítico

Nº		**Preguntas**	**SI**	**NO**	**PAR**
1		Existen políticas tendientes a tomar medidas de seguridad para respaldar la información.			
2	*	La empresa hace backups (copias de seguridad).			
*	**2A**	Los backups se hacen en forma constante (diariamente)			
	2B	Los backups se guardan en un lugar seguro.			
	2C	El medio de respaldo que utiliza la empresa cumple con los objetivos que esta requiere.			
	2D	Los backups son revisados, para cerciorarse que cuando se necesiten estén en condiciones óptimas			
3		La empresa posee un Mirror (Servidor Espejo)			
	3A	El MIrror está en un lugar distinto al de la empresa.			
	3B	El funcionamiento del Mirror es óptimo y constante.			

SEGURIDAD LÓGICA

Ítem Nº 7: Programas que protegen la información para que no sea interceptada y/o modificada
Nivel de Criticidad: Crítico

Nº		Preguntas	SI	NO	PAR
1		Existen políticas tendientes a proteger la información para que no sea interceptada y/o modificada.			
2	*	La empresa cuenta con un Antivirus que cumpla con las normas legales (licencia).			
*	2A	El Antivirus se actualiza periódicamente.			
	2B	La configuración del Antivirus permite que esté en constante alerta.			
3		La información que es enviada por empresa a través de Internet es encriptada			

Nota: Las preguntas que tienen un asterisco son las claves.

Como ya se ha dicho, la metodología a utilizar estará conformada por estándares (preguntas) que se establecerán según las necesidades que se evaluarán, debido a esto es fundamental conocer bien que son los estándares, definiendo su concepto y las características que deben tener para cumplir con los objetivos. Enseguida se analizarán tales puntos respecto a los estándares.

3.1 Estándares de evaluación

Son medidas o normas, que sirven como referencia de cómo realizar una serie de acciones o actividades determinadas. Además se utilizan como herramientas de medición, los cuales deben tener cierta flexibilidad sin dejar de ser imparciales.

Los estándares deben ser escritos con claridad y bien formulados con el objeto de que se han entendidos de la misma forma por todo el personal de la

empresa y obtengan una mala interpretación. La comprensión de los estándares por parte de todos, será fundamental para que estos lleguen a ser verdaderas metas organizacionales.

Para ayudar a las organizaciones a desarrollar estándares de seguridad de la información, se han creado algunos organismos, los cuales definen estándares que las organizaciones deben considerar para una mayor seguridad. Uno de estos organismos creados es la Organización Internacional de Estándares (ISO), que realizó estándares internacionales de seguridad de la información, publicando la conocida ISO-17799 (Ver Pág. 69), la cual es una norma técnica de seguridad de la información reconocida a nivel mundial. La ISO 17799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

Sin duda, la palabra estándar esta relacionado con buenas prácticas, sin importar de qué aspecto sean estas, debido a que existen diversas políticas para controlar distintas áreas u objetivos.

Si una empresa adopta políticas de seguridad de información, debe tener estándares claramente estipulados para tal ámbito, es decir, los estándares están sujetos a las políticas de la empresa. Para que se cumplan eficientemente las políticas que adopta una empresa, deben existir procedimientos que apunten al logro de tales políticas.

Según la compañía Symantec Corporation (http://www.symantec.com/) encargada sobre soluciones de seguridad global, conocida a nivel mundial como líder en tecnología de seguridad Internet, explica y analiza las diferencias entre políticas, estándares y procedimientos

Fuente:http://www.symantec.com/region/mx/enterprisesecurity/content/expert/LAM_1155.html

- *Una política de seguridad explica con documentación el **por qué** una organización protege su información.*

- *Los estándares de la organización explican con documentación lo **qué** la organización quiere hacer para implementar y administrar la seguridad de su información.*

- *Los procedimientos explican con documentación exactamente **cómo** la organización obtendrá los requerimientos ordenados por estándares y políticas de nivel superior.*

♦ Políticas de seguridad

Las políticas de seguridad de la información en una organización son un simple documento, que explica el enfoque del medio ambiente, del personal y de los procesos en donde se aplica, así también como las consecuencias que pueden ocurrir con su incumplimiento. Además forman parte de un conjunto de políticas que generalmente las organizaciones deben cumplir junto con otras políticas que apuntan

a solucionar áreas específicas como los recursos humanos, finanzas, etc. Estas otras políticas deben ser complementadas y respaldadas con las Políticas de Seguridad de la Información.

- **Procedimientos**

Los procedimientos de seguridad de la información, establecen de una manera detallada las operaciones que se necesitan realizar, para lograr los requerimientos especificados en el Estándar que se aplica a una determinada actividad.

La aplicación de esta metodología se hará basándose en técnicas de Auditoría aplicadas a las distintas fuentes *(ver página 99),* donde se obtendrá la información, para lograr el objetivo principal del Seminario.

3.2 Técnicas de Auditoría para recopilar Evidencia

Son los métodos prácticos de investigación y prueba que el Auditor utiliza para comprobar la razonabilidad de la información, que le permita emitir su opinión profesional.

Con el fin de desarrollar el proceso de evaluación a las diferentes empresas seleccionadas, a continuación se nombrarán y explicarán algunas técnicas de Auditoría, desde un ámbito de una Auditoría Informática, estas tienen el objeto de cerciorarse de que la información que se obtiene en los distintos análisis, es fehaciente, competente y suficiente.

Las técnicas de Auditoría, que se podrán utilizar en el desarrollo práctico de este trabajo son las siguientes:

OBSERVACIÓN. Presencia física de cómo se realizan ciertas acciones o procesos en la organización.

El Auditor se cerciora de la forma en que se realizan ciertas acciones, dándose cuenta ocularmente de la forma en que el personal de la empresa las realiza.

Ejemplo: La observación física, será sin duda, una de las técnicas más utilizadas en el proceso de evaluación a las diferentes empresas, observando la realidad de cómo realizan los procesos y conociendo personalmente los equipos, materiales, infraestructura y personal de la organización.

INSPECCIÓN. Es el examen físico de los bienes materiales o de los documentos, con el objeto de cerciorarse de la existencia de un activo o elemento sujeto a examen.

Ejemplo: Se revisará la existencia de extintores en los diferentes lugares de la empresa en donde exista un computador, verificando además si estos son del tamaño adecuado a las necesidades de la empresa y si se encuentran en buenas condiciones para usarlos en caso de alguna circunstancia.

USO DE ESPECIALISTAS. Obtención de información, de una persona independiente de la empresa examinada, que posee conocimientos o habilidades en campo o área especifica. Esta técnica se utiliza en caso de que el Auditor no pueda cerciorase por si sólo en algunas circunstancias particulares.

Ejemplo: Esta técnica se podrá utilizar en determinados aspectos, como al momento de solicitar información a un experto en informática, para ver la efectividad de los programas o su funcionamiento.

ENTREVISTA. Es un encuentro, reunión y conversación entre dos o más personas con el objetivo de tratar un tema o asunto determinado para aclarar, explicar o resolver las situaciones que son de interés.

Ejemplo: Esta será una cita entre el Auditor y el personal específico de la Empresa sujeta a análisis, es decir, con el encargado del área informática, en donde se le realizarán todas las preguntas necesarias que se estimen conveniente para reunir la evidencia suficiente y competente.

DATOS DE PRUEBA. El objetivo es conocer que hace el programa y la acción de los controles implementados en los sistemas. Consiste en probar directamente el funcionamiento de algunos programas.

Las técnicas de datos de prueba se usan durante una Auditoría alimentando datos al sistema de cómputo de una entidad, y comparando los resultados obtenidos con resultados predeterminados.

Ejemplo: Ingresar personalmente alguna password realizando varios intentos fallidos, para probar si existe el bloqueo de entrada al sistema al fallar una cantidad determinada de veces.

La evidencia debe ser suficiente y competente para que se cumplan los objetivos de una Auditoría. Es por ello, que para poder cerciorarse de que la información que se obtuvo en las diferentes Empresas es relevante y confiable, deben existir fuentes que comprueben, fundamenten y respalden que los resultados obtenidos son fehacientes.

Estas fuentes serán la base de la información que se obtendrá, mediante las distintas técnicas de Auditoría que se aplicarán en la evaluación de la seguridad informática que poseen las diferentes empresas sujetas a análisis.

3.3 Fuentes de donde emana la evidencia

Las fuentes pueden ser documentos, personas, acciones, etc, es todo a lo que el Auditor recurre para obtener información, producto de la aplicación de algunas Técnicas de Auditoría.

Algunas de las fuentes que proporcionarán los datos relevantes en la Auditoría, serán por ejemplo;

- Las confidencias, declaraciones o respuestas que emita el **personal de la empresa** cuando se les solicite en determinados aspectos, relacionados con el tema que sé esta Auditando.

- Los **documentos**, en donde se estipulan las políticas, medidas y procedimientos que se deben realizar en la organización, para una mejor seguridad y control interno. Cabe mencionar que aquí no sólo se deben considerar los documentos internos de la organización, además existen los documentos de las diferentes empresas externas, las cuales acreditan las confirmaciones que se les solicitan. Ejemplo: aquí cabe mencionar los contratos de seguros que posee la empresa.

- La **infraestructura de la organización** es una fuente importante para el tema de la seguridad informática, especialmente desde el punto de vista físico, debido que al aplicar las técnicas de Auditoría como la observación e inspección sobre la calidad de las construcciones de la empresa.

- Los resultados o respuestas que arrojan los **sistemas informáticos** al aplicar las pruebas de datos para comprobar su efectividad, son otra fuente de información para respaldar el trabajo del Auditor.

3.4 Interpretación de los resultados

En cuanto a la interpretación de los resultados obtenidos, es fundamental el criterio del Auditor, para determinar la criticidad e importancia de cada ítem, pero para determinar el riesgo informático en las áreas de seguridad física y lógica (acceso lógico) en cada empresa y a nivel general, se tomará como base la estructura expuesta por la segunda metodología que le pertenece a Don Pablo Ibarra, debido que tal método es fácil de utilizar, y además tiene claramente delimitados los parámetros, para medir los niveles de riesgo.

Es conveniente aclarar que estos resultados no serán publicados detallando el nombre de la entidad, debido a que se debe cuidar la confidencialidad de cada empresa que prestó su colaboración para el desarrollo del Seminario, pero estas si serán nombradas como A, B, C, etc, publicando el nivel de riesgo que existe en cada una de ellas, para finalmente dar una visión general y así revelar el nivel de riesgo existente en la ciudad de Chillán.

En relación, a la elección de las empresas que se evaluarán en el desarrollo del tema de esta investigación, se explicará a continuación como se llegó a una muestra de 10 empresas.

4. Selección de las empresas sometidas a examen

Luego de llevarse a cabo, numerosas entrevistas con empresas de la ciudad de Chillán, a las cuales se le pidió su cooperación para el desarrollo del Seminario, al momento de plantear, que el tema era analizar su Seguridad Informática lo encontraban muy interesante, donde en forma unánime todas las empresas reconocieron que aún estaban en “pañales” y les faltaba mucho por recorrer, pero igualmente muchas se rehusaron en colaborar con este estudio, debido a que los puntos a tratar eran muy delicados y algunas no estaban dispuestas a correr el

riesgo de que personas externas analizarán su Seguridad Informática. Esto es la confirmación de lo leído en los libros y en publicaciones de Internet, los cuales indicaban que si bien las empresas están en forma lenta tomando conciencia que es de vital importancia, contar con una buena Seguridad Informática, poco hacen para ello, porque aún la inversión que es necesaria se mira como un gasto y no es considerada dentro del presupuesto que hacen las organizaciones.

En cuanto a la selección de las empresas, hubiese sido ideal el tomar un método estadístico, para que todas las organizaciones tuviesen la oportunidad de ser seleccionadas, pero lamentablemente no pudo ser así, porque para realizar este proyecto, la comisión evaluadora de la Universidad del Bío-Bío de Chillán, puso como requisito, el contar con empresas a las cuales se les iba a aplicar lo abordado por este Seminario, debido a que en años anteriores se han presentado innumerables anteproyectos que son aprobados y al final no se logra poner en práctica lo abordado, debido a que no existe la suficiente colaboración para el desarrollo practico de la teoría. Por ello, en primer lugar se trabajó en la búsqueda de las empresas, para luego dedicarse a elaboración teórica de la Memoria. Dadas estas condiciones y las áreas en seguridad informática que se quieren abordar, las empresas que se consideraron para solicitarles su colaboración tienen los siguientes requisitos.

- Que su sistema de información estuviese basado en sistemas computacionales.
- Que la red informática esté compuesta de a lo menos xx nodos.
- Que la empresa sea relevante dentro de la provincia de Ñuble.
- Que procesos administrativos claves dependan de las tecnologías de Información.

- Que fuese la matriz, porque estas generalmente tienen sus servidores dentro de la empresa.

En la ciudad de Chillán, existen grandes empresas, pero sin duda, que una gran cantidad de ellas son sucursales, y por supuesto estas manejan la informática desde su casa matriz, por ende, se focalizó a aquellas empresas que cumplían con los requisitos expuestos anteriormente. Al final se logró contar con una muestra de 10 organizaciones, que están dentro de las más representativas de la ciudad, y estas son:

1. Rabie S.A.
2. Carnes Ñuble
3. Hospital Herminda Martín de Chillán
4. Cooperativa Copelec
5. Librería Blue-Mix
6. Ferretería Madrid
7. Rodaméndez
8. Cecinas Villablanca
9. INSUCO (Instituto Superior de Comercio)
10. Buses Línea Azul

Es preciso comentar, que muchas veces se encontró con la voluntad para ayudar, pero no lo permitían las políticas de la empresa y en otras ocasiones simplemente no estaban dispuestas a darle un poco de tiempo a tema planteado.

En el siguiente Capítulo se comentará la experiencia vivida en terreno, dando a conocer los resultados obtenidos de la aplicación del tema investigado, relevando los niveles de riesgo en Seguridad Informática.

CAPÍTULO III

APLICACIÓN DE LA METODOLOGÍA

Luego de conocer conceptos generales referentes a la seguridad informática en el Capitulo I y con la elección y adaptación de la metodología estándar en el Capitulo II, ahora en el presente Capitulo veremos la aplicación de la Metodología, dando a conocer los resultados reales obtenidos por el desarrollo de la teoría expuesta anteriormente. Aquí se mostrarán y analizarán los niveles de Seguridad Informática, en las áreas de acceso físico y lógico, que existen en la muestra de empresas de la ciudad de Chillán, señalando conclusiones individuales de cada una de ellas, lo cual nos permitirá determinar la realidad en términos generales de cómo se presentan las empresas respecto a los temas abordados.

