
MARIA DOLORES CERINI

E-MAIL

DOLORESCERINI@YAHOO.COM.AR
DOLORESCERINI@HOTMAIL.COM

PABLO IGNACIO PRÁ

E-MAIL

PABLO_PIP@YAHOO.COM.AR
PABLOPIP@HOTMAIL.COM



ABSTRACT**PLAN DE SEGURIDAD INFORMÁTICA**

En el presente trabajo final desarrollamos una **auditoría de seguridad informática** y **un análisis de riesgos** en una empresa de venta de automotores, con el fin de relevar la consistencia de los sistemas de información y de control, la eficiencia y efectividad de los programas y operaciones, y el cumplimiento de los reglamentos y normas prescriptas. Como resultado se detallan las debilidades encontradas y se emiten recomendaciones que contribuyan a mejorar su nivel de seguridad.

Esto se llevó a cabo como medio para el desarrollo de un **plan de seguridad informática**, donde se definen los lineamientos de la planeación, el diseño e implantación de un modelo de seguridad con el objetivo de establecer una cultura de la seguridad en la organización. Asimismo, la obliga a redactar sus propios procedimientos de seguridad, los cuales deben estar enmarcados por las **políticas** que conforman este plan.

El propósito de establecer este plan es proteger la información y los activos de la organización, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que debe asumir cada uno de los empleados de la organización.

TRABAJO FINAL

PLAN DE SEGURIDAD

INFORMÁTICA



UNIVERSIDAD CATÓLICA DE CÓRDOBA
FACULTAD DE INGENIERÍA
Escuela de Ingeniería de Sistemas

Presentado por
María Dolores Cerini - Pablo Ignacio Prá

Tutor:
Ing. Aldo Spesso

Octubre de 2002

AGRADECIMIENTOS

Debemos destacar el apoyo incondicional de nuestras familias, quienes supieron tener paciencia y asistirnos en todo lo que estaba a su alcance para que este estudio resulte posible.

También deseamos agradecerles por adelantado porque sabemos que nos seguirán apoyando y ayudando siempre que los necesitemos.

ÍNDICE GENERAL

AGRADECIMIENTOS.....	2
ÍNDICE GENERAL	3
PRÓLOGO.....	5
INTRODUCCIÓN	6
AUDITORÍA DE SEGURIDAD INFORMÁTICA	7
AUDITORÍA DE SEGURIDAD INFORMÁTICA	8
<i>Objetivo General</i>	8
<i>Alcance</i>	8
<i>Metodología Aplicada</i>	9
<i>Normativas Empleadas</i>	10
<i>Informe de Relevamiento</i>	12
1- Seguridad Lógica	14
2- Seguridad de las Comunicaciones	19
3- Seguridad de las Aplicaciones.....	31
4- Seguridad Física.....	35
5- Administración del CPD	40
6- Auditorías y Revisiones	46
7- Plan de Contingencias	51
<i>Informe de Debilidades y Recomendaciones</i>	55
1- Seguridad Lógica	56
2- Seguridad de las Comunicaciones	66
3- Seguridad de las Aplicaciones.....	71
4- Seguridad Física.....	75
5- Administración del CPD	78
6- Auditorías y Revisiones	86
7- Plan de Contingencias	93
<i>Conclusión</i>	97
PLAN DE SEGURIDAD INFORMÁTICA.....	98
PLAN DE SEGURIDAD INFORMÁTICA	99
<i>Objetivo General</i>	99
<i>Antecedentes</i>	99
<i>Alcance</i>	99
<i>Vigencia</i>	99
<i>Autoridad de Emisión</i>	99
<i>Contenido</i>	99
<i>Desarrollo</i>	100
1- Seguridad Lógica	101
2- Seguridad de Comunicaciones	105
3- Seguridad de las Aplicaciones.....	110
4- Seguridad Física.....	115
5- Administración del CPD	119
6- Auditorías y Revisiones	123
7- Plan de Contingencias	127
CONCLUSIÓN	130
ANEXO I – ANÁLISIS DE RIESGOS	131
1- INTRODUCCIÓN	132
2- ACTIVOS Y FACTORES DE RIESGOS	133
3- POSIBLES CONSECUENCIAS Y MEDIDAS EXISTENTES	136
4- CÁLCULO DE NIVELES DE VULNERABILIDAD	148
5- CONCLUSIONES	156
5.1 Niveles de Vulnerabilidad.....	156
5.2 Análisis de Importancias.....	157

5.3	<i>Valores Máximos, Mínimos y Reales</i>	<i>158</i>
5.4	<i>Porcentajes de Riesgos Cubiertos.....</i>	<i>159</i>
ANEXO II – CUESTIONARIOS		160
1-	RELEVAMIENTO INICIAL.....	161
2-	SEGURIDAD LÓGICA.....	163
3-	SEGURIDAD EN LAS COMUNICACIONES	171
4-	SEGURIDAD DE LAS APLICACIONES	181
5-	SEGURIDAD FÍSICA.....	186
6-	ADMINISTRACIÓN DEL CENTRO DE CÓMPUTOS	191
7-	AUDITORÍAS Y REVISIONES	194
8-	PLAN DE CONTINGENCIAS	201
GLOSARIO		206
BIBLIOGRAFÍA		214

Durante los últimos años de nuestra carrera nos planteamos el interrogante sobre la temática a desarrollar en el trabajo final, y nos propusimos varios objetivos que queríamos cumplir.

Teníamos la intención de aprender nuevos conceptos que no hayamos desarrollado durante el transcurso de la carrera, y queríamos realizar un trabajo de investigación para ejercitar el autoaprendizaje adquirido en el ambiente universitario.

El tema a desarrollar debía ser de actualidad, innovador; y poder aplicarse a la realidad, poder ser llevado a la práctica con los conocimientos adquiridos y afrontar así nuestro desenvolvimiento en esta materia. Por último, debía ayudarnos a construir nuestro perfil como futuros profesionales.

Todas estas razones nos encaminaron hacia la Seguridad Informática, lo que nos permitió plasmar nuestra investigación en un enfoque enteramente práctico.

Como actividad inicial desarrollamos una auditoría de seguridad, con el fin de relevar la consistencia de los sistemas de información y de control, la eficiencia y efectividad de los programas y operaciones, y el cumplimiento de los reglamentos y normas prescriptas. Todo esto con el fin de definir las políticas que conformen un plan de seguridad informática.

El paso siguiente para establecer estándares de protección de los recursos informáticos de la empresa sería la creación de los manuales de procedimientos, tarea que se verá facilitada con el respaldo de la auditoría y las políticas de seguridad realizadas en el presente trabajo.

Actualmente la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que desemboca en la aparición de nuevas amenazas en los sistemas informáticos.

Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan. De esta manera las políticas de seguridad informática surgen como una herramienta para concienciar a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de cada organización. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el por qué de ello, es decir que pueden tomarse como una forma de comunicación entre los usuarios y los gerentes.

De acuerdo con lo anterior, el implementar políticas de seguridad requiere un alto compromiso con la organización, agudeza, destreza y experiencia técnica para detectar fallas y debilidades, y constancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas.

Para la generación de las políticas mencionadas, resulta conveniente la ejecución de una auditoría de seguridad informática. Esta es una disciplina que, a través de personas independientes de la operación auditada y mediante el empleo de técnicas y procedimientos adecuados, evalúa el cumplimiento de los objetivos institucionales con respecto a la seguridad de la información y emite recomendaciones que contribuyen a mejorar su nivel de cumplimiento.