Para facilitar la comprensión de los resultados arrogados por la aplicación de la Metodología, en primer lugar, se mostrarán 10 gráficos correspondientes a cada una de las empresas que se evaluó, 7 gráficos por cada uno de los ítems que integra la metodología y además se graficaron 4 estándares clasificados claves, que a nuestro juicio son los más relevantes.

Todos estos gráficos estarán acompañados de conclusiones y observaciones que se obtuvieron en el desarrollo en terreno de la Metodología, donde se reflejará la compleja realidad sobre los niveles de riesgos en Seguridad Informática que presenta cada empresa. Además se señalan situaciones, en donde las empresas están más débiles o presentan sus mayores problemas.

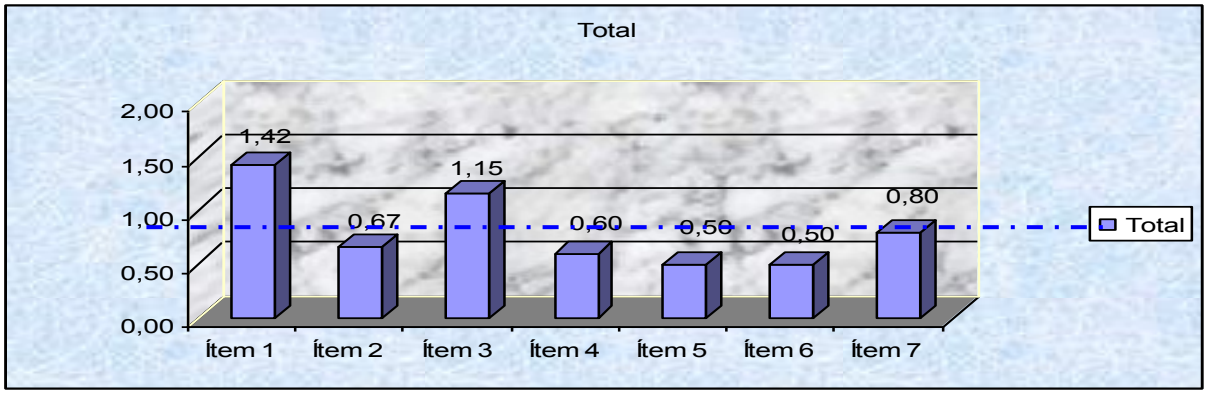
A continuación, se mostrarán los resultados en forma gráfica por cada una de las empresas evaluadas, las que se identificarán con letras del abecedario

empezando por la "A", con la finalidad de proteger la imagen y confidencialidad de cada una de ellas.

1. Conclusiones por Empresa.

1.1 EMPRESA "A"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
A	Ítem 1	Objetivo Organizaciones en Informática	1,42	Muy Importante
	Ítem 2	Seguridad Ambiental	0,67	Poco Importante
	Ítem 3	Seguridad de acceso a las áreas críticas	1,15	Importante
	Ítem 4	Mantención, controles y reparaciones del equipamiento	0,60	Poco Importante
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	0,50	Poco Importante
	Ítem 6	Medidas de Seguridad para respaldar la información	0,50	Poco Importante
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,80	Importante
		Promedio	**0,81**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

De los 7 Ítems evaluados, 4 de ellos arrojan resultados que están dentro del nivel de riesgo **"Poco Importante"**, pero el ítems número 5, tiene un NO como respuesta en una pregunta considerada clave, por lo tanto, en forma inmediata pasa a clasificarse en el nivel de riesgo **"Máximo".**

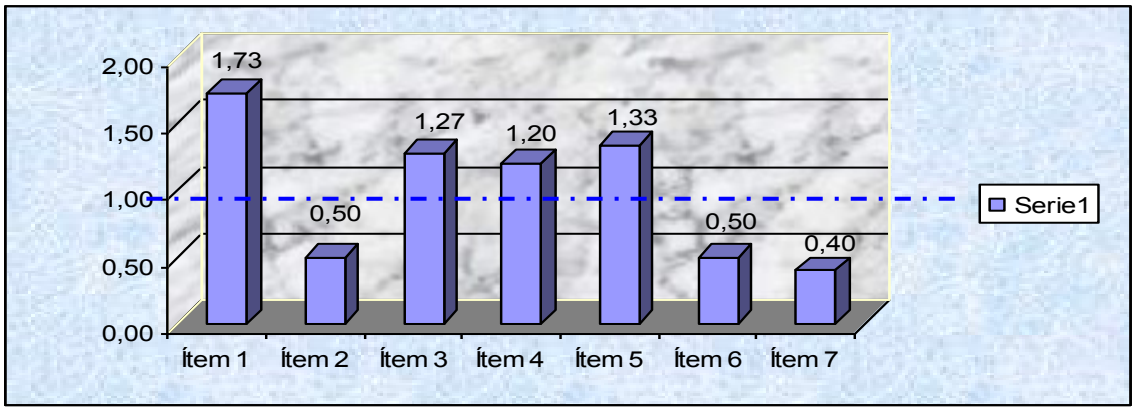
El Ítems 1 arrojó un resultado clasificado en un nivel de riesgo **"Muy Importante"** y el Ítems 3 y 7 arrojaron un resultado clasificado en un nivel de riesgo **"Importante"**

Por lo antes mencionado, se pude concluir:

La empresa **A,** en cuanto a sus niveles de seguridad que apuntan a salvaguardar los accesos lógicos, tiene mucho que mejorar en lo referente a la creación, renovación de passwords y otros puntos. En relación a la seguridad física, la empresa está relativamente bien, teniendo que mejorar la ubicación del Servidor y acceso al mismo. Lo referente a los Objetivos Organizaciones, es preocupante debido a que los responsables de asignar recursos para fortalecer la seguridad informática, sólo exigen y buscan que los sistemas funcionen y no se esfuerzan por prepararse a contingencias de esta índole.

1.2 EMPRESA "B"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
B	Ítem 1	Objetivo Organizaciones en Informática	1,73	Muy Importante
	Ítem 2	Seguridad Ambiental	0,50	Poco Importante
	Ítem 3	Seguridad de acceso a las áreas críticas	1,27	Muy Importante
	Ítem 4	Mantención, controles y reparaciones del equipamiento	1,20	Importante
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	1,33	Muy Importante
	Ítem 6	Medidas de Seguridad para respaldar la información	0,50	Poco Importante
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,40	Poco Importante
		Promedio	**0,99**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

De los 7 ítems evaluados, existe 2 clasificado como **"Muy Importante"**, pero el ítem número 5, tiene un NO como respuesta en una pregunta considerada clave, por lo tanto, en forma inmediata pasa a clasificarse en el nivel de riesgo **"Máximo".** También se encuentran 3 ítems clasificados en un nivel de riesgo **"Poco Importante"**

El ítem 4 es el único clasificado en un nivel de riesgo **"Importante"**

Por lo antes mencionado, se pude concluir:

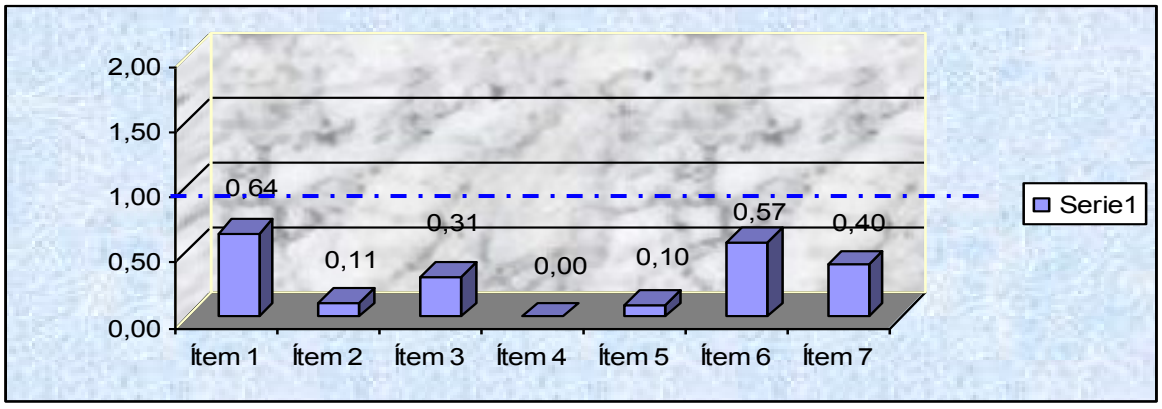
La empresa **B,** no cuenta con un buen resguardo de sus sistemas informáticos, debido a que su seguridad de acceso es deficiente tanto en la parte física como lógica, contando por pocas barreras o restricciones para personas, ya sean internas como ajenas a la empresa, un punto preocupante en la seguridad de acceso lógico es el otorgamiento de passwords al personal para acceder a los sistemas informáticos de la empresa y creación de políticas de seguridad informática.

En cuanto los Objetivos Organizaciones, es preocupante debido a que no están definidos claramente, debiendo mejorar mucho la comunicación interna de la empresa y planes tanto a corto, como largo plazo para el departamento informático.

Lo mejor que presenta la empresa es el aspecto de seguridad física ambiental, pero deben aumentar la protección del servidor, dejando en un lugar distinto a los otros computadores y con una puerta que proteja su integridad.

1.3 EMPRESA "C"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
C	Ítem 1	Objetivo Organizaciones en Informática	0,64	Poco Importante
	Ítem 2	Seguridad Ambiental	0,11	Prácticamente Nulo
	Ítem 3	Seguridad de acceso a las áreas críticas	0,31	Poco Importante
	Ítem 4	Mantención, controles y reparaciones del equipamiento	0,00	Prácticamente Nulo
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	0,10	Prácticamente Nulo
	Ítem 6	Medidas de Seguridad para respaldar la información	0,57	Poco Importante
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,40	Poco Importante
		Promedio	**0,30**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

De los 7 ítems evaluados, existen 4 de ellos los cuales otorgaron resultados clasificados como un nivel de riesgo **"Poco Importante"**

Los 3 ítems restantes arrojaron resultados de un nivel de riesgo clasificado **"Prácticamente Nulo"**

Por lo antes mencionado, se pude concluir:

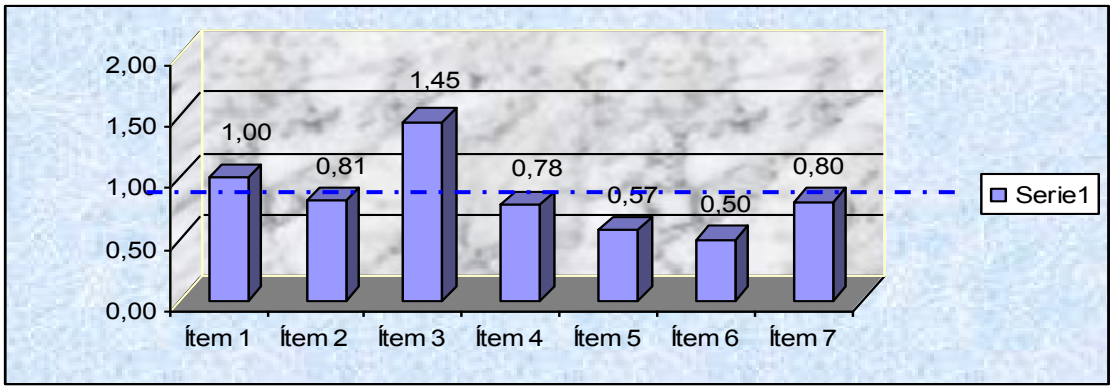
La empresa **C,** cuenta con políticas y medidas de seguridad informática importantes, lo cual ayuda bastante a proteger su información, además de los activos con los que cuenta. Igualmente es fundamental mejorar en cuanto a los Objetivos Organizaciones, creando un comité de planificación para el departamento informático, confeccionando manuales de operaciones por escritos de los procedimientos que se deben realizar, siendo evaluados estos en periodos determinados.

Con respecto a la seguridad física la empresa se encuentra bastante bien, pero debe contar con extintores ubicados en las mismas salas donde se encuentran los computadores.

Por último, un tema importante es que las passwords contemplen la combinación de caracteres alfanuméricos, es decir, que permita para la creación números y letras, siendo ideal un mínimo de 6 caracteres.

1.4 EMPRESA "D"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
D	Ítem 1	Objetivo Organizaciones en Informática	1,00	Importante
	Ítem 2	Seguridad Ambiental	0,81	Importante
	Ítem 3	Seguridad de acceso a las áreas críticas	1,45	Muy Importante
	Ítem 4	Mantención, controles y reparaciones del equipamiento	0,78	Importante
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	0,57	Poco Importante
	Ítem 6	Medidas de Seguridad para respaldar la información	0,50	Poco Importante
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,80	Importante
		Promedio	**0,85**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

De los 7 Ítems evaluados, 4 de ellos arrojan resultados que están dentro del nivel de riesgo **"Importante"**, pero el ítems número 3, tiene un NO como respuesta en una pregunta considerada clave, por lo tanto, en forma inmediata pasa a clasificarse en el nivel de riesgo **"Máximo".**

El Ítems 3 arrojó un resultado clasificado en un nivel de riesgo **"Muy Importante"** y el Ítems 5 y 6 arrojó un resultado clasificado en un nivel de riesgo **"Poco Importante"**

Por lo antes mencionado, se pude concluir:

La empresa **D,** muestra su mayor preocupación en la seguridad de acceso físico a las áreas más críticas de la empresa, es decir, existe poca preocupación por restringir que las personas accedan a lugares donde se pueden realizar daños irreparables.

También es necesario; contar con más medidas para proteger los equipos computacionales, crear conciencia al personal de la empresa, que cosas tan sencillas pueden ser de mucha utilidad a la hora de un desastre. Un buen comienzo es por colocar letreros que prohíban el acceso a personas no autorizadas, consumir alimentos e ingerir líquidos en los computadores, etc.

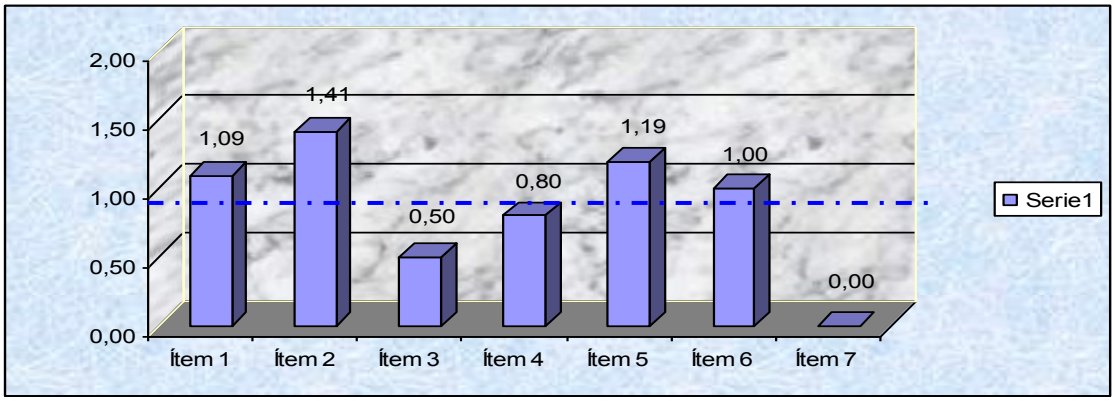
Referente a los Objetivos Organizaciones, se debe tomar más en cuenta y darle un mayor tiempo a este tema, con la finalidad de alcanzar los objetivos a corto y largo plazo que la empresa desea lograr, existiendo una buena comunicación interna, para que los responsables de la sistemas informáticos y personal en general tome conciencia de que la seguridad informática es esencial para proteger la información.

La mantención de los equipos casi no existe, ya que sólo se realiza al momento de fallar un equipo computacional, una buena mantención puede ahorrar bastante tiempo y costo, debido a que la empresa no cuenta con equipos de respaldo en caso de que alguno presente algún problema, lo cual puede ser muy perjudicial paralizando los procesos, lo que puede llegar a provocar perdidas inesperadas.

Lo mejor que presenta la empresa **D,** es su seguridad de acceso lógico, con barreras y medidas que ayudan a impedir que puedan vulnerar su seguridad, pero como ya se ha dicho no basta sólo con proteger este aspecto, sino que debe haber una seguridad informática global.

1.5 EMPRESA "E"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
E	Ítem 1	Objetivo Organizaciones en Informática	1,09	Importante
	Ítem 2	Seguridad Ambiental	1,41	Muy Importante
	Ítem 3	Seguridad de acceso a las áreas críticas	0,50	Poco Importante
	Ítem 4	Mantención, controles y reparaciones del equipamiento	0,80	Importante
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	1,19	Importante
	Ítem 6	Medidas de Seguridad para respaldar la información	1,00	Importante
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,00	Prácticamente Nulo
		Promedio	**0,86**	



Según lo expuesto en el gráfico 5 se puede comentar lo siguiente:

De los 7 Ítems evaluados, 4 de ellos arrojan resultados que están dentro del nivel de riesgo **"Importante"**, pero el ítems número 5 y 6, tienen un NO como respuesta en una pregunta considerada clave, por lo tanto, en forma inmediata pasa a clasificarse en el nivel de riesgo **"Máximo".**

El Ítems 2 arrojó un resultado clasificado en un nivel de riesgo **"Muy Importante",** el Ítems 3 arrojó un resultado clasificado en un nivel de riesgo **"Poco Importante"** y el Ítems 7 arrojó un resultado clasificado en un nivel de riesgo **"Prácticamente Nulo"**

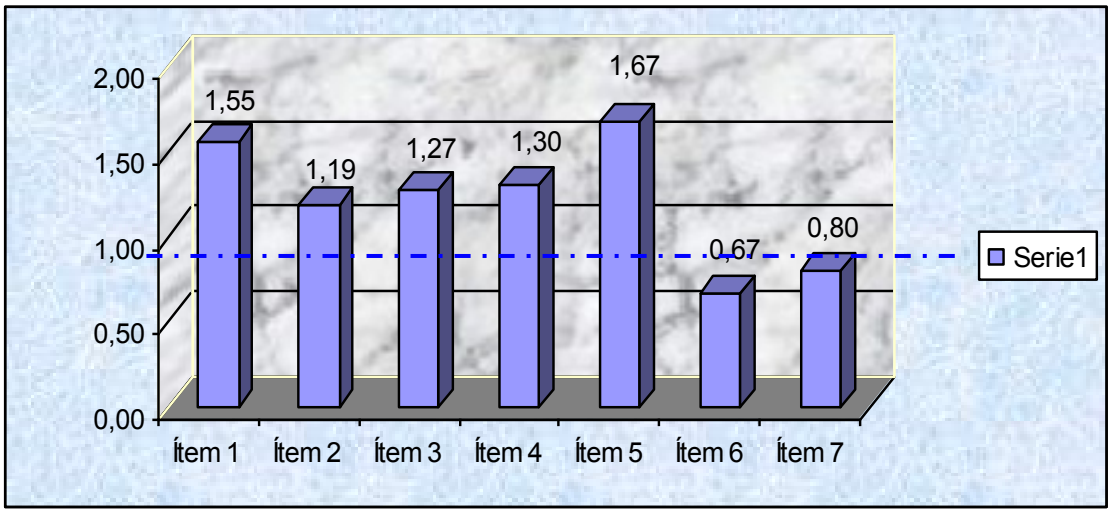
Por lo antes mencionado, se pude concluir:

La empresa **E,** presenta sus mayores problemas en la seguridad de acceso lógico y en el respaldo de la información, siendo estos dos aspectos esenciales en una empresa que maneje su información con sistemas informáticos. Debe tener una mayor preocupación en cuanto al otorgamiento de claves y la protección de estas, entregando material de apoyo al personal para la correcta creación de estas.

Otro aspecto negativo de la empresa **E,** es la seguridad física ambiental, existiendo un bajo interés en el lugar, donde están instalados los equipos computacionales y lo más preocupante "el servidor", el cual, se encuentra desprotegido, con cables y soportes no adecuados para ello. Además el lugar físico donde se encuentra, no es de construcción sólida, ni es aprueba de inundaciones y tampoco cuenta con las medidas básicas en caso de existir un incendio.

1.6 EMPRESA "F"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
F	Ítem 1	Objetivo Organizaciones en Informática	1,55	Muy Importante
	Ítem 2	Seguridad Ambiental	1,19	Importante
	Ítem 3	Seguridad de acceso a las áreas críticas	1,27	Muy Importante
	Ítem 4	Mantención, controles y reparaciones del equipamiento	1,30	Muy Importante
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	1,67	Muy Importante
	Ítem 6	Medidas de Seguridad para respaldar la información	0,67	Poco Importante
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,80	Importante
		Promedio	**1,23**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

De los 7 Ítems evaluados, 4 de ellos arrojan resultados que están dentro del nivel de riesgo **"Muy Importante"**

El Ítems 2 y 7 arrojaron un resultado clasificado en un nivel de riesgo **"Importante"** pero el ítems número 6 tiene un NO como respuesta en una pregunta considerada clave, por lo tanto, en forma inmediata pasa a clasificarse en el nivel de riesgo **"Máximo".**

El Ítems 6 arrojó un resultado clasificado en un nivel de riesgo **"Poco Importante".**

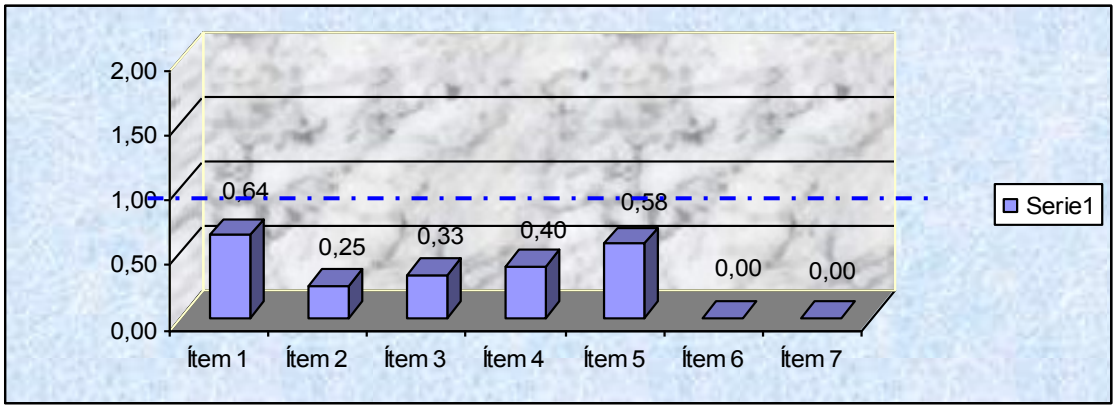
Por lo antes mencionado, se pude concluir:

La empresa **F,** presenta grandes problemas en general en su seguridad informática, esto se debe mayormente, a que recientemente están manejando su información con sistemas informáticos, siendo novatos en este ámbito, pero igualmente ahora manejan su página de Internet, mediante la cual pueden realizarse transacciones de venta, por lo que deben realizar una mayor inversión de recursos

en fortalecer sus accesos lógicos, debido a que están expuestos al ingreso de un Hackers o cualquier intruso que desee alterar o perjudicar sus acciones a través de la página.

1.7 EMPRESA "G"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
G	Ítem 1	Objetivo Organizaciones en Informática	0,64	Poco Importante
	Ítem 2	Seguridad Ambiental	0,25	Prácticamente Nulo
	Ítem 3	Seguridad de acceso a las áreas críticas	0,33	Poco Importante
	Ítem 4	Mantención, controles y reparaciones del equipamiento	0,40	Poco Importante
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	0,58	Poco Importante
	Ítem 6	Medidas de Seguridad para respaldar la información	0,00	Prácticamente Nulo
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,00	Prácticamente Nulo
		Promedio	**0,31**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

De los 7 Ítems evaluados, 4 de ellos arrojan resultados que están dentro del nivel de riesgo **"Poco Importante"**,

El Ítems 2, 6 y 7 arrojaron un resultado clasificado en un nivel de riesgo **"Prácticamente Nulo"** pero el ítems número 6 tiene un NO como respuesta en una pregunta considerada clave, por lo tanto, en forma inmediata pasa a clasificarse en el nivel de riesgo **"Máximo".**

Por lo antes mencionado, se pude concluir:

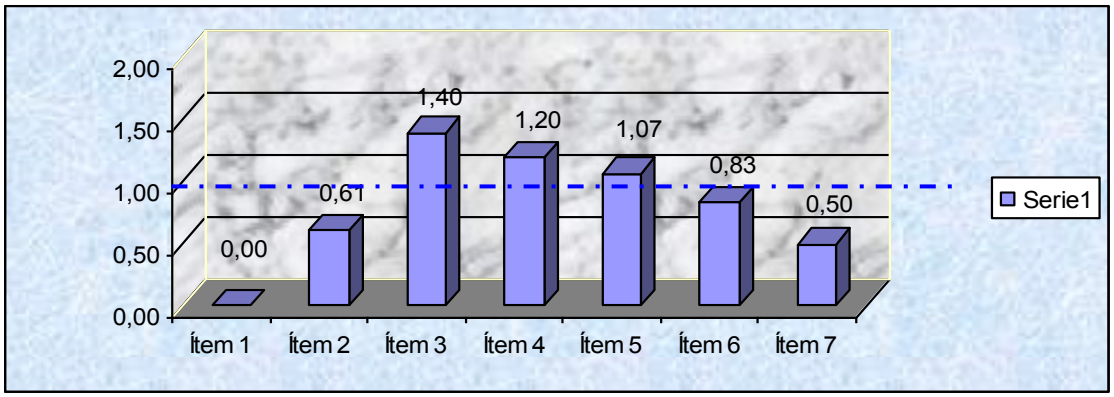
La empresa **G,** en general presenta niveles de seguridad informática adecuados en todos sus aspectos, contando con políticas, medidas y barreras para proteger sus sistemas informáticos.

Lo más preocupante de esta empresa son sus objetivos organizacionales en informática, donde seria ideal crear un comité de planificación del departamento informática, además contar con un manual de procedimientos por escrito de las distintas labores que se deben realizar en el departamento, realizando una evaluación o revisión en determinados periodos de tales procedimientos.

Tal empresa esta en proceso de mejorar aun más su seguridad informática, por lo cual, esta evaluando proyectos, los cuales espera implementar a corto plazo, debido a ser una empresa de gran magnitud.

1.8 EMPRESA "H"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
H	Ítem 1	Objetivo Organizaciones en Informática	0,00	Prácticamente Nulo
	Ítem 2	Seguridad Ambiental	0,61	Poco Importante
	Ítem 3	Seguridad de acceso a las áreas críticas	1,40	Muy Importante
	Ítem 4	Mantención, controles y reparaciones del equipamiento	1,20	Importante
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	1,07	Importante
	Ítem 6	Medidas de Seguridad para respaldar la información	0,83	Importante
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,50	Poco Importante
		Promedio	**0,80**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

De los 7 Ítems, el primer ítem referente a Objetivos Organizacionales en Informática no fue aplicado a la empresa en cuestión, debido a que por ser una institución educacional su objetivo principal es educar y por lo tanto, no manejan personal permanente para desarrollar el área de informática, sino más bien, según las necesidades que se vayan presentando se toman decisiones en este ámbito. Al momento que quisimos evaluar los estándares de este ítem, estas hubieran arrojado una respuesta NO realizando preguntas, dando un resultado en un nivel de riesgo máximo, pero no evaluaremos este ítem, considerando su posición como empresa, pero dejaremos bien claro que no justifica para nada el ser una Empresa de carácter Institucional el no constar con Objetivos Organizacionales en Informática, por lo tanto, esta empresa queda en deuda, en cuanto a mejorar este aspecto.