AUDITORÍA DE SEGURIDAD INFORMÁTICA

LA EMPRESA S.A.**AUDITORÍA DE SEGURIDAD INFORMÁTICA****OBJETIVO GENERAL**

El objetivo general consiste en la realización de una **Auditoría Informática** en **La Empresa S.A.** con el fin de relevar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una **Política de Seguridad**, donde se definirán los lineamientos para promover la implementación de un modelo de seguridad en toda la organización.

ALCANCE

La **Auditoría Informática** propuesta comprende fundamentalmente la planificación y ejecución de los siguientes aspectos:

1. EVALUACIÓN DE LA SEGURIDAD LÓGICA
 - 1.1. Identificación de usuarios
 - 1.2. Autenticación de usuarios
 - 1.3. Passwords
 - 1.4. Segregación de funciones
2. EVALUACIÓN DE LA SEGURIDAD EN LAS COMUNICACIONES
 - 2.1. Topología de red
 - 2.2. Comunicaciones externas
 - 2.3. Configuración lógica de red
 - 2.4. Mail
 - 2.5. Antivirus
 - 2.6. Firewall
 - 2.7. Ataques de red
3. EVALUACIÓN DE LA SEGURIDAD DE LAS APLICACIONES
 - 3.1. Software
 - 3.2. Seguridad de bases de datos
 - 3.3. Control de aplicaciones en PC's
 - 3.4. Control de datos en las aplicaciones
 - 3.5. Ciclo de vida del desarrollo del software
4. EVALUACIÓN DE LA SEGURIDAD FÍSICA
 - 4.1. Equipamiento
 - 4.2. Control de acceso físico al centro de cómputos
 - 4.3. Control de acceso a equipos
 - 4.4. Dispositivos de soporte
 - 4.5. Estructura del edificio
 - 4.6. Cableado estructurado

5. EVALUACIÓN DE LA ADMINISTRACIÓN DEL CPD

- 5.1. Administración del CPD
- 5.2. Capacitación de usuarios
- 5.3. Backup
- 5.4. Documentación

6. EVALUACIÓN DE LAS AUDITORÍAS Y REVISIONES

- 6.1. Chequeos del sistema
- 6.2. Responsabilidad de los encargados de seguridad
- 6.3. Auditorías de control de acceso
- 6.4. Auditorías de redes

7. EVALUACIÓN DEL PLAN DE CONTINGENCIAS

- 7.1. Plan de administración de incidentes
- 7.2. Backup de equipamiento
- 7.3. Estrategias de recuperación de desastres

METODOLOGÍA APLICADA

La metodología utilizada para la realización de la presente Auditoría Informática se basa en el desarrollo de las siguientes actividades:

- a. Definición de los objetivos de la auditoría y delimitación del alcance.
- b. Análisis de fuentes de datos y recopilación de información.
- c. Generación del plan de trabajo, asignación de recursos y establecimiento de plazos de tiempo.
- d. Generación de cuestionarios y adaptaciones realizadas a los mismos en base a los perfiles de los entrevistados.
- e. Proceso de Relevamiento:
 - e.i Entrevistas a:
 - ~ Miembros del Directorio: Gerente General y Gerente Contable.
 - ~ Responsable del Departamento de Sistemas: administrador.
 - ~ Personal del Centro de Cómputos: programador, administrador de Web, responsables del mantenimiento.
 - ~ Usuarios del sistema: personal del área administrativa y vendedores.
 - ~ Especialistas externos: especialista en LINUX y redes informáticas; Auditor de Sistemas del BCRA, certificado por CISA.
 - e.ii Recolección de documentos organizacionales.
 - e.iii Reconocimiento del entorno y del ámbito de trabajo.
- f. Desarrollo de un análisis de riesgos.
- g. Análisis de los datos relevados, hallazgos de debilidades y generación de recomendaciones.
- h. Discusión de resultados y obtención de la conclusión.
- i. Planteamiento de políticas de seguridad.
- j. Presentación del informe definitivo a las autoridades de La Empresa.

NORMATIVAS EMPLEADAS

Para la realización de la presente Auditoría Informática se utilizaron los siguientes estándares y guías:

1. ESTÁNDARES:

1- **BCRA** (Banco Central de la República Argentina)

- a) Anexo a la Comunicación “A” 2659, fechado el 23/01/1998 “Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática” del Banco Central de la República Argentina (BCRA).
- b) Anexo a la Comunicación “C” 30275, fechado el 12/03/2001 “Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática. Fe de erratas” del Banco Central de la República Argentina (BCRA).
- c) Anexo a la Comunicación “A” 3198, fechado el 30/03/2001 “Texto ordenado actualizado de las Normas sobre Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática” del Banco Central de la República Argentina (BCRA).

2- **COBIT** (Control Objectives for Information Technology)

- a) “Audit Guidelines” 3ra. Edición. COBIT, fechado en Julio de 2000.
- b) “Control Objectives” 3ra. Edición. COBIT, fechado en Julio de 2000.

3- **ISO** (International Standard Organization)

- a) “Estándar de Seguridad ISO 17799” (British Standard 7799)

4- **DoD** (Department of Defense of the United States) **Rainbow Series Library**

- a) “Trusted Network Interpretation of the TCSEC” (TNI), 31 July 1987. (Red Book), National Computer Security Center (NCSC).
- b) “Password Management Guideline”, 1985. (Green Book)

5- **SIGEN** (Sindicatura General de la Nación)

- a) “Normas generales de control interno”, Resolución SIGEN N° 107/98. SIGEN, Agosto de 1998.
- b) “Normas de auditoria externa de la Auditoria General de la Nación” Auditoría General de la Nación, Octubre de 1993

2. GUÍAS DE REFERENCIA Y SOPORTE:

1- **ISACA** (Information Systems Audit and Control Association)

- a) “Planning the IS Audit” ISACA, 1998.
- b) “Normas generales para la auditoría de los sistemas de información” ISACA, 1997.