El Ítems 4, 5 y 6 arrojaron un resultado clasificado en un nivel de riesgo **"Importante"** el Ítems 2 y 7 arrojaron un resultado clasificado en un nivel de riesgo **"Poco Importante"** y por ultimo el ítem 3 arroja un resultado clasificado en un nivel de riesgo **"Muy Importante"**

Por lo antes mencionado, se pude concluir:

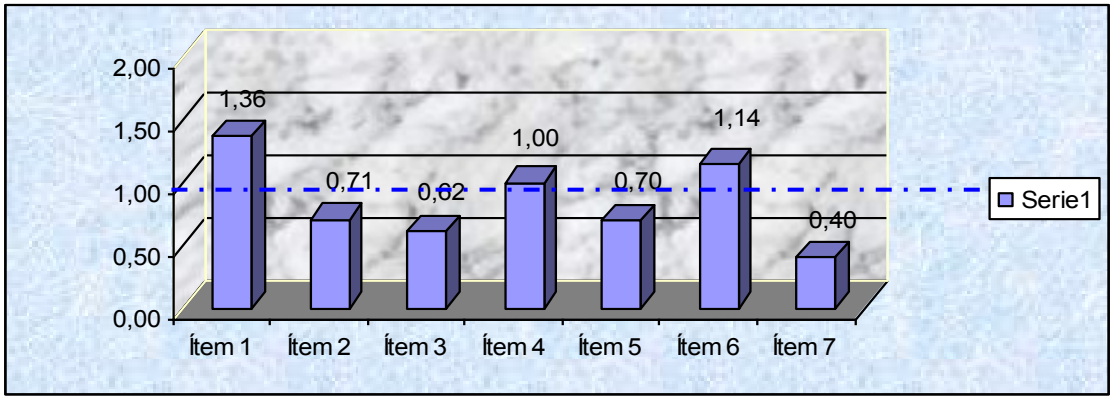
La empresa **H,** su mayor problema lo presenta en el respaldo de la información, debido a que no lo efectúa copias de seguridad diariamente como debería realizarlo, además debe guardar tales respaldos o copias en lugares seguros y ojala en un sitio distinto del que se trabaja normalmente, con el objetivo de que al momento de querer recurrir a alguna información, esta este disponible y en perfectas condiciones.

Su seguridad de acceso físico muestra un nivel preocupante, el cual debe tener un mayor cuidado debido a la gran cantidad de personas que diariamente acceden a la institución por diferentes motivos, para ello se deben tomar medidas serias de restricción a los lugares con equipos computacionales.

En el aspecto de seguridad física ambiental la empresa muestra una mayor inversión, debido a su sólida construcción y materiales de apoyo que ayudarían bastante a la hora de ocurrir algún desastre.

1.9 EMPRESA "I"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
I	Ítem 1	Objetivo Organizaciones en Informática	1,36	Muy Importante
	Ítem 2	Seguridad Ambiental	0,71	Poco Importante
	Ítem 3	Seguridad de acceso a las áreas críticas	0,62	Poco Importante
	Ítem 4	Mantención, controles y reparaciones del equipamiento	1,00	Importante
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	0,70	Poco Importante
	Ítem 6	Medidas de Seguridad para respaldar la información	1,14	Importante
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,40	Poco Importante
		Promedio	**0,85**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

De los 7 Ítems evaluados, 4 de ellos arrojan resultados que están dentro del nivel de riesgo **"Poco Importante"**, pero el ítems número 5, tiene un NO como respuesta en una pregunta considerada clave, por lo tanto, en forma inmediata pasa a clasificarse en el nivel de riesgo **"Máximo".**

El Ítems 4 y 6 arrojaron un resultado clasificado en un nivel de riesgo **"Importante"** pero el ítems número 6, tiene un NO como respuesta en una pregunta considerada clave, por lo tanto, en forma inmediata pasa a clasificarse en el nivel de riesgo **"Máximo".**

El Ítems 1 arrojó un resultado clasificado en un nivel de riesgo **"Muy Importante"**

Por lo antes mencionado, se pude concluir:

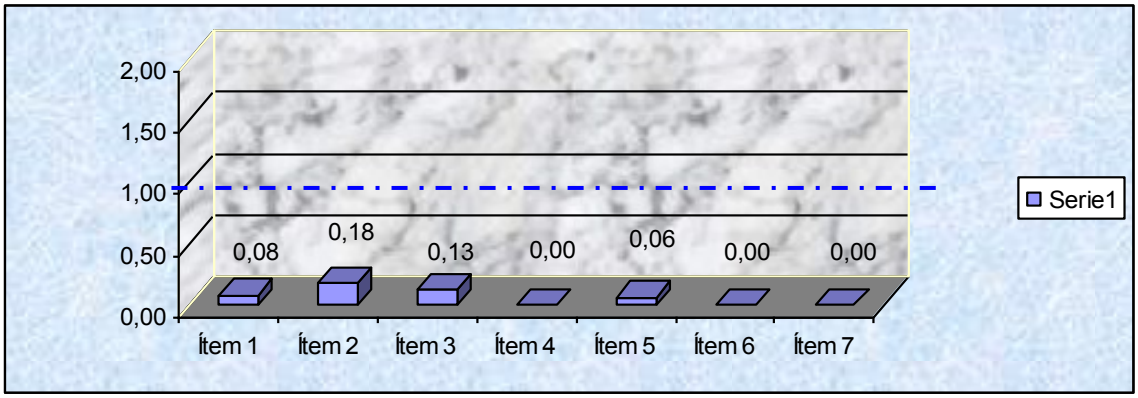
La empresa **I,** en cuanto a los niveles de seguridad que apuntan a salvaguardar los accesos lógicos, tiene mucho que mejorar en lo referente a la creación, renovación y eliminación de las passwords, en caso de que los trabajadores ya no cumplan ninguna función para la empresa.

El respaldo de la información, no se efectúa diariamente como debería realizarse, además debe guardar las copias de seguridad en lugares seguros y ojala en un sitio distinto del que se trabaja normalmente, con el objetivo de que al momento de querer recurrir a alguna información, esta este disponible y en perfectas condiciones.

Otro punto preocupante de esta empresa, son sus objetivos organizacionales en informática, donde seria ideal crear un comité de planificación del departamento informática, además constar con un manual de procedimientos por escrito de las distintas labores que se deben realizar en el departamento, realizando una evaluación o revisión en determinados periodos de tales procedimientos.

1.10 EMPRESA "J"

EMPRESA	ÍTEM	TITULO POR ITEMS	Total	Clasificación
J	Ítem 1	Objetivo Organizaciones en Informática	0,08	Prácticamente Nulo
	Ítem 2	Seguridad Ambiental	0,18	Prácticamente Nulo
	Ítem 3	Seguridad de acceso a las áreas críticas	0,13	Prácticamente Nulo
	Ítem 4	Mantención, controles y reparaciones del equipamiento	0,00	Prácticamente Nulo
	Ítem 5	Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	0,06	Prácticamente Nulo
	Ítem 6	Medidas de Seguridad para respaldar la información	0,00	Prácticamente Nulo
	Ítem 7	Programas que protegen la información para que no sea interceptada y/o modificada	0,00	Prácticamente Nulo
		Promedio	**0,06**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

De los 7 ítems evaluados todos arrojaron resultados con un nivel de riesgo **"Prácticamente Nulo"**

Del análisis realizado, sin duda, la empresa **J** es la mejor evaluada dentro de la muestra de la ciudad de Chillán, además posee medidas y políticas que ayudan bastante a proteger su información.

Es importante mencionar que sus niveles los niveles de riesgo de la Empresa J son bajos, pero también debe señalarse que la seguridad absoluta es imposible, el riesgo siempre esta presente dentro o fuera de la organización independientemente de las medidas o barreras que la empresa posee para su protección.

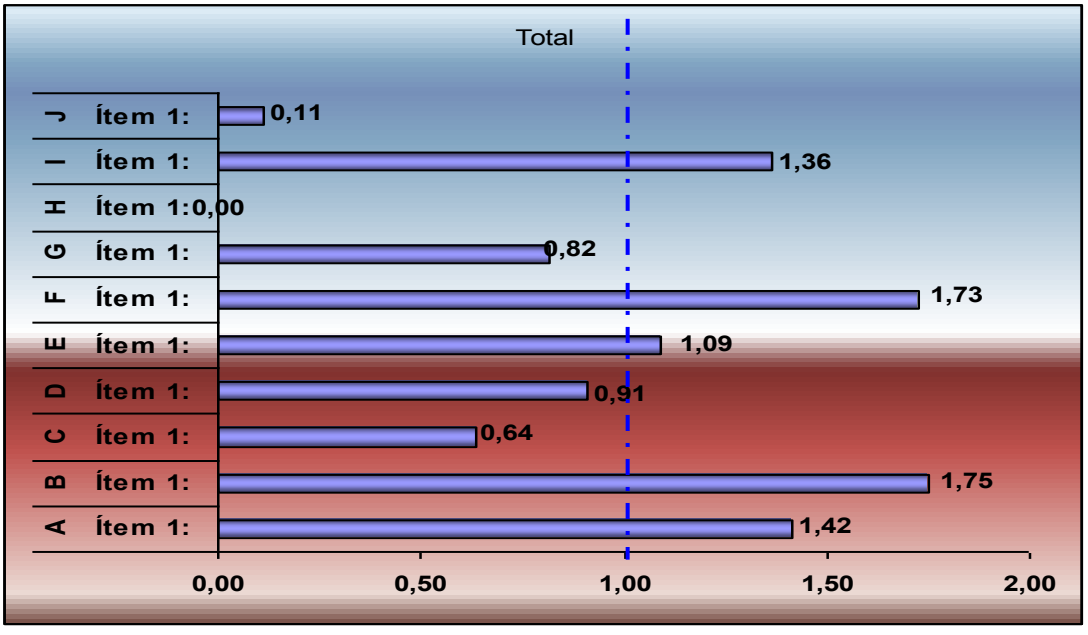
Por ello, la empresa J debe estar en permanente actualización de sistemas, antivirus o cualquier otro programa o dispositivo que mejore su seguridad, además en cuanto al personal que trabaja en la empresa debe capacitarse y orientarse a que respeten y cumplan con los requisitos y medidas tomadas por la organización. También debieran agregar afiches que prohíban ingerir alimentos o líquidos cerca de los equipos computacionales, el ingreso con disquete o dispositivos que provienen de algún uso desconocido de otro lugar.

A continuación, se mostraran 7 gráficos por cada Ítems que evalúa la Metodología.

2. Conclusiones por Ítems.

2.1 ÍTEM 1: Objetivo Organizaciones en Informática

EMPRESA	ÍTEMS	Total	Clasificación
A	Ítem 1:	1,42	Muy Importante
B	Ítem 1:	1,73	Muy Importante
C	Ítem 1:	0,64	Poco Importante
D	Ítem 1:	0,91	Importante
E	Ítem 1:	1,09	Importante
F	Ítem 1:	1,73	Muy Importante
G	Ítem 1:	0,82	Importante
H	Ítem 1:	0,00	NO aplicable
I	Ítem 1:	1,36	Muy Importante
J	Ítem 1:	0,11	Prácticamente Nulo
	Promedio	**1,40**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

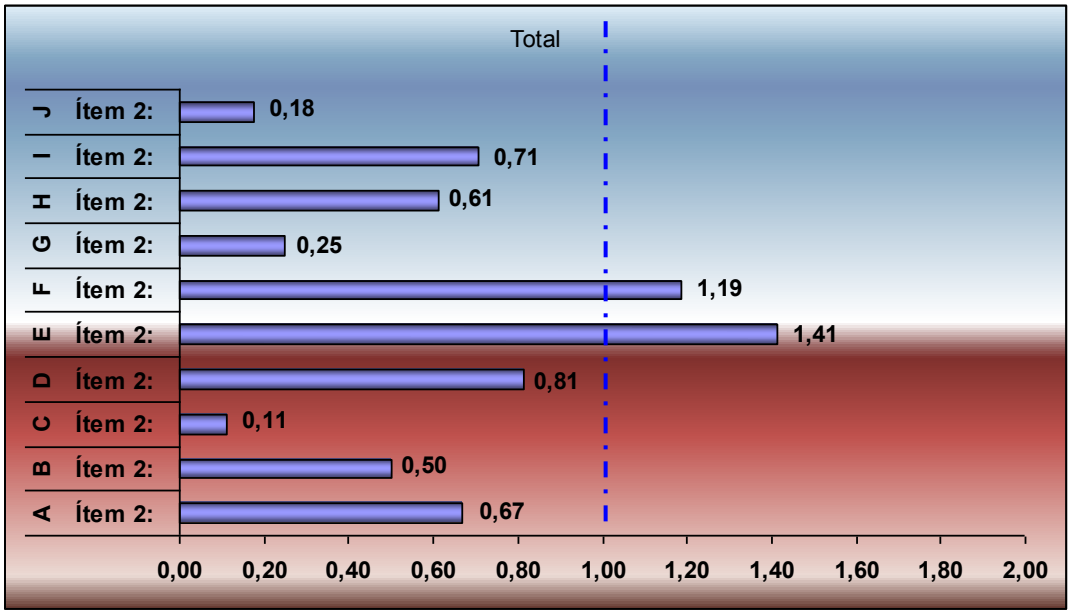
Al evaluar el Ítems 1, existen 4 empresas que arrojan resultados que están dentro del nivel de riesgo clasificados como **"Muy Importante",** 3 empresas como **"Importante",** 1 empresa como **"Poco Importante"**, 1 empresa como **"Prácticamente Nulo**" y 1 empresa como **"No Aplicable**".

El resultado anterior, demuestra lo sub-desarrollado que nos encontramos en cuanto a los Objetivos Organizacionales en Informática, que apunten a establecer una estructura organizacional adecuada para soportar los cambios y necesidades tecnológicas.

La empresa H tiene una clasificación "No Aplicable" porque es un establecimiento educacional y como es sabido, el objetivo de estas instituciones es enseñar y facilitar el manejo de una gran herramienta como lo es el Computador, por lo que sus mayores esfuerzos económicos apuntan a que todo el alumnado tenga acceso al manejo y aprendizaje del computador. Pero seria bueno para la organización analizar los puntos tratados en este ítem, que sin duda, le ayudaría a mejorar lo que actualmente existe.

2.2 ÍTEM 2: Seguridad Física Ambiental

EMPRESA	ÍTEM	Total	Clasificación
A	Ítem 2:	0,67	Poco Importante
B	Ítem 2:	0,50	Poco Importante
C	Ítem 2:	0,11	Prácticamente Nulo
D	Ítem 2:	0,81	Importante
E	Ítem 2:	1,41	Muy Importante
F	Ítem 2:	1,19	Importante
G	Ítem 2:	0,25	Prácticamente Nulo
H	Ítem 2:	0,61	Poco Importante
I	Ítem 2:	0,71	Poco Importante
J	Ítem 2:	0,18	Prácticamente Nulo
	Promedio	**0,92**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

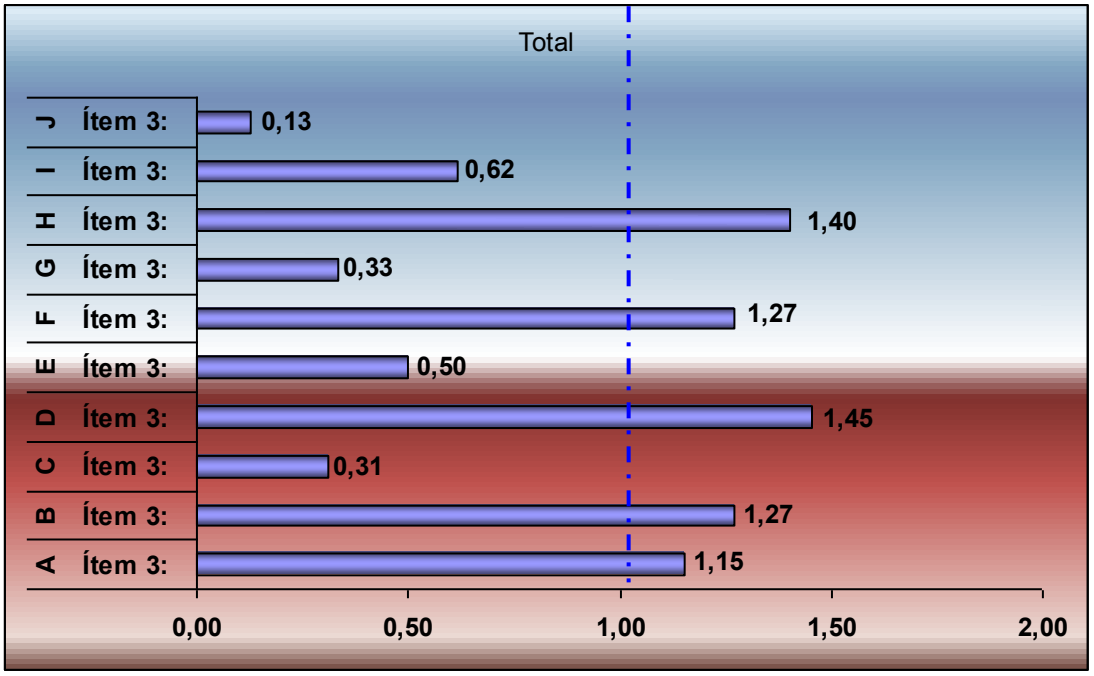
Al evaluar el Ítems 2, hay 3 empresas que arrojan resultados que están dentro del nivel de riesgo clasificados como **"Prácticamente Nulo",** 4 empresas como **"Poco Importante",** 2 empresas como **"Importante"** y 1 empresa como **"Muy Importante".**

Es este Ítem las empresas están en su mayoría bien evaluadas con respecto a su nivel de Riesgo en Seguridad Informática, debido a que el 40% está clasificada como "Poco Importante, 30% como "Prácticamente Nulo" y 20% como "Importante", con estos resultados obtenidos podemos concluir que es muy baja la probabilidad de que ocurra un problema que sea producto de alguna falla que involucre la Seguridad Ambiental.

Lo anterior, nos indica que las empresas se han preocupado de otorgarles a sus trabajadores un ambiente lo más agradable posible, donde por supuesto beneficia la seguridad tanto personal como el de sus herramientas de trabajos (computadores).

2.3 ÍTEM 3: Seguridad de acceso físico a las áreas críticas

EMPRESA	ÍTEM	Total	Clasificación
A	Ítem 3:	1,15	Importante
B	Ítem 3:	1,27	Muy Importante
C	Ítem 3:	0,31	Poco Importante
D	Ítem 3:	1,45	Muy Importante
E	Ítem 3:	0,50	Poco Importante
F	Ítem 3:	1,27	Muy Importante
G	Ítem 3:	0,33	Poco Importante
H	Ítem 3:	1,40	Muy Importante
I	Ítem 3:	0,62	Poco Importante
J	Ítem 3:	0,13	Prácticamente Nulo
	Promedio	**1,21**	



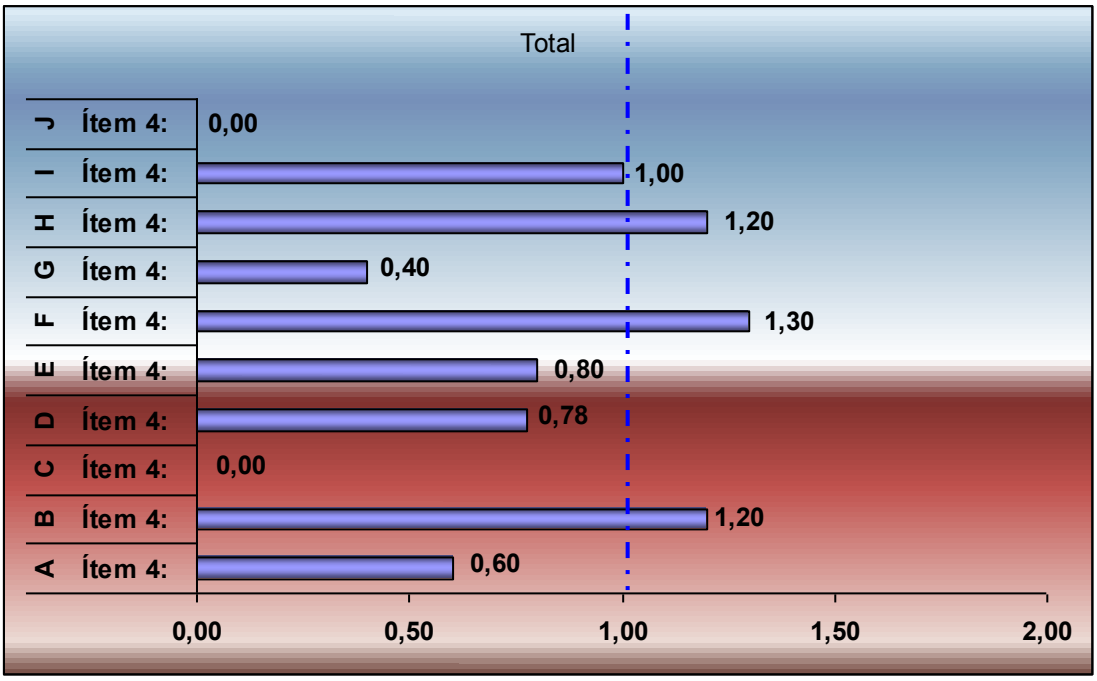
Según lo expuesto en el gráfico se puede comentar lo siguiente:

Al evaluar el Ítems 3, existen 4 empresas que arrojan resultados que están dentro del nivel de riesgo clasificados como **"Muy Importante",** 4 empresas como **"Poco Importante",** 1 empresa como **"Importante",** 1 empresa como **"Prácticamente Nulo"**

Los resultados anteriores, demuestran la poca importancia que las empresas le otorgan a la restricción a las áreas críticas donde se ubican los Servidores y computadores, además se utiliza muy poco los avisos visuales para restringir el acceso. Por ejemplo; en una de las empresas que se visitó, nos sorprendió lo fácil que era acceder al Servidor de la empresa. Además no contaba con los más mínimos resguardos necesarios, para que algún funcionario lo pasare a llevar. Por ello, en este punto debe mejorarse bastante, debido a que el fácil acceso a las áreas criticas, puede llegar a ser muy perjudicial y en algunos casos los daños son irreparables.

2.4 ÍTEM 4: Mantenciones y reparaciones de los equipos computacionales.

EMPRESA	ÍTEM	Total	Clasificación
A	Ítem 4:	0,60	Poco Importante
B	Ítem 4:	1,20	Importante
C	Ítem 4:	0,00	Prácticamente Nulo
D	Ítem 4:	0,78	Importante
E	Ítem 4:	0,80	Importante
F	Ítem 4:	1,30	Muy Importante
G	Ítem 4:	0,40	Poco Importante
H	Ítem 4:	1,20	Importante
I	Ítem 4:	1,00	Importante
J	Ítem 4:	0,00	Prácticamente Nulo
	Promedio	**1,04**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

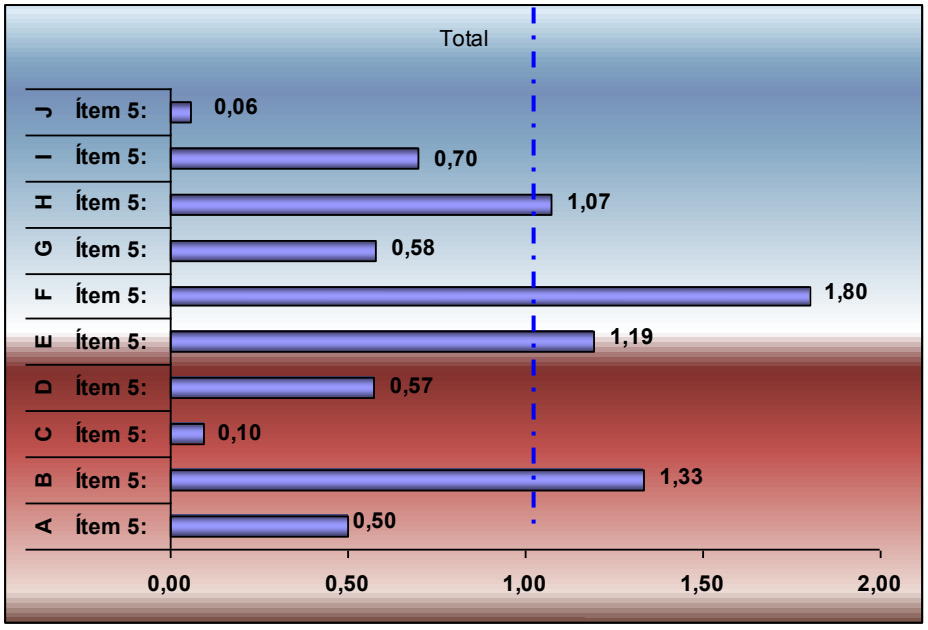
Al evaluar el Ítems 4, hay 5 empresas que arrojan resultados que están dentro del nivel de riesgo clasificados como **"Importante",** 1 empresas como **"Muy Importante",** 2 empresas como **"Poco Importante",** 2 empresas como **"Prácticamente Nulo".**

El resultado anterior, indica que la mayoría de las empresas busca que funcionen sus sistemas y en caso de fallas tratan de repararlos lo más rápido posible, pero son muy pocas las empresas que trabajen en prevenir y anticiparse a las posibles fallas, que se podrían evitar con una programada mantención y por supuesto acompañado con un buen plan de contingencia.

Un buen aseo, limpieza y mantención de los equipos computacionales, puede ser de gran ayuda a la hora de necesitarlos, por lo que se recomienda que no solamente se realicen reparaciones, sino que también exista un buen cuidado preventivo de ellos, para el correcto y continuo funcionamiento de los computadores.

2.5 ÍTEM 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados (virus, hackers, etc.)

EMPRESA	ÍTEM	Total	Clasificación
A	Ítem 5:	0,50	Poco Importante
B	Ítem 5:	1,33	Muy Importante
C	Ítem 5:	0,10	Prácticamente Nulo
D	Ítem 5:	0,57	Poco Importante
E	Ítem 5:	1,19	Importante
F	Ítem 5:	1,67	Muy Importante
G	Ítem 5:	0,58	Poco Importante
H	Ítem 5:	1,07	Importante
I	Ítem 5:	0,70	Poco Importante
J	Ítem 5:	0,06	Prácticamente Nulo
	Promedio	**1,13**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

Al evaluar el Ítems 5, existe 2 empresas que arroja un resultado que está dentro del nivel de riesgo clasificado como **"Muy Importante",** 2 empresas como

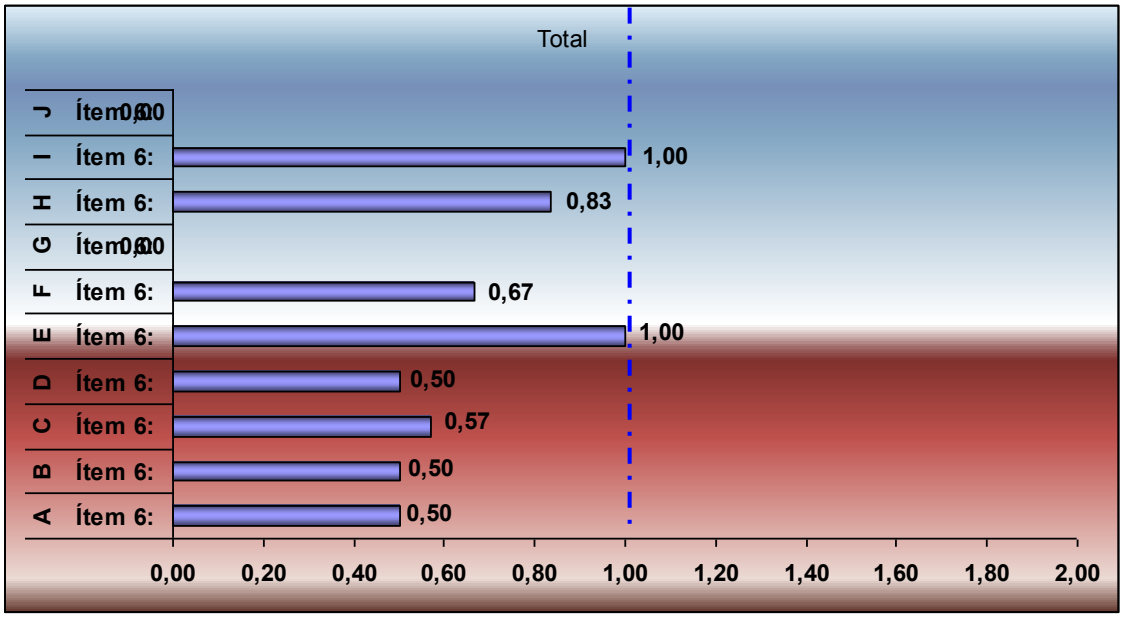
"Importante", 4 empresas como **"Poco Importante"**, y 2 empresas como **"Prácticamente Nulo".**

El resultado anterior, nos indica que en su mayoría las empresas se han preocupados de tomar medidas, poniendo barreras de entrada para los hackers, virus, etc. Un dato curioso, pero real. Una empresa de la muestra fue vulnerada su seguridad informática y tomó como medida contratar a un hackers para proteger e impedir la entrada a intrusos no deseados. Pero lamentablemente se toman medidas y se reacciona una vez que haya pasado algún desastre y no se trabaja en prevenir.