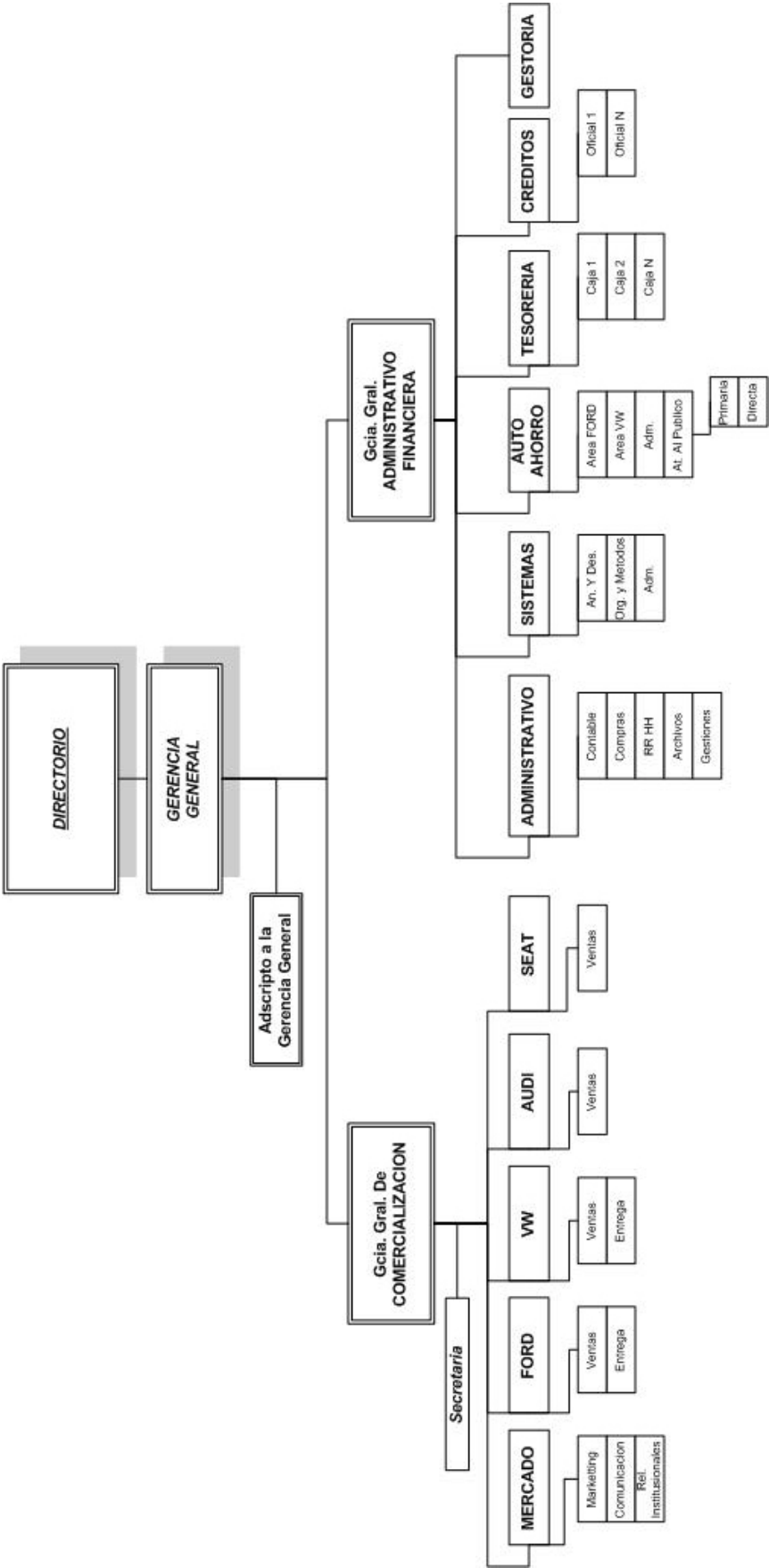
- 2- **NIST** (National Institute of Standards and Technology - U.S. Department of Commerce)
 - a) “Generally Accepted Principles and Practices for Securing Information Technology Systems”. Marianne Swanson y Barbara Guttman, 1996.
 - c) “Guide for Developing Security Plans for Information Technology Systems” Marianne Swanson, 1998.
 - d) “Security Self-Assessment Guide for Information Technology Systems” Marianne Swanson, 2001.
 - e) “Automated Tools for Testing Computer System Vulnerability” W. Timothy Polk, 1992.
 - f) “The Common Criteria for Information Technology Security Evaluation” v2.1 (ISO IS 15408)
- 3- **Cisco Systems**
 - a) “Cisco SAFE: A Security Blueprint for Enterprise Networks”. Sean Convery y Bernie Trudel, Cisco Systems. 2000.
 - b) “Beginner's guide to network security” Cisco Systems. 2001
- 4- **“Tutorial de seguridad”** CERT (Computer Emergency Response Team).
- 5- **“IT Baseline Protection Manual - Standard security safeguards”**. Bundesanzeiger – Verlag, Alemania. 2001.
- 6- **“Handbook of Information Security Management”** Hal Tipton and Micki Krause, Consulting Editors, 1998.
- 7- **“Internet Security Professional Reference, Second Edition”** Autores multiples, New Riders Publishing, 1997.

INFORME DE RELEVAMIENTO

La organización auditada, **La Empresa S.A.**, es una concesionaria automotriz, con aproximadamente 209 empleados, distribuidos en una casa central y tres sucursales. Cuenta con varios puestos de venta, asociados a las distintas fábricas de vehículos que representa. La estructura jerárquica de la organización se muestra en el organigrama presente.

A continuación se describen los datos y la información recogida durante el relevamiento realizado a La Empresa S.A., detallando cada uno de los controles que se implementan en la actualidad.

ORGANIGRAMA LA EMPRESA S.A.



1- SEGURIDAD LÓGICA

OBJETIVO DE AUDITORÍA: los auditores deberán evaluar los controles de accesos de los usuarios a las plataformas de procesamiento informático y a los datos que éstas gestionan, con el fin de señalar las irregularidades que obstaculicen la confidencialidad, exactitud y disponibilidad de la información, y las mejoras que fueran factibles de efectuarse.

1.1 IDENTIFICACIÓN DE USUARIOS

1.1.1 ALTAS

Cuando un usuario nuevo ingresa a la empresa, el área de Recursos Humanos toma sus datos, dando de **alta su legajo** sin embargo, no existe un procedimiento formal a seguir para realizar estas tareas. Si este usuario necesita del sistema informático, Recursos Humanos hace el pedido al Departamento de Sistemas, donde se genera el alta del usuario al sistema. Los **datos** que se ingresan en la cuenta son los siguientes:

- ID de usuario, inicialmente será el número de legajo, aunque pudimos comprobar que no se corresponde realmente con éste número.
- Password, inicialmente será el número de legajo, y se instruye al usuario para que lo modifique.
- Nombre y apellido completo, se obtiene del archivo de Recursos Humanos.
- Sucursal de la Empresa donde trabajará.
- Grupo al que pertenece, según el área de la empresa que le fue asignada por el Departamento de Recursos Humanos. Pudimos comprobar que en algunos casos este campo permanece vacío permitiendo que el usuario acceda a todos los menús del sistema.
- Fecha de expiración del password de un año. Aunque para algunos usuarios este campo no se completa, permitiendo que nunca se actualice la contraseña.
- Fecha de anulación de la cuenta para dar de baja la cuenta..
- Contador de intentos fallidos, se bloquea el login si el contador es igual a dos (si el usuario ha ingresado mal la contraseña dos veces seguidas), en este caso el usuario debe solicitar al administrador la reactivación de la cuenta.
- Autorización de imprimir ya que no todos los usuarios pueden imprimir los datos del sistema.
- Autorización de ingreso al área de usados ya que no todos los usuarios tienen acceso a los datos de este sector.

1.1.2 BAJAS

Las **cuentas de los usuarios no se eliminan** del sistema, se deshabilitan actualizándoles la fecha de anulación de dicha cuenta. De esta forma los datos de las cuentas dadas de baja quedan almacenados en el disco y no es posible repetir los ID's de usuarios anteriores para nuevos empleados.

No hay ningún **procedimiento** formal para dar de baja un usuario del sistema. El departamento de Recursos Humanos informa al sector de Cómputos, y allí se procede a dar de baja el empleado una vez que se ha desvinculado de la empresa.

1.1.3 MANTENIMIENTO

No se lleva a cabo ninguna **revisión periódica ni control** sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.

1.1.4 PERMISOS

El control de acceso en la empresa no se basa en los **perfiles de los usuarios** y la asignación o denegación de permisos a los mismos, sino más bien en perfiles de grupos. Estos grupos se generan en concordancia con las áreas de la empresa y es el Departamento de Recursos Humanos el que asigna cada usuario a un grupo determinado. Luego, los usuarios son dados de alta en el sistema, y los administradores del sistema son los encargados de la asignación de permisos.