En este aspecto las empresas suelen preocuparse, pero la mayoría de ellas, sólo protege los aspectos mas básicos que existen, por lo que es fundamental que las políticas o medidas que se toman para proteger la seguridad lógica, estén en permanente actualización, porque todos los días se están inventando nuevos programas para vulnerar las barreras de entrada que ponen las empresas, para dañar los sistemas proteger sus recursos tecnológicos.

2.6 ÍTEM 6: Medidas de Seguridad para respaldar la información

EMPRESA	ÍTEM	Total	Clasificación
A	Ítem 6:	0,50	Poco Importante
B	Ítem 6:	0,50	Poco Importante
C	Ítem 6:	0,57	Poco Importante
D	Ítem 6:	0,50	Poco Importante
E	Ítem 6:	1,00	Importante
F	Ítem 6:	0,67	Poco Importante
G	Ítem 6:	0,00	Prácticamente Nulo
H	Ítem 6:	0,83	Importante
I	Ítem 6:	1,00	Importante
J	Ítem 6:	0,00	Prácticamente Nulo
	Promedio	**0,80**	



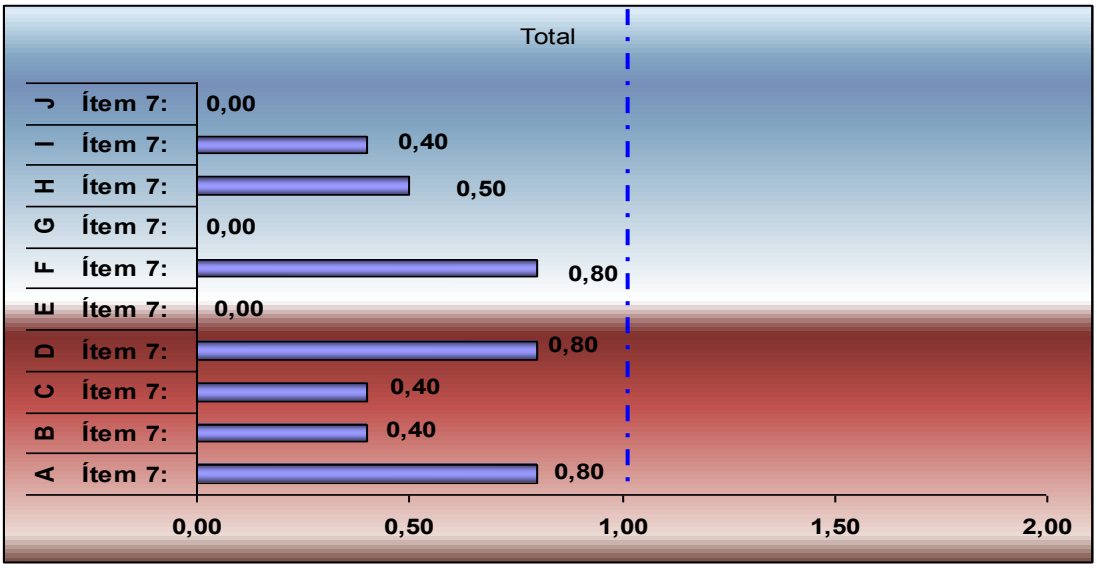
Según lo expuesto en el gráfico se puede comentar lo siguiente:

Al evaluar el Ítems 6, existen 3 empresas que arrojan resultados que están dentro del nivel de riesgo clasificados como **"Importante",** 5 empresas como "**Poco Importante**" y 2 empresas como "**Prácticamente Nulo**",

El resultado anterior, señala que las empresas están respaldando su información, pero no todas en forma diaria, esto lo realizan debido a que saben que es muy costoso reponer y a veces es irreversible el daño que puede provocar la pérdida de la información. En la visita que se hizo durante el desarrollo de la presente Memoria, nos percatamos que si bien se estaba guardando respaldos de la información, estas no se estaban dejando en lugares adecuados, así como por ejemplo, en una empresa dejaba los respaldos en el mismo lugar donde se encontraba el Servidor, lo ideal, es que se guarde en un lugar geográfico distinto al Servidor, un buen ejemplo, es el atentado a las torres gemelas de New York, la mayoría de las empresas ubicadas en esas dependencias pudieron seguir operando a los días siguientes.

2.7 ÍTEM 7: Programas que protegen la información para que no sea interceptada y/o modificada.

EMPRESA	ÍTEM	Total	Clasificación
A	Ítem 7:	0,80	Importante
B	Ítem 7:	0,40	Poco Importante
C	Ítem 7:	0,40	Poco Importante
D	Ítem 7:	0,80	Importante
E	Ítem 7:	0,00	Prácticamente Nulo
F	Ítem 7:	0,80	Importante
G	Ítem 7:	0,00	Prácticamente Nulo
H	Ítem 7:	0,50	Poco Importante
I	Ítem 7:	0,40	Poco Importante
J	Ítem 7:	0,00	Prácticamente Nulo
	Promedio	**0,59**	



Según lo expuesto en el gráfico se puede comentar lo siguiente:

Al evaluar el Ítems 7, hay 3 empresas que arrojan resultados que están dentro del nivel de riesgo clasificados como **"Importante",** 4 empresas como "**Poco Importante**" y 3 empresas como "**Prácticamente Nulo**".

El resultado anterior, indica que en general el riesgo en el traslado de la información es bajo, pero debemos estar consientes, que como se ha dicho en anteriores ocasiones, la información es muy importante para las organizaciones, debido a ello, estas deben tomar las medidas necesarias para que la información no sea interceptada por personas no autorizadas. Hoy en día la Internet es fundamental para el desarrollo y crecimiento de los negocios de una empresa, debido a esto existe la necesidad de programas y herramientas para filtrar o encriptar la información, ya que por cualquier robo o perdida de información esta no les sea útil a los receptores no autorizados.

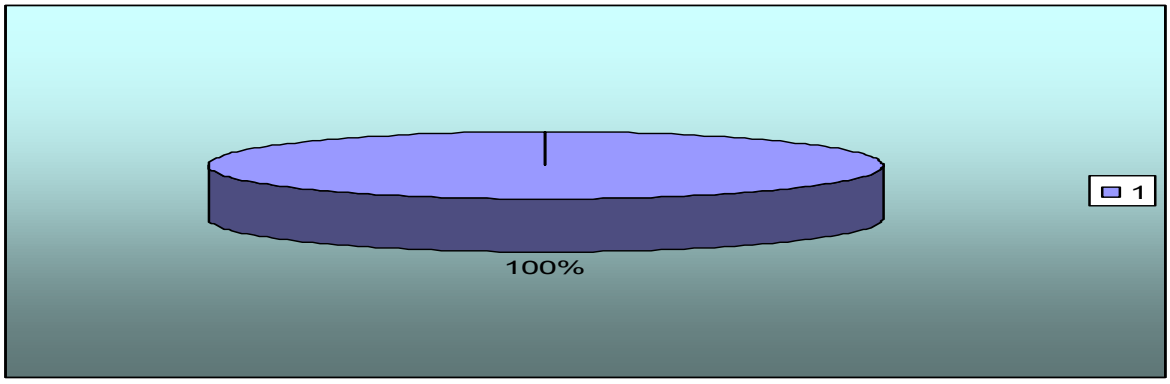
Los siguientes gráficos se enfocaron según nuestro criterio de Auditor, donde se eligieron estándares considerados claves dentro de la seguridad informática.

El primer gráfico que se señala a continuación apunta al ámbito de la seguridad física de cualquier organización. Por ello, dentro de esta seguridad se ha escogido el estándar relacionado con la UPS, sistema de alimentación ininterrumpido, sin duda, un aspecto fundamental para el correcto y constante funcionamiento de las tareas o actividades que se desarrollan en el transcurso de una empresa, tal dispositivo asegura que por cualquier causa de un corte de energía, los equipos computacionales sigan funcionando perfectamente una cantidad de tiempo determinado, (esto va a depender de las características de la UPS) para guardar la información.

3. Conclusiones de una muestra de estándares claves.

3.1 Estándar: ¿La empresa cuenta con un Sistema de Alimentación Ininterrumpido (U.P.S)?.

EMPRESA	ÍTEM	RESPUESTA	Total	Clasificación
A	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
B	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
C	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
D	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
E	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
F	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
G	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
H	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
I	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
J	Ítem 2: Seguridad Ambiental	SI	0.00	Prácticamente Nulo
		Promedio	**0.00**	



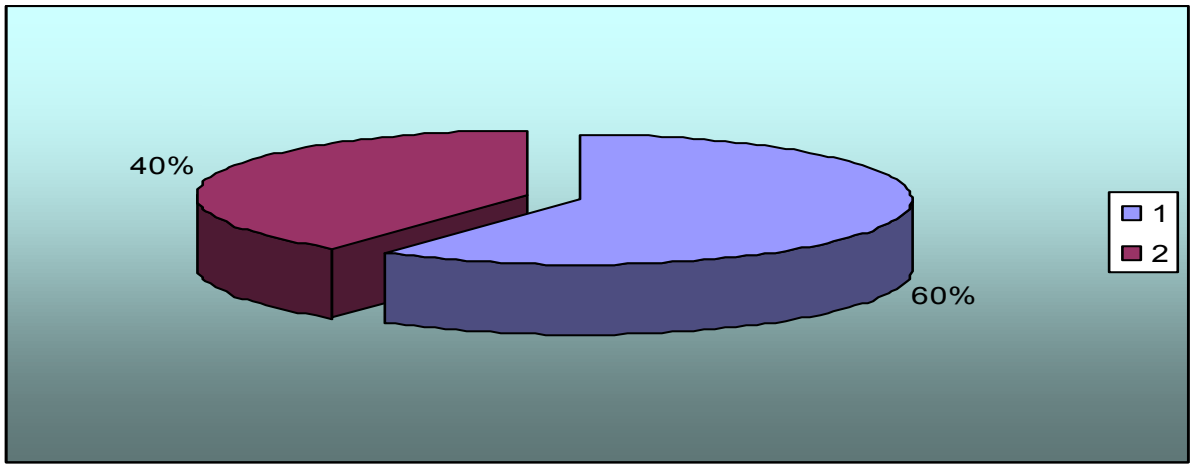
Aquí se puede concluir, que todas las empresas cuentan con este dispositivo de seguridad de alta importancia, arrojando niveles de riesgo en este aspecto prácticamente nulos.

Lo que queda por reforzar, es la actualización y mejora de este dispositivo de seguridad, ya que en algunas oportunidades una buena UPS puede ahorrar bastantes costos en caso de provocarse algún desastre.

Enseguida se analizará otra pregunta relacionada con la seguridad física de una Empresa.

3.2 Estándar: ¿La empresa cuenta con un dispositivo firewall?

EMPRESA	ÍTEM	RESPUESTA	Total	Clasificación
A	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	NO	2.00	Máximo
B	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	NO	2.00	Máximo
C	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
D	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
E	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
F	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	NO	2.00	Máximo
G	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
H	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	NO	2.00	Máximo
I	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
J	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
		Promedio	**1.14**	



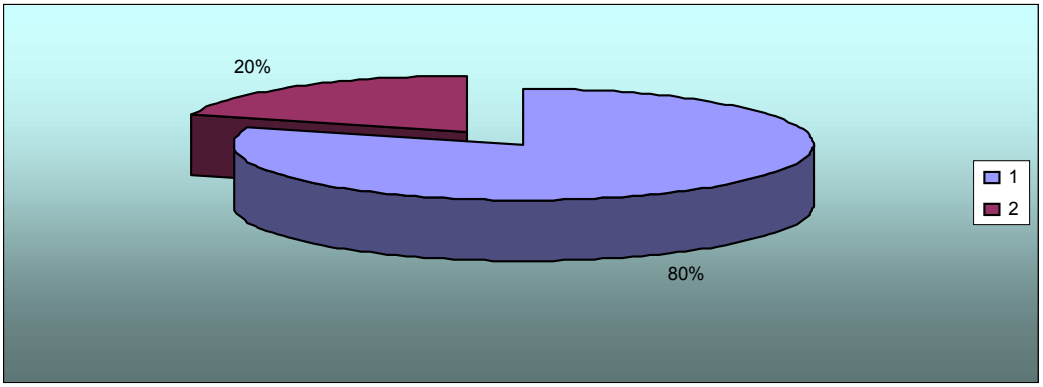
En el gráfico señalado anteriormente se puede concluir que no todas las empresas cuentan con un firewall, lo cual es una situación muy preocupante, debido a que todas ellas cuentan con el uso de Internet. El 40% de ellas no cuenta con un firewall, lo cual es un porcentaje demasiado elevado para este ámbito, provocando un riesgo considerable para la vulnerabilidad en la entrada de personas no autorizadas a los sistemas que manejan las distintas empresas.

Hoy en día tener acceso a la Red es fundamental para el desarrollo y competitividad empresarial, por lo tanto, las empresas deben contar con un dispositivo firewall para la protección de su información y no solamente las empresas, debido a que sin un firewall, los computadores de una Organización o incluso del hogar se exponen directamente al ataque de extraños. Esto significa que la seguridad de los computadores está en constante peligro, más aún si la conexión Internet es de banda ancha, ya que al estar todo el día conectado se transforma en un blanco fácil de ataques mal intencionados.

Desde el punto de vista de la seguridad lógica, se analizará lo siguiente:

3.3 Estándar: ¿Al personal de la empresa, se le otorga una password, para acceder a los sistemas de la empresa?

EMPRESA	ÍTEM	RESPUESTA	Total	Clasificación
A	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
B	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	NO	2.00	Máximo
C	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
D	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
E	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
F	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	NO	2.00	Máximo
G	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
H	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
I	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
J	Ítem 5: Barreras de Entrada, que impiden y controlan el acceso a los usuarios no autorizados	SI	0.00	Prácticamente Nulo
		Promedio	**0.57**	



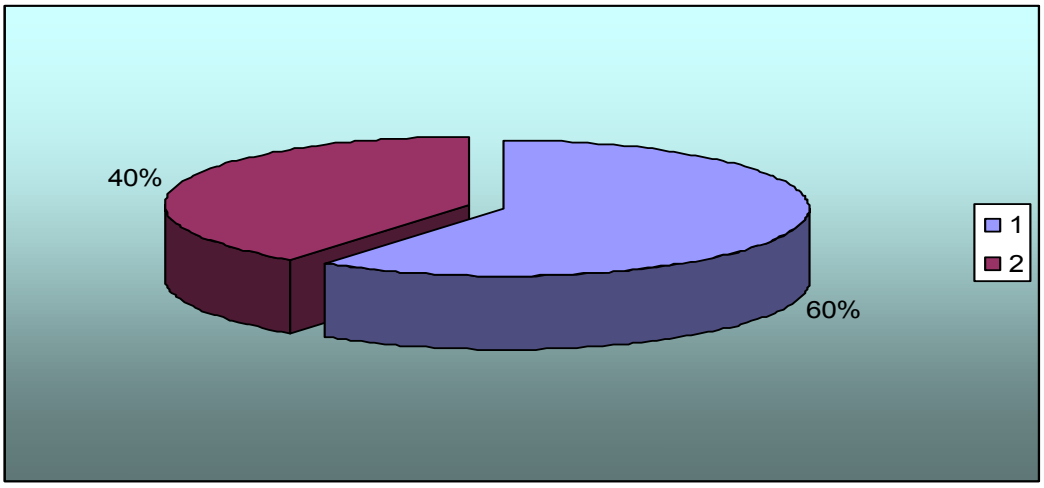
El tema de las password es primordial para una seguridad informática, no tan sólo es poseerlas sino también deben ir de la mano con la privacidad, estas deben ser personales y de acuerdo a un perfil de cada usuario.

De las 10 empresas evaluadas 8 de ellas exigen una password para el ingreso a los computadores, es decir, un 80% de las empresas. Este porcentaje es muy bueno reflejando que en este aspecto las cosas están bien, pero hay que tener mucho cuidado aquí, debido a que esto puede ser engañador, debido a que si bien una gran cantidad de la muestra cuenta con la exigencia de una password, dentro de estas empresas no todas cumplen con condiciones adecuadas que se deben tener en cuenta en el tema de las password como son: cambiar la password cada cierto tiempo determinado, que la password obligue a tener un número de caracteres y que estos sean alfanuméricos, además al fallar 2 o 3 intentos en el ingreso el sistema debiera bloquearse.

Otro aspecto en cuanto a seguridad lógica que se analizará será el de los respaldos de la información, llamados backups o copias de seguridad.

3.4 Estándar: ¿La empresa realiza backups diariamente (copias de seguridad)?

EMPRESA	ÍTEM	RESPUESTA	Total	Clasificación
A	Ítem 6: Medidas de Seguridad para respaldar la información	NO	2.00	Máximo
B	Ítem 6: Medidas de Seguridad para respaldar la información	NO	2.00	Máximo
C	Ítem 6: Medidas de Seguridad para respaldar la información	SI	0.00	Prácticamente Nulo
D	Ítem 6: Medidas de Seguridad para respaldar la información	SI	0.00	Prácticamente Nulo
E	Ítem 6: Medidas de Seguridad para respaldar la información	SI	0.00	Prácticamente Nulo
F	Ítem 6: Medidas de Seguridad para respaldar la información	NO	2.00	Máximo
G	Ítem 6: Medidas de Seguridad para respaldar la información	SI	0.00	Prácticamente Nulo
H	Ítem 6: Medidas de Seguridad para respaldar la información	NO	2.00	Máximo
I	Ítem 6: Medidas de Seguridad para respaldar la información	SI	0.00	Prácticamente Nulo
J	Ítem 6: Medidas de Seguridad para respaldar la información	SI	0.00	Prácticamente Nulo
		Promedio	**1.14**	



El respaldo de la información es una medida o política que toda empresa debe tener, sin importar la envergadura o tamaño de la empresa, este aspecto siempre debe estar presente en una organización independientemente de su finalidad.

De las 10 empresas evaluadas el 100% de ellas realiza copias de seguridad a su información, lo cual es un excelente resultado, pero donde se produce un alto nivel de riesgo, es en que estas copias de seguridad no se realizan diariamente, más bien un 40% de ellas no hace un respaldo diario y tampoco todas las empresas guardan estos respaldos en lugares seguros de algún robo o desastre.

CONCLUSIONES

Cuando se presentó la oportunidad de hacer nuestra Memoria, donde íbamos a incursionar en el área informática, nos cuestionamos y fuimos cuestionados, donde se repetía las siguientes interrogantes, ¿Ustedes manejan el lenguaje de programación?, ¿Saben que es una Ram, Disco Duro, Procesador, Router, Firewall, UPS, etc?, a decir verdad sabíamos muy poco y en algunos puntos nada, pero de todas manera quisimos tomar este desafío e incursionar en el área de la Informática y más específicamente en las áreas de seguridad física y lógica en cuanto a su acceso, debido a que nuestro punto primordial nunca fue programar, ni ser expertos en informática, sino que el objetivo fue, realizar una evaluación, desde el punto de vista de un Auditor, a un grupo de empresas de la ciudad de Chillán, de cómo presentan su realidad en cuanto a sus niveles de riesgo en seguridad informática.

Durante el transcurso de la Memoria cada día que pasaba nos dábamos cuenta que no nos habíamos equivocados en tomar el tema, al contrario, se confirmaba la hipótesis de que era muy provechoso recibir opiniones emitidas por profesionales, que si bien no son del área, pueden también emitir observaciones con otro prisma, lo que puede llegar a ser un gran aporte.

En la práctica, tuvimos que entrevistar a distintos trabajadores de importantes empresas en la ciudad de Chillán, en la mayoría de los casos, profesionales expertos y con bastante experiencia laboral, donde podemos comentar que fue una actividad muy satisfactoria y provechosa.

Cada vez que procedíamos a realizar la aplicación de la Metodología, siempre comentábamos como íbamos a encontrar la empresa, muchas veces nos equivocamos, por ejemplo, cuando fuimos a una empresa que es grande a nivel Nacional y además es exportadora de sus productos, nosotros pensábamos que íbamos a encontrar, sofisticados sistemas que estarían resguardados por una

seguridad también de primer nivel, pero en realidad no fue así, nos encontramos con serios problemas en seguridad física y lógica, que no reflejaban el prestigio de su marca. Sin embargo, estaban trabajando para mejorar y se percibió que las ganas estaban, además a futuro se iba a gestionar para invertir en recursos financieros y humanos.

En otra ocasión, cuando fuimos a una empresa pequeña comentábamos que dudábamos encontrar sistemas informáticos sofisticados y mucho menos con un buen nivel de seguridad informática, sin embargo, nos encontramos con un sistema no muy avanzado, con niveles de seguridad informáticos mejorables pero aceptable, lo preocupante, es que al ser una empresa pequeña, la seguridad informática no estaba dentro de las prioridades, porque el objetivo que se esperaba alcanzar con el sistema informáticos era controlar los stock de los productos y ayudar en la gestión de tareas básicas. Por lo tanto, a corto plazo no se veía un mejoramiento sustancial en la seguridad informática física y en sus accesos lógicos.

En conclusión, antes de aplicar la metodología, comentábamos como nos imaginábamos que íbamos a encontrar a las empresas, donde a menudo nos equivocábamos e incluso, antes de entrar a una empresa ha aplicar la metodología, apostábamos una bebida o un helado, es mas en una ocasión ambos especulamos que los niveles de seguridad informáticos se encontrarían bien, por lo tanto, no hubo apuesta, sin embargo, ambos estábamos equivocados, porque era desastroso el nivel se seguridad informáticos encontrado en la empresa.

Con el trabajo realizado en la presente Memoria, podemos comentar que fue muy positivo, debido a que pudimos aprender cosas nuevas, desarrollar nuestras capacidades y analizar un tema muy interesante de la actualidad, donde se pudo observar la realidad de los niveles de seguridad que tienen las empresas. Además el conocimiento adquirido nos ha ayudado en nuestro desempeño profesional, donde constantemente estamos tomando decisiones que afectan a la seguridad de la

información que manejamos, dentro de las funciones desarrolladas en forma diaria en la empresa que estamos trabajando.

Conclusión General, de los resultados obtenidos en la aplicación de la Metodología elegida.

Podemos mencionar que la Memoria expuesta, consta de tres capítulos claramente definidos:

El **Primer Capítulo** es el más extenso, compuesto por un marco introductorio definiendo y conociendo conceptos importantes relacionados con el tema de esta investigación. También se señalan ejemplos de cómo se presenta la seguridad informática a nivel mundial, donde quedo en manifiesto que día a día crecen los esfuerzos por alcanzar niveles óptimos de seguridad informática, debido a que le están dando la importancia que se merece, el asegurar la información obtenida y generada en las organizaciones, donde la experiencia de algunas de ellas enseñan a otras empresas a cuidar de este activo tan preciado como lo es la información, pero según los estudios hechos a nivel mundial, indican que falta para llegar a tener los niveles óptimos, donde la actualización de los sistemas de seguridad debe ser una preocupación constante.

El **Segundo Capítulo**, esta enfocado a la metodología de seguridad informática, dando ejemplos de algunas ya existentes y definiendo la metodología estándar que fue la base para el desarrollo del presente trabajo, donde se eligió una muestra de 10 empresas de la ciudad de Chillán, para aplicar la metodología elegida. También se señaló en este capítulo, como se llevó a cabo el desarrollo y evaluación de la metodología, dando a conocer las diferentes técnicas de Auditoria que fueron utilizadas, con la finalidad de entregar la evidencia suficiente y competente para cumplir el objetivo.

Por último, el **Tercer Capítulo**, esta compuesto por los resultados que arrojo la aplicación en terreno de la metodología, donde se entregaron conclusiones por Ítems, por algunas preguntas claves y por cada una de las empresas involucradas en el análisis. Estos resultados fueron analizados e interpretados, para finalmente entregar nuestra opinión sobre los distintos niveles de seguridad informática que presentaron las empresas evaluadas, donde las conclusiones están dirigidas a empresas sin identificar su identidad, con la finalidad de proteger la confidencialidad de cada una de ellas, respetando lo que se planteo al principio de esta investigación, pudiendo de esta manera, llegar a las conclusiones finales de la evaluación, entregando las debilidades y fortalezas que poseen las diferentes empresas.

Es así como podemos indicar que el riesgo en seguridad informática en las áreas físicas y acceso lógico es alto, porque los resultados así lo demuestran, cabe señalar, que existen empresas que han tomado conciencia sobre la importancia que tiene la seguridad informática para proteger sus equipos computacionales y su activo más importante que es la información. A nuestro juicio lo más importante para resguardar la información es estar en permanente alerta y actualización, debido a que la informática es una ciencia que día a día avanza a pasos agigantados, dejando a su paso herramientas informáticas que exigen una constante actualización, para el normal funcionamiento y desarrollo de las organizaciones.

Ahora vamos exponer conclusiones por cada ítem, donde destacaremos lo más relevante:

Ítems 1: Objetivos Organizacionales en Informática

En este ítem la mayoría de las empresas, el nivel de riesgo estuvo clasificado como “Muy Importantes” e “Importantes”, lo que da una señal que no existe una estructura sólida para que se desarrolle y perdure en el tiempo un nivel óptimo de seguridad informática, porque en este ítems se revisa si existen por ejemplo: planes

a largo plazo para el departamento informático, políticas para la planificación o dirección del departamento de informática y otros estándares más que están contemplados en este ítems. Lo anterior, es resultado de que en nuestra provincia son pocas las empresas que destinan los recursos humanos y financieros necesarios, para formar una estructura sólida que abarque los estándares que se desarrollan en este ítems, y así evitar que sea vulnerada la seguridad informática de la organización. Lo que si quedo claro, es que las personas encargadas tienen las ganas de mejorar y cada día se trabaja para ello, pero las decisiones de destinar recursos las toman los altos mandos. Hubo una empresa, a la cual no se pudo aplicar este ítem, el argumento fue que el rubro de la organización es la educación, donde enseña las bondades y beneficios que tiene el saber utilizar de buena forma una gran herramienta como lo es el computador, por lo tanto, ellos cumplían su objetivo primordial sin tener esas políticas, pero de todas maneras, sería bueno para la organización analizar los puntos tratados en este ítem, debido a que ellos se encuentran en proceso de implementar su pagina Web, y quien sabe mas adelante pueden llegar a realizar operaciones en Internet, ya sean matriculas u otras.

Ítems 2: Seguridad Ambiental.

En este ítem la mayoría de las empresas sus niveles están clasificados como “Poco Importante” y “Prácticamente Nulo”, el cual, nos indica que las empresas se han preocupado de la seguridad ambiental, donde se han tomado medidas para minimizar el riesgo y de esta forma resguardar los recursos informáticos y humanos, pero de igual forma tuvimos una empresa dedicada al trasporte de pasajeros con una mala evaluación en este ámbito, ya que su infraestructura no era la adecuada, para proteger sus activos. Donde se ubicaba el servidor, la construcción no era de material sólido y tampoco contaba con cortafuegos, el cableado estaba desprotegido y no constaba con extintores en caso de incendio, por lo que sus niveles de riesgo en seguridad ambiental eran altísimos, pero como se dijo anteriormente la mayoría de las empresas, si constaban con las medidas necesarias para proteger este ámbito.

Ítems 3: Seguridad de acceso a las áreas críticas.

En este ítems se encuentran los niveles de seguridad informática, clasificados como “Muy Importante” y Poco Importante”, lo cual refleja que no todas las organizaciones le dan la importancia que se merecen a los puntos tocados por este ítem, el cual, evalúa por ejemplo: la ubicación del servidor y de los computadores; la restricción al acceso de personas no autorizadas; que existan avisos visuales que restrinjan el acceso a la sala donde se ubica el servidor, entre otros. Sin embargo, cuando estábamos en una empresa se observó que el servidor estaba expuesto a los rayos de sol y no estaba en un lugar seguro, por ende, era fácil vulnerar su seguridad informática, donde el que quisiera podría cuasar daño a la empresa, deteniendo sus sistemas, con solo botar o desconectar el servidor. Estábamos enfrente de un riesgo y daño inminente

Ítems 4: Mantención, controles y reparaciones del equipamiento.