El sistema informático está desglosado en una gran cantidad **módulos** diferentes, donde cada uno de ellos es un programa en sí mismo. De esta manera cada usuario del sistema, según el grupo al que pertenece en la organización, dispone de los **accesos directos** a los programas que corresponden a su área. Así, los usuarios solo pueden interactuar con los datos a los que dichos módulos les permiten acceder. Los accesos directos a los que el usuario tiene acceso los genera el administrador del sistema a mano, una vez que el usuario fue dado de alta.

A medida que la responsabilidad del usuario en la empresa es mayor, son necesarios más datos, y por ende más módulos, o accesos a programas. Esto quiere decir que en un cargo gerencial puede haber 15 módulos disponibles, mientras que, a modo de ejemplo, los vendedores solo tienen un módulo de consulta de datos. Comprobamos que en ciertos casos sobran funcionalidades. A modo de ejemplo, toda el área de Gestoría tiene disponible un mismo menú, aunque haya funciones que ciertos empleados no necesiten, y al tratar de acceder a datos críticos el sistema requerirá nuevamente el número de legajo y el password. Este control sirve para comprobar que el usuario logeado es el mismo que está intentando acceder a estos datos sensibles, de manera que si este segundo login no coincide con el primero, los datos no serán mostrados.

No existe en el sistema informático una **lista de control de acceso** que se utilice para identificar los tipos de permiso que tiene cada usuario con respecto a los datos. Solo existe una relación entre los sectores de la empresa, los menús y los usuarios correspondientes a cada sector, y en las carpetas de documentación del desarrollo relativas a cada módulo de programa se explica la relación que existe entre cada módulo de programa y los datos. Al no existir esta lista de control de acceso, resulta complicado identificar qué datos puede modificar cada usuario.

No se tiene en cuenta ninguna **restricción horaria** para el uso de los recursos. Tampoco se considera una **restricción física sobre la máquina** desde donde se logea cada usuario.

1.1.5 INACTIVIDAD

Si el usuario permanece un período de tiempo logeado **sin actividad**, el sistema no ejecuta ninguna acción; los administradores solo advierten a los usuarios sobre la necesidad de no dejar las máquinas logeadas e inactivas.

Si las cuentas de usuarios permanecen varios días sin actividad, por licencias o por vacaciones no pasan a un **estado de suspensión**.

El **usuario root** se logea en los servidores durante las 24 horas del día, debido a que éstos equipos no se apagan en ningún momento.

1.1.6 CUENTAS DE USUARIO

Los usuarios del departamento de ventas **no son identificados en forma personal**, sino que usan todos el mismo nombre y contraseña para ingresar al sistema informático. Este módulo del sistema solo permite hacer consultas a las bases de datos, (listas de precios, planes de ventas, etc.) generalmente desde el salón de ventas, pero no les está permitido hacer ninguna modificación a los datos.

Los usuarios del sistema pueden tener abiertos, al mismo tiempo, todos los menús a los que están autorizados, y varias sesiones del mismo menú. No se hacen restricciones en cuanto a la **cantidad de sesiones** que los usuarios pueden utilizar simultáneamente.

No se eliminan los usuarios que vienen por default en el sistema operativo, como son las **cuentas “Guest”**, éstas cuentas permanecen activas en el sistema sin que ningún usuario las utilice.

En la empresa hay tres personas con **perfil de administrador**. Cada una de ellas tiene su cuenta con un password personal, pero a fines prácticos, los tres conocen todas los password de las demás cuentas, ya que no hay una clara definición de tareas. Además, el administrador puede **logearse desde cualquier terminal** de la empresa lo que resulta riesgoso ya que podría, por error, abandonar ese puesto de trabajo dejando esa terminal logeada con su usuario administrador.

Existe, además, un servicio de **mantenimiento externo** que utiliza la misma cuenta del administrador para hacer modificaciones en los sistemas operativos de los servidores vía Internet, ya que el administrador del centro de cómputos le suministró el password. Una vez finalizado el mantenimiento, el administrador del sistema no cambia la contraseña, de manera que ésta continúa siendo conocida por personal externo.

1.2 AUTENTICACIÓN

En la **pantalla de login** de los sistemas se muestran los siguientes datos:

- Nombre de usuario (a completar por el usuario),
- Password (a completar por el usuario),
- Opción para cambiar el password.

Cuando un usuario ingresa su password al sistema, aparecen **asteriscos** en lugar de mostrar el dato que está siendo ingresado. Una vez que algún usuario ha logrado logearse en el sistema, **aparece en pantalla el nombre del usuario** logeado.

Existe una aplicación de importante y significativa sensibilidad con la cual es posible **gestionar los datos de los usuarios**, incluidos sus permisos y contraseñas. Esta aplicación solo puede ser ejecutada si el usuario logeado es el administrador, a través de la línea de comandos de Windows, tipeando todo el camino hasta ella, ya que no hay íconos de acceso directo desde ninguna terminal.

Los **datos de autenticación** de los usuarios del sistema de la empresa se almacenan en el servidor de aplicaciones Linux, en un archivo de texto plano, sin ningún control de acceso (sin encriptación o password de acceso). Este archivo es administrado por el AcuServer, ya que forma parte del sistema de archivos indexados de la empresa. Además, estos datos son transferidos, desde la terminal que se está logeando hasta el servidor, en formato de texto plano.

Dentro de la empresa no se usa ningún tipo de **firma digital**, ni para mensajes internos ni para los externos ya que las directivas de importancia no son enviadas vía mail.

En cuanto a la configuración de las estaciones de trabajo, no hay ningún control de acceso a sus **sistemas BIOS**, de manera que al momento del encendido de la máquina cualquier persona podría modificar sus opciones de configuración.

1.3 PASSWORDS

1.3.1 GENERACIÓN

Los **passwords** que existen en la empresa son generados en forma manual, sin procedimientos automáticos de generación. Como restricción, deben tener una longitud máxima de 10 caracteres, numéricos o alfanuméricos.

Cuando se da de alta un empleado en el sistema, su **password se inicializa** con el mismo nombre de la cuenta (que es igual al número de legajo del usuario), advirtiéndole al usuario que lo cambie, pero sin realizar ningún control sobre la modificación del mismo.

Durante la auditoría pudimos comprobar que los password de acceso a los usuarios root de ambos servidores Linux eran iguales.

1.3.2 CAMBIOS

Los cambios en los **passwords** los hacen los usuarios a través de la pantalla del login, allí hay un botón que muestra la opción para su modificación. Aunque generalmente los passwords **no son actualizados** por los usuarios, permaneciendo iguales por largos períodos de tiempo, ya que tienen un plazo de expiración de 1 año.

No se controla si el usuario utiliza siempre el **mismo password**, simulando cambiarlo pero ingresando nuevamente la clave que ha estado usando hasta ahora.

Si un usuario **olvida** su password, debe advertirle al administrador del sistema, el cual se fijará (con el sistema de administración de perfiles de usuario) cuál es la clave del usuario. Al decírsela, no se requiere que el usuario la modifique, no se controla esta situación. Ocurre lo mismo cuando un usuario ingresa mal su contraseña dos veces seguidas: el sistema lo **bloqueará** y el usuario no podrá ingresar, por lo que deberá recurrir al administrador.

1.4 SEGREGACIÓN DE FUNCIONES

No se implementa ningún régimen de **separación de tareas**, para evitar que un solo empleado realice la totalidad de una operación.

Tampoco se lleva a cabo ninguna **rotación de personal**, solo se han modificado las tareas de algunos de los vendedores, debido al poco trabajo que tienen en su sector; o se realizan suplencias cuando algún empleado toma vacaciones.

2- SEGURIDAD DE LAS COMUNICACIONES

OBJETIVO DE AUDITORÍA: durante la Auditoría Informática se deberá evaluar la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente e ininterrumpida de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro, comprobando el cumplimiento de las normas de seguridad de la información.

2.1 TOPOLOGÍA DE RED

2.1.1 COMPONENTES DE RED

La red informática de la empresa se compone del siguiente equipamiento:

- 100 PC's distribuidas entre las 4 sucursales, con aproximadamente 60 de ellas en la casa central,
- 2 Servidores Hewlett Packard, uno para aplicaciones y otro para Internet,
- 4 antenas de transmisión radial,
- 3 enlaces de fibra óptica,
- cables UTP categoría 5,
- conexión ADSL de 512 KBPS, como salida a Internet,
- 3 módem de 56 KBPS para conexión con las fábricas,
- un switch CISCO 4000 en la casa central. Características:
 - 6 salidas de fibra óptica, con tres de ellas utilizadas y tres libres,
 - 2 canales de radio, con uno solo utilizado, conectado a un equipo de radio CISCO, y desde allí a la antena, comunicándose así con el resto de las sucursales,
 - soporte para telefonía sobre IP (próximamente las comunicaciones telefónicas internas de la casa central se desarrollarán con este método, usando la línea telefónica solo para las comunicaciones al exterior),
- patchera conectada al switch central con 64 entradas para PC's,
- 6 switches CISCO 1900 de 12 entradas, uno en cada una de las sucursales,
- 6 patcheras, conectadas a cada switch,
- 2 hubs de 100 MB.

2.1.2 DESCRIPCIÓN DE LA RED

- **Enlaces radiales entre sucursales:** existe una conexión a través de enlaces radiales que conectan la casa central con el resto de las sucursales, implementado con una topología de tipo BUS, ya que todos los puntos de conexión no pueden verse entre sí de manera de formar alguna otra topología más eficiente. Los datos viajan encriptados mediante un sistema de encriptación propio de las antenas CISCO.
- **Fibra óptica entre secciones:** las conexiones entre las distintas secciones de la casa central (Usados; Ford, Audi y LandRover; Vw, Seat y Chevrolet)

se realizan a través de 3 canales de fibra óptica. Se implementó de esta forma debido a la corta distancia entre los puntos y a la alta velocidad requerida en el cable.

- **UTP en conexiones internas:** la totalidad del tendido de cables en el interior de la empresa se realizó con UTP categoría 5.
- **Switches:** los switches han sido programados para realizar un tipo de ruteo: direccionan los paquetes transmitidos por sector, según la dirección IP que traen, distinguiendo a que sector de la empresa van. De esta manera, al no repetir los paquetes de datos a toda la red, se disminuye el uso de ancho de banda y se evita la divulgación de los mensajes, mejorando la seguridad de la topología de Bus.
- **Puestos de venta off-line:** los puestos de venta que la empresa mantiene en shoppings, por ejemplo, no tienen conexión con el servidor. Las transacciones que se realicen allí, ya sean ventas o planes de ahorro, se efectúan en papel y luego son cargadas a la base de datos del servidor en la casa central.

2.2 CONEXIONES EXTERNAS

2.2.1 FÁBRICA

La comunicación con las fábricas (tanto de Ford como de VW) está restringida a una **conexión vía módem**, con aplicaciones propias de ambas fabricas. Éstas proveen a la empresa de una clave y contraseña de usuario y un proveedor de Internet. La empresa se conecta directamente a la fábrica a través de la aplicación suministrada, y baja de allí una actualización diaria de archivos necesaria para la gestión. De la misma manera los archivos son transferidos hacia las fábricas.

Los usuarios de la **sección de repuestos** tiene una conexión on line con los administradores del depósito de Ford de Buenos Aires, para consultas sobre el stock de los productos. La fábrica de VW no tiene sistema de consulta on line, sino que hace actualizaciones diarias de estos datos vía módem. Estas máquinas no tienen ningún control especial con respecto a la conexión a Internet. Tienen instalado Internet Explorer con la posibilidad de navegar y los datos que se transmiten por estos módem no pasan por el firewall, sino que directamente se comunican al exterior.

Los datos que van a VW o Ford se generan en el **formato propio** de la aplicación, luego se zipean, y se transmiten. Para bajar datos se realiza el mismo procedimiento pero en sentido inverso.

2.2.2 SERVIDOR DE INTERNET

Para la **conexión a Internet** se utiliza un servidor Proxy de Linux llamado Squid, ubicado en el servidor de Internet. Su salida al exterior es a través de una conexión ASDL de 512 KBPS, suministrada por un ISP. Este Proxy se configuró de manera estricta, de forma que solo tiene conexión al exterior un rango de direcciones IP definido por la Gerencia.

En el servidor Proxy se seleccionaron las direcciones IP de las máquinas que pueden salir al exterior, de esta manera se controla el acceso a Internet. Este Proxy es el que

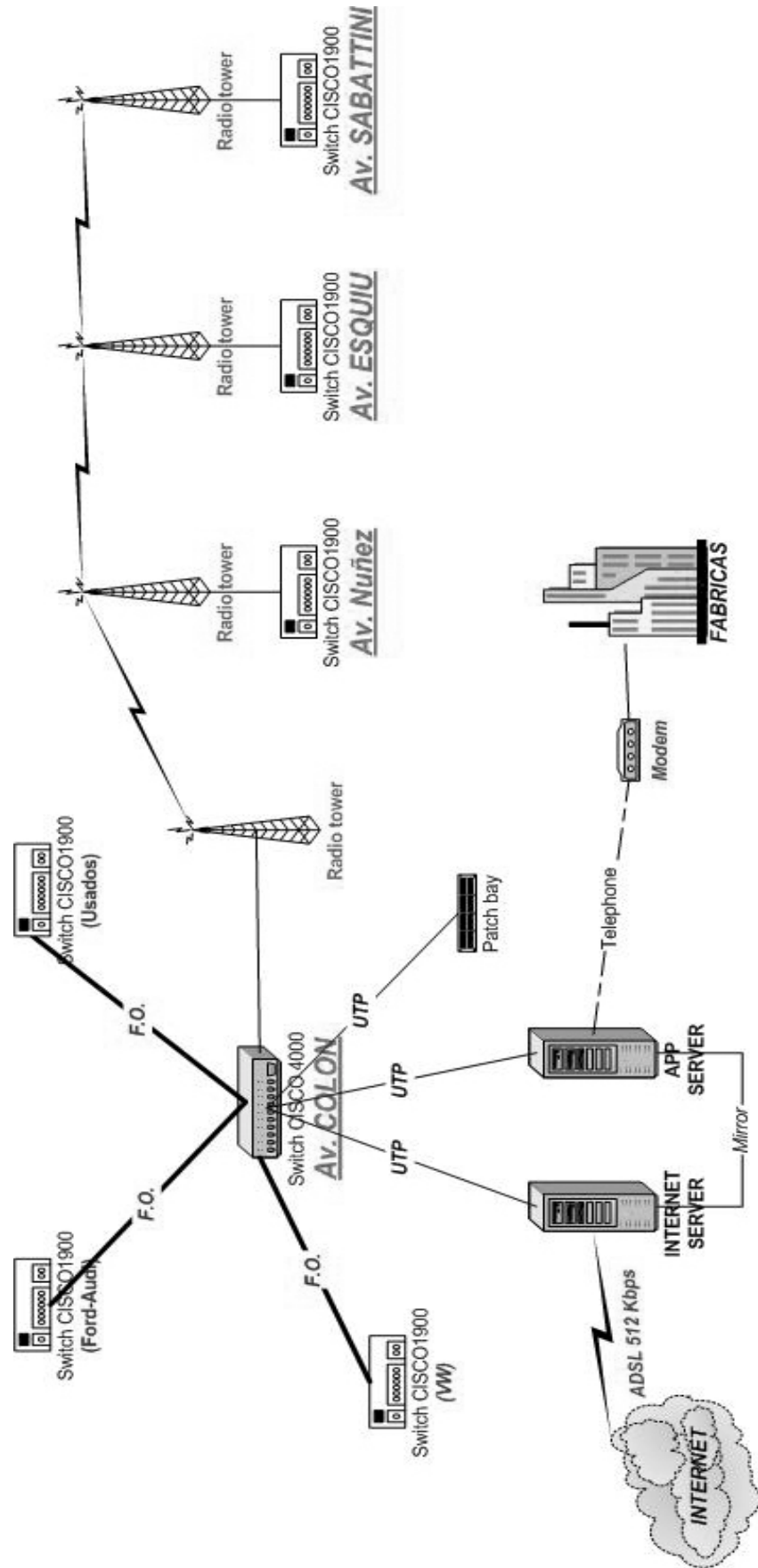
proporciona de acceso a Internet al resto de las sucursales a través de los enlaces radiales.

Como **conexión de respaldo** a Internet se puede utilizar una conexión vía módem. Actualmente el módem no se encuentra instalado en el servidor, para su protección física, pero puede ser instalado y configurado rápidamente ante cualquier contingencia con la conexión de ADSL.

2.2.3 SERVIDOR DE HOSTING

El servidor de hosting se eligió según el precio y los servicios ofrecidos. No se ofrece ninguna medida de seguridad ni política de respaldo en caso de problemas, pero no se han registrado problemas hasta el momento.

GRÁFICO
 TOPOLÓGICO DE
 RED



2.3 CONFIGURACIÓN LÓGICA DE RED

2.3.1 INTEROPERATIVIDAD WINDOWS - LINUX

Los recursos de Linux se comparten en la red de Windows usando una aplicación llamada **Samba**. Con esta aplicación, una porción del disco del servidor de aplicaciones se encuentra compartida con la red de Windows. Esto hace posible el entendimiento entre Windows y Linux, permitiendo a los usuarios de Windows acceder a datos que se encuentren en el sector compartido del servidor Linux, a través del Explorador de Windows.

El Samba tiene la capacidad de realizar autenticación, administrar perfiles, y demás opciones de seguridad de los recursos compartidos, donde se le establece un nivel de seguridad determinado a cada uno de los recursos de la red.

No todas las utilidades son usadas en la empresa, solo se utiliza el Samba como herramienta de comunicación entre los distintos sistemas operativos.

2.3.2 RECURSOS COMPARTIDOS

El entorno de red de cada uno de los usuarios está configurado para que le usuario no vea toda la red, sino solo una parte de la misma. Pero no hay ninguna medida tomada para que un usuario no comparta sus datos con otro usuario.

En la empresa, la configuración de esta aplicación no permite que haya visibilidad a las carpetas compartidas de los servidores, debido a que están en el área compartida del disco con la aplicación Samba, pero no disponibles para los usuarios en el Explorador de Windows.

Ninguno de los equipos comparte sus archivos, a excepción de los siguientes:

- En el **servidor de Internet** se comparten dos carpetas. Una es la utilizada para almacenar las actualizaciones del antivirus y los instaladores más utilizados, y la otra es la que emplea la aplicación que sincroniza la fecha y hora de las PC's de la red.
- En el **servidor de aplicaciones** se comparte una carpeta donde los usuarios de Marketing guardan los datos que necesiten grabar en un CD, ya que la grabadora se encuentra en éste servidor.

En el área compartida del disco con la aplicación Samba se encuentran los datos de la empresa (archivos indexados), las aplicaciones del sistema informático de la empresa (ejecutables) y los sistemas en desarrollo. Los usuarios, desde Windows, acceden a los ejecutables de las aplicaciones a través de una aplicación de Cobol, llamada RunTime. Esta aplicación accede a un archivo de configuración del servidor donde se almacena un parámetro, similar al Path de DOS, que direcciona al ejecutable, el cual tiene la propiedad de lectura, solamente. A través de éste camino, los usuarios pueden tener acceso a los programas en el servidor, de otro modo no sería posible, ya que el Explorador de archivos de Windows no tiene visibilidad sobre las carpetas del servidor.

2.4 MAIL

No todos los empleados tienen una cuenta de mail, solo hay 47 cuentas de correo ya que hay muchos empleados que no necesitan este servicio, Todos los Jefes de Área disponen de una, por este motivo esta vía de comunicación llega a todo el personal de la empresa. Este medio se utiliza para enviar todo tipo de información.

2.4.1 HERRAMIENTAS

La empresa cuenta con un sistema de **mail externo y uno interno**. El interno está alojado en el servidor de Internet de la empresa, y permite la comunicación entre el personal de los distintos departamentos. Mientras que el externo se aloja en un servidor ajeno. Ambos sistemas de mail poseen diferentes dominios. El mail interno tiene como dominio @mail.com mientras que el externo tiene el dominio @la-empresa.com.

El correo se lee con Outlook Express en las PC's de la empresa. En el servidor se usa el **SendMail**, un administrador de correo de Linux, configurado por los técnicos encargados del mantenimiento, y gestionado por el administrador del centro de cómputos. Algunas máquinas tienen instalado un software llamado IncrediMail, que proporciona utilidades varias, como avisos animados de nuevos mail. Para los empleados que no tienen instalado este software, existe un programa que chequea la cuenta pop de cada usuario y avisa al usuario si ha arribado un nuevo mail, cada cinco minutos.

El **Outlook Express** se instala con su configuración por default y puede ser modificado por el usuario, el que puede modificar las siguientes características:

- vista previa,
- confirmación de lectura,
- block sender,
- controles ActiveX y Scripts.

2.4.2 ALTA DE USUARIOS DE MAIL

Si un empleado necesita una dirección de mail, porque su puesto de trabajo lo amerita, el Gerente del área al que pertenece le avisa al administrador del centro de cómputos, y éste le asigna una casilla de correo.

Los usuarios que existen en Linux son el root, otro usuario que crea Linux por defecto en la instalación, y todos los usuarios que tienen cuentas de mail, debido a que para tener una cuenta de mail hay que estar definido como usuario en el sistema.

Cuando se genera una nueva cuenta de mail, el administrador del sistema debe definir al usuario:

- en el servidor de hosting del ISP,
- luego debe darlo de alta en el sistema operativo del servidor de Internet interno de la empresa (con el mismo nombre de usuario y la misma contraseña que la usada en el ISP),
- después debe configurar el SendMail,
- y por último el Outlook Express de la máquina del empleado.

En el momento de generar la nueva cuenta, el administrador le asigna un nombre y un password a la nueva cuenta -de manera que los usuarios no tienen conocimiento de sus passwords, ya que el administrador los configura en el Outlook Express y allí se almacenan. Esto impide que un empleado utilice la cuenta de otro, ya que la única persona que conoce las contraseñas es el administrador del centro de cómputos.

Las **cuentas externas** de los usuarios no están publicadas en Internet. Lo que se publica en la página son cuentas generales con alias, que apuntan a las cuentas de los Jefes de Áreas, por ejemplo existe una cuenta de ventas (ventas@la-empresa.com) que está dirigida a la cuenta del Gerente de Ventas.

2.4.3 RECEPCIÓN Y ENVÍO DE MAILS

Cada diez minutos el SendMail **chequea las casillas** de correos del servidor de hosting. En el caso que exista algún mensaje nuevo, éste los baja al servidor de Internet. Los Outlook Express de las máquinas de los usuarios chequean el servidor de Internet cada cinco minutos. Cuando actualizan sus bandejas de entrada, el mail es borrado del servidor y enviado a la máquina del usuario, sin quedar ninguna copia del mismo en el servidor.

En el caso del envío de mails, este no hace el mismo recorrido. La diferencia radica en que el mail interno no va hasta servidor de Internet del ISP, sino que el SendMail identifica al destinatario y, si es un destinatario interno, le modifica el dominio de la casilla (cambia @la-empresa.com por @mail.com) y lo envía a la casilla interna. En caso de ser un destinatario externo lo envía directamente al ISP.

Los empleados no usan el mail solamente para **funciones laborales**, sino también con fines personales. Es posible ver los mail que se envían, pero actualmente no se realizan controles, de manera que pueden usarlo para cualquier fin. No se hace ningún control para comprobar si los usuarios se suscriben a listas de correo, no hay prohibiciones en este sentido.

2.4.4 CUOTAS DE DISCO

En el momento en que se crea un usuario de mail en el **SendMail**, se le asigna una cuota de disco del servidor de Internet para los mensajes de entrada, con un tamaño de 4MB para cada usuario. No existe límite de tamaño para los mensajes de salida ya que no quedan almacenados en el servidor.

Si alguna de las casillas llega a los 4MB, entonces el SendMail manda un mail al usuario avisando que se está quedando sin espacio de disco, deja de recibir el correo y se bloquea la casilla.

Existe una cuenta de mail que le asignó **FORD** a uno de los Gerentes, con un tamaño de 2MB y que, debido a que recibe una gran cantidad de mails diarios, por lo general se satura ya que los mensajes son bajados a la PC directamente por el usuario desde el Outlook Express, sin mediar el SendMail.

2.4.5 OPCIONES SEGURAS DE CONFIGURACIÓN

- **Copia Oculta (CCO)**

Los empleados de Gerencia usan el campo de copia oculta, generalmente para comunicarse con las fábricas, y cuando se envían mensajes a diferentes áreas, se les adjunta una copia oculta al Jefe del Sector.

- **Junk Mail**

No hay ninguna configuración especial para evitar el correo basura o mail bombing. Pero como las direcciones son locales, manejadas con servidores propios, no han ocurrido problemas en este sentido.

El servidor de mail no puede ser utilizado para enviar correo SPAM, ya que desde el firewall no se permite que un usuario externo envíe mails desde el servidor de la empresa.

- **Antivirus**

El antivirus que está en el servidor de Internet chequea el mail, inspeccionando todos los mensajes entrantes y salientes, y sus archivos adjuntos. En el caso de encontrar un mail infectado, se encarga de borrarlo, y el root envía un mail al destinatario del mensaje avisando que el mismo se eliminó.

- **Chat y File Sharing**

No están prohibidos los programas de chateo (generalmente se usa el MSN). Tampoco están prohibidos los programas de file sharing. Esto se da porque los servicios que utilizan estos programas no están deshabilitados.

- **Prioridades**

No se implementa un sistema de prioridades de los mensajes.

- **Copia de seguridad**

No se generan copias de seguridad de los mensajes, ni en el SendMail ni en el Outlook Express de los usuarios.

- **Privacidad – Firma digital – Encriptación de mails**

No se utilizan firmas digitales ni encriptación en el correo electrónico. Algunos usuarios utilizan firmas de Outlook para enviar sus mensajes. No hay prohibiciones de envíos de archivos confidenciales vía mail.

2.5 ANTIVIRUS

En la empresa no ha habido grandes problemas con virus, a excepción de una gran cantidad de PC's con Windows infectadas con el virus K-Lez, pero este virus no afectó a los servidores Linux. Esta infección generó gran tráfico de red y congestionó las líneas, pero pudieron erradicarse con el uso del antivirus F-Prot para DOS.

2.5.1 HERRAMIENTAS

En la empresa disponen de una versión corporativa del **Norton Antivirus**, de manera que en el servidor de aplicaciones hay una versión para el servidor y en el resto de las PC's hay una versión cliente de este antivirus. En el servidor de Internet está instalado el **PC Cillin** de Trend Micro para el control de virus. Ambos antivirus están ejecutándose continuamente y controlan la recepción y el envío de mail, tanto en el servidor como en las PC's. Hay discos de rescate o de emergencia del antivirus **F-Prot**, con los que se bootea desde DOS, usados para la restauración de máquinas infectadas.

2.5.2 ACTUALIZACIÓN

De Internet se actualizan las **listas de virus** del Norton Antivirus a través de un script, y el archivo ejecutable se almacena en una carpeta del servidor. Los usuarios son los responsables de actualizar sus propios antivirus y para esto tienen en su escritorio un icono apuntando a la última actualización bajada de Internet.

Este script, al ejecutarse y bajar las actualizaciones, envía un mail a los usuarios advirtiéndoles que actualicen el programa. No se hacen chequeos ocasionales para ver si se han actualizado los antivirus.

2.5.3 ESCANEOS DE VIRUS

No se hacen escaneos periódicos buscando virus en los servidores ni en las PC's. No hay ninguna frecuencia para realizar este procedimiento, ni se denominó a ningún responsable. En algunas máquinas (en las que han tenido problemas frecuentes con virus), cuando el equipo se inicia, entonces comienza un escaneo del Norton antes del inicio de Windows.

2.6 FIREWALL

2.6.1 CONFIGURACIÓN DE SERVICIOS DEL FIREWALL

El firewall que existe en la empresa es un servicio del kernel de Linux, configurado de manera que se prohíben todos los servicios y solo se habilitan los necesarios (postura de negación preestablecida).

Se configuró en base a una política que discrimina tres clases de paquetes de red:

- los paquetes entrantes a la red,
- los paquetes salientes de la red,
- los paquetes en tránsito.

Por defecto, lo que no se habilite explícitamente está prohibido. Así se les va a denegar el acceso a todos los paquetes de entrada y a los paquetes en tránsito, mientras que a los de salida se les permite la salida. Algunas de las reglas más importantes son:

- Se aceptan todos los paquetes que van o vienen de la **red interna**, pero se les pone una máscara (con la dirección IP del servidor) para evitar que en el exterior se conozcan las direcciones de red interna. Cuando vuelve la respuesta al paquete se le cambia la dirección nuevamente.
- Todos los datos que van dirigidos a **un puerto 80** (HTTP), se redireccionan al Proxy.
- No hay restricciones a los **puertos de salida**.
- Se aceptan los mensajes **loop back**, para comunicación de la red consigo misma.
- Se aceptan los datos que entran por el puerto que se usa para la **sincronización horaria** en la red (servicios Date y Time).
- Se acepta el puerto 22, del **SSH** (Secure Shell).
- Los datos que están en **tránsito** son aceptados si provienen de la red interna.

- Se acepta el acceso de los **puertos altos** (son los puertos mayores al 1023): desde éstos puertos altos vienen todas las conexiones TCP/IP desde cualquier cliente externo. Es decir, cuando es necesario salir de la red, como un cliente, de un puerto local a un puerto remoto, el Linux asigna un puerto local alto. Así es que se deben permitir que ingresen datos desde los puertos altos, de otra manera no habría ningún paquete entrante.
- Se prohíbe el ingreso desde cualquiera de los **puertos bajos**, a excepción de los explícitamente permitidos (como el puerto 22, usado para mantenimiento).

Los siguientes servicios no se encuentran deshabilitados explícitamente mediante reglas del firewall, pero no será posible acceder a ellos, salvo a través del SSH:

- No se deshabilitan los **shell** y **login**, lo que significa que se puede acceder a los servicios remotos, como el **RSHELL**, **REXEC** y **RLOGUIN**.
- Está habilitado el **TALK** (que permite hacer un chat con otra máquina),
- Está habilitado el **FINGER** (que devuelve datos del usuario que está logeado en esa máquina, como nombre, estado, correo, etc.)
- Está habilitado el **SYSTAT** (que devuelve datos sobre el estado del sistema)
- Están habilitados los **APPLETS** y los **SCRIPTS**.

Algunos servicios no son necesarios y sin embargo se encuentran habilitados en forma permanente, como el FTP, ya que existe un usuario que debe utilizar este servicio para comunicarse con las fábricas al menos una vez por mes.

En el servidor de Internet se encuentran habilitados permanentemente los puertos necesarios para el funcionamiento de la red y algunos servicios están deshabilitados y se activan solo cuando son necesarios, estos son llamados **servicios on demand**.

El SSH utiliza SSL (Secure Socket Layer) o sea una capa de servicios segura, en reemplazo de los servicios tradicionales. El **mantenimiento** de los servidores de la empresa se realiza a través de acceso remoto, usando SSH (Secure Shell), en reemplazo del Telnet por su seguridad ya que en SSH la información viaja cifrada y ante tres intentos fallidos de ingresar una contraseña corta la comunicación, mientras en el Telnet transmite en texto plano y no tiene restricciones de la cantidad de contraseñas que pueden ingresarse, facilitando el ataque de fuerza bruta.

Al disponer de un servicio ADSL, la empresa tiene asignado un número **IP variable** en su servidor de Internet, el cual le proporciona mayor seguridad porque evita, de alguna manera, los intentos de intrusión. Esta no es una complicación para el mantenimiento ya que este número IP es registrado bajo un dominio ficticio en un sitio de Internet. Para tener acceso a este servidor de dominios se requiere una contraseña de acceso creada y administrada por el encargado de servicio técnico. Una vez conseguido este número IP, el servicio técnico accede a las máquinas de la empresa para realizar las modificaciones necesarias.

2.6.2 *TESTEO DE LA RED*

El **encargado de mantenimiento** controla que los servicios permitidos sean los correctos, pero esta tarea la realiza sin ninguna frecuencia. Debido a que estas pruebas que se realizan no son formales, no se genera documentación alguna.

Nunca se hicieron **pruebas de auto-hackeo**, ni escaneos, ni intentos de intrusión o de escucha. Tampoco se hace un testeo periódico de puertos o de los servicios que están habilitados. Solo se revisan las instalaciones cuando hay quejas de los usuarios.

El firewall monitorea los **intentos de ingresos**, generando logs y mails por cada evento, pero no genera alertas ni warnings ante algún supuesto problema.

Además disponen del **WebMin** para monitorizar ciertos parámetros de la red, como el tráfico de red, aunque estos parámetros no son controlados con períodos determinados ni se generan alarmas ante problemas.

2.6.3 FALLA EN SERVIDORES

En el caso que haya algún problema con el servidor de Internet, no se usaría el servidor de aplicaciones como reemplazo. Para la empresa es preferible prescindir de los servicios de Internet hasta que el servidor sea reparado, a arriesgar los datos del servidor de aplicaciones exponiéndolos en Internet.

En el caso que falle el firewall sería una falla segura, ya que los controles funcionan a bajo nivel (a nivel del kernel) y esta falla implicaría que el sistema operativo del servidor está inestable, de manera que nadie tendría acceso desde ni hacia la red externa (Internet).

2.6.4 PARCHES DE SEGURIDAD DEL LINUX

Las **versiones del sistema operativo instaladas** en los servidores son antiguas, por lo que casi no se consiguen actualizaciones. Esto puede repercutir en la seguridad de los servicios usados, como el SSH, generando nuevas vulnerabilidades.

El servidor de Internet tuvo una sola reinstalación del kernel de Linux, mientras que el de aplicaciones necesitó varios parches para intentar solucionar un problema en particular. Estos cambios se documentan cada vez que se realizan.

2.7 ATAQUES DE RED

En la empresa no disponen de **herramientas destinadas** exclusivamente para prevenir los ataques de red, en principio debido a que no se han presentado, hasta el momento, problemas en este sentido.

Tampoco hay **zonas desmilitarizadas** ya que no se justifica por el nivel de costo que esto implicaría, ya que solo se dispone de un servidor y, por sobre todo, debido a que no hay datos publicados on line desde el interior de la empresa.

2.7.1 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS - INTRUSION DETECTION SYSTEM)

En la empresa no se han registrado intrusiones, solo tres intentos de intrusión que fueron impedidos por el firewall, el cual envió mails al usuario root del sistema operativo informando de los mismos.

No hay herramientas para detección de intrusos, solo cuentan con la configuración del firewall.

2.7.2 NEGACIÓN DE SERVICIO (DOS - DENIAL OF SERVICE)

No hay controles con respecto a la ocurrencia de Denial of Service. No existen herramientas que lo detecten, ni hay líneas de base con datos sobre la actividad

normal del sistema para así poder generar avisos y limitar el tráfico de red de acuerdo a los valores medidos.

Disponen de una herramienta de monitoreo, Monitor, que se ejecuta en una página HTML con datos sobre:

- tráfico de red,
- cantidad de archivos abiertos,
- cantidad de usuarios conectados a la red,
- uso de la memoria del servidor,
- uso del swap.

Además el kernel de Linux está capacitado para reconocer ciertos tipos de **Denial of Service** como TCP SYN Flood, Ping of Death, entre otros. De todas maneras el momento en el que Linux reconoce estos ataques es tardío ya que los canales de red ya estarán congestionados, y solo logra evitarse la congestión de los canales internos de la red.

2.7.3 SNIFFING Y SPOOFING

En la empresa la red se encuentra **segmentada** a través de switches, que efectivamente reducen la posibilidad de sniffing, ya que direccionan los paquetes de red de acuerdo al destino que tienen (sector de la empresa al que están dirigidos). Así se evita que el paquete viaje a través de toda la red o por destinos innecesarios.

Además los equipos de **radio** de la empresa encriptan los datos físicamente, por lo que el sniffing en estos tramos de la red resultaría más difícil.

No existe ninguna herramienta anti-spoofing. Como ya dijimos, el acceso externo esta prohibido, debido a ser una máquina que funciona en modo cliente (no es un servidor de páginas Web), no obstante esto el firewall explícitamente deniega cualquier tráfico de la red externa que posea una dirección fuente que debería estar en el interior de la red interna.

2.7.4 ATAQUE A LOS PASSWORDS

El archivo de los passwords del sistema no se almacena en el **directorio** por default del Linux, en el /etc/passwd, aquí solo se almacena un archivo con los nombres y demás datos de usuarios. Este archivo está en texto