En este ítem la mayoría de las empresas, tiene sus niveles de seguridad clasificados como “Importante”, esto es preocupante porque como sabemos, por lo general, las empresas les interesa que no fallen sus sistemas computacionales, pero se han olvidado de tomar algunas medidas que le ayudarían a minimizar el riesgo, para que sus sistemas informáticos no fallen, porque como dice un dicho popular *“más vale prevenir que curar”.* Los resultados nos indican que son muy pocas las empresas que hacen mantención a sus equipos computacionales, por ende, se desgastan más haciendo reparaciones que mantenciones, lo que trae como consecuencia un mayor gasto o costo para la empresa, por que sería distinto si hay que cambiar una pieza o todo el computador a un trabajador, mientras se está haciendo la mantención, porque por lo general se hacen fuera del horario o cuando el PC no está siendo ocupado, en cambio, si por una mala o nula mantención no funciona el computador, la persona deja de trabajar y a lo mejor el interrumpir su trabajo provoca serios trastornos en los procesos de toda la organización, lo que

conlleva a que los costos sean mayores. Por ejemplo: En una empresa de prestigio de la ciudad de Chillán, tubo un percance con el Servidor, debido al no realizar mantenciones periódicas, estuvo toda una tarde sin poder seguir con sus procesos rutinarios y lo más curioso es que contaban con un Servidor de emergencia, el cual, se activaba sólo cuando fallaba el principal, pero debido a que hace bastante tiempo que no se activaba y que no tenia una mantención periódica, tampoco funcionó. Hay que comentar que se aprendió la lección y ahora es una de las empresas, que su nivel de riesgo en este ítem es “Prácticamente Nulo”, la empresa se dedica a varios rubros, donde los principales son la línea blanca, automotriz y electricidad.

Ítems 5: Barreras de entrada, que impiden y controlan el acceso a los usuarios no autorizados (virus, hackers, etc.).

En este ítem la mayoría de las empresas sus niveles en seguridad informática están clasificados como “Poco Importante” y “Prácticamente Nulo”, lo que da una señal, que las organizaciones están preocupadas en tomar medidas, para impedir el ingreso de intrusos indeseables. Un hecho anecdótico que ocurrió en una empresa dedicada a producción y ventas de cecinas, la cual, tuvo serios problemas para impedir que intervinieran y controlar el ingreso de usuarios no autorizados, debido a que en reiteradas ocasiones fueron visitados por algunos hackers, que trajo como consecuencia, interrupciones en el normal funcionamiento de la empresa y además muchos dolores de cabeza, por ende, tomaron como medida contratar un hacker para proteger sus sistemas informáticos.

Ítems 6: Medidas de Seguridad para respaldar la información.

En este ítem la mayoría de las empresas sus niveles de riesgo informáticos están clasificados como “Poco Importante” y Prácticamente Nulo**”,** lo que muestra lo preocupadas que están las empresas por respaldar la información, debido a que saben que el no hacerlo, podrían traerles daños que en ocasiones pueden ser

irreparables. Sin embargo, detectamos que no todas las empresas lo realizan diariamente, es comprensible debido a los costos que conllevaría tomar esta medida, pero lo que no es aceptable, es que se hagan respaldos y se dejen en el mismo lugar físico, donde se encuentra el Servidor, por ejemplo: cuando visitamos una empresa nos dimos cuenta que los respaldos estaban, literalmente hablando, encima del Servidor. Siendo lo ideal, que se deje en un lugar geográfico distinto, por ejemplo; enviar los respaldos a una sucursal ubicada en la ciudad de Concepción, considerando que la Casa Matriz esta en la ciudad de Chillán. Además se detectó que en la mayoría de las empresas, se realizan respaldos, pero no se chequean si están en condiciones de ser utilizados en cualquier momento.

Ítems 7: Programas que protegen la información para que no sea interceptada y/o modificada.

En este ítem la gran mayoría de las empresas tiene sus niveles de seguridad informática clasificados como “Poco Importante” y “Prácticamente Nulo”, lo que da una clara señal que se han tomado medidas y han destinados recursos para comprar programas que protejan su información. Con la experiencia que en la actualidad se cuenta, en relación, al daño que pueden provocar los virus a los sistemas, por ende, se han preocupado de contar con antivirus, lo cuales, son actualizados periódicamente.

Por todo lo investigado y expuesto por la presente Memoria podemos concluir que a las empresas, les falta trabajar bastante en seguridad informática, pero la percepción que nos quedo cuando fuimos a desarrollar el tema en terreno, es esperanzador, porque todas las personas entrevistadas estaban conciente que aún faltaba mucho por mejorar en lo que ha seguridad informática se refiere, pero lamentaban en no contar con recursos económicos necesarios para mejorar su seguridad, por lo tanto, es necesario que los altos mandos de las empresas, evalúen este tema y consideren dentro de su planificación financiera asignar mayores

recursos, donde el objetivo sea constar con el personal adecuado y la tecnología necesaria, para alcanzar las metas organizacionales que deseen lograr.

No podemos dejar de mencionar, la buena voluntad de las empresas en prestar su cooperación, sin duda, sin ellas no hubiese sido posible llegar al objetivo, para ver la realidad presente en seguridad informática en cuanto al acceso lógico y físico que tienen las organizaciones. La disponibilidad de tiempo, que nos otorgaron los trabajadores de las distintas empresas fue esencial, debido a que se pudo conocer tranquilamente toda la infraestructura del área informática, percatándonos físicamente, comprobando las cualidades y falencias de sus sistemas.

EMPRESA	NOMBRE
1. Rabie S.A.	Cecilia del Valle
	Martín Ríos
2. Carnes Ñuble	Rodrigo Romero
3. Hospital Herminda Martín de Chillán	Pablo Ibarra
	Gastón Vergara
4. Cooperativa Copelec	Eduardo Laudrie
	Octavio Muñoz
5. Librería Blue-Mix	Patricio Pastene
6. Ferretería Madrid	Claudio Jara
7. Rodaméndez	Nelson Ibañez
8. Cecinas Villablanca	Mario Villablanca
	Eduardo Moraga
9. INSUCO (Instituto Superior de Comercio).	Pedro Guajardo
	Oscar Becerra
10. Buses Línea Azul	Carlos Retamal

Para finalizar, es preciso comentar, que el trabajo de investigación y desarrollo que está plasmado en la presente Memoria, puede ser utilizado para ser aplicado a cualquier organización, que base sus procesos en sistemas de información

informatizados, donde sería un buen aporte para mejorar a corto y largo plazo los niveles de riesgo en seguridad informática en las áreas de acceso físico y lógico, que fueron tratados en el presente trabajo de investigación. Como sabemos, la seguridad informática es muy amplia y abarca muchos otros puntos, por ende, este trabajo podría servir de base para complementarse y así poder abarcar más áreas de la seguridad informática. Incluso por los resultados obtenidos en la aplicación de la Metodología, creemos que puede ser utilizado para desarrollar un software informático, para facilitar la aplicación, obtención e interpretación de resultados y de esta forma, proporcionar información para gestionar la toma de decisiones más rápida y precisa.

Se hará entrega un Compad Disk a las empresas que se prestaron de buena voluntad, para desarrollar la presente Memoria. Donde se le informará a cada una la letra que se asigno a su empresa.

BIBLIOGRAFÍA

Autores : Del Peso Navarro, Emilio; Piattini Velthuis Mario.
Titulo Publicación : Auditoría informática: un enfoque práctico.
Nº de Edición : 2ª. Edición. Ampl.. y Rev.
Lugar de Publicación : México, Alfaomega.
Año Publicación : 2001
Paginación : 660 p. ; 22 cm.

Autor : Hernández Hernández, Enrique.
Titulo Publicación : Auditoría en informática, un enfoque metodológico y práctico.
Lugar de Publicación : México, CECSA.
Año Publicación : 1995
Paginación : 315 p. il; 25 cm.

Autor : Cepeda Alonso, Gustavo.
Titulo Publicación : Auditoría y control interno.
Lugar de Publicación : Santafé de Bogotá.
Año Publicación : 1997
Editorial : McGraw-Hill Interamericana.
Paginación : 234 p. ; 24 cm.

Autor : Oz, Effy.
Titulo Publicación : Administración de sistemas de información.
Nº de Edición : 2ª. Edición.
Lugar de Publicación : México: Thomson Learning.
Año Publicación : 2001
Paginación : 688 p. : il; 27 cm.

Autor : Colegio de Contadores de Chile.
Titulo Publicación : Normas de Auditoría generalmente aceptadas. (NAGA 23-35)
Lugar de Publicación : Santiago, Chile: Colegio de Contadores de Chile.
Año Publicación : 1997-1999
Paginación : 1 V. (Varias paginaciones); 25 cm.

Autor	: Labadía Bonastre, José Antonio.
Titulo Publicación	: Protección de activos informáticos.
Lugar de Publicación	: Madrid: Mapfre.
Año Publicación	: 1994
Paginación	: 436p. ; 22 cm.

Autor	: Universidad del Bío-Bío Depto. Auditoría e Informática (Chile)
Titulo Publicación	: Conceptos básicos de computación, un poco de historia, configuración computacional, sistemas operativos, conceptos de red, sistemas de información.
Lugar de Publicación	: Chillán, Universidad del Bío-Bío Depto. Auditoría e Informática.
Año Publicación	: 1995
Paginación	: 150 h. : il; 28 cm.

Autor	: Ibarra Ávila, Pablo.
Titulo Publicación	: Auditoría a la seguridad y control de la información en ambiente windows NT
Nº de Edición	: 1ª. Edición
Lugar de Publicación	: Chillán: Universidad del Bío-Bío depto. Auditoría e Informática.
Año Publicación	: 2000
Paginación	: 135 h. : il; 29 cm.

Sitios Web

Sitio 1	http://www.isaca.org/standard Normas de Auditoría de Sistema de Información.
Sitio 2	http://www.microsoft.com Temas varios sobre Seguridad Informática.
Sitio 3	Http://www.segu-info.com.ar Temas varios sobre Seguridad Informática.
Sitio 4	http://www.virusprot.com Noticias, publicaciones sobre Seguridad Informática.
Sitio 5	http://www.monografias.com Trabajos varios relacionados con la Memoria.

Sitio 6	http://www.svetlian.com/seguridad Noticias, publicaciones sobre Seguridad Informática.
Sitio 7	http://www.ine.cl Temas varios sobre las empresas
Sitio 8	http://www.sekureit.com/ Consultora en Seguridad Informática
Sitio 9	http://www.cnnenespanol.com Noticias sobre atentados a violar la Seguridad Informática.
Sitio 10	http://www.elrinconcito.com/ Diccionario de términos informáticos.
Sitio 11	http://www.virusprot.com Temas sobre virus.
Sitio 12	http://www.delitosinformaticos.com/ Informes sobre hechos de vulnerabilidad en Seguridad Informática

ANEXOS

A continuación presentaremos cada una de las empresas que compone la muestra, a la cual se les realizo la evaluación mediante la aplicación de la metodología escogida, la que se concreto con diferentes técnicas de Auditoría.

En primer lugar nombraremos a la empresa Librería Blue Mix, ubicada en la calle 5 de abril Nº 1071. Esta se dedica a la venta minorista y mayorista de útiles de oficina. En esta empresa se entrevisto a el Sr. Patricio Pastene, encargado del área informática, el día 26 de agosto del 2004 a las 12 hrs.

En segundo lugar esta la empresa Ferretería Madrid S.A. ubicada en la calle Isabel Riquelme Nº 671. Esta ofrece una completa variedad de materiales para el hogar y la construcción. En esta empresa se entrevisto el Sr. Claudio Jara, encargado del área informática de la empresa, el día 26 de agosto del 2004 a las 18:30 hrs.

En tercer lugar esta la empresa Cooperativa Copelec, ubicada en la calle 18 de septiembre Nº 688. Esta dedica su principal actividad a la distribución de energía eléctrica, continuando con la comercialización de bienes y servicios. En esta empresa se entrevisto el Sr. Octavio Muñoz, encargado del área informática de la empresa, el día 30 de agosto del 2004 a las 16:00 hrs.

En cuarto lugar esta la empresa de buses Línea Azul, ubicada en la calle Arturo Prat Nº 17. Esta ofrece una completa variedad de materiales para el hogar y la construcción. En esta empresa se entrevisto el Sr. Carlos Retamal, encargado del área informática de la empresa, el día 07 de septiembre del 2004 a las 15:15 hrs.

En quinto lugar esta la empresa Rodamendez Ltda. Ubicada en la calle Arauco Nº 920. Esta ofrece la comercialización, importación y distribución de rodamientos y elementos de transmisión de potencia. En esta empresa se entrevisto el Sr. Nelson Ibáñez, encargado del área informática de la empresa, el día 14 de septiembre del 2004 a las 10:30 hrs.

En sexto lugar esta la empresa Carnes Ñuble S.A. ubicada en Panamericana Norte Km. 3. Esta es una planta faenadora de productos carnívoros para satisfacer las variadas necesidades del consumo. En esta empresa se entrevisto el Sr. Rodrigo Romero, encargado del área informática de la empresa, el día 14 de septiembre del 2004 a las 15:00 hrs.

En séptimo lugar esta la empresa Cecinas Villablanca, ubicada en la Avenida Collin Nº 999. Esta ofrece una completa variedad de cecinas y especialmente longanizas. En esta empresa se entrevisto el Sr. Eduardo Moraga encargado del área informática de la empresa, el día 21 de septiembre del 2004 a las 15:30 hrs.

En octavo lugar esta la empresa INSUCO, Instituto Superior de Comercio, ubicada en la calle Libertad Nº 125. Esta se dedica a educar mediante la enseñanza Técnica Profesional. En esta empresa se entrevisto el Sr. Jorge Becerra, encargado del área informática de la empresa, el día 23 de septiembre del 2004 a las 18:30 hrs.

En noveno lugar esta la empresa Rabie S.A. ubicada en la calle El Roble Nº 770, pisos 8,9 y 10. Esta ofrece la distribución de productos para abastecer al comercio detallista. En esta empresa se entrevisto el Sr. Martín Ríos, en cuanto al área lógica y el Sr. Miguel Astudillo, en cuanto al área física, el día 20 de julio del 2005 a las 15:30 hrs.

En décimo lugar esta la empresa Hospital Herminda Martín, ubicada en la calle Francisco Ramírez Nº 10. Esta ofrece un servicio público a la comunidad. En esta empresa se entrevisto el Sr. Gastón Vergara, encargado del área informática de la empresa, el día 28 de julio del 2005 a las 14:40 hrs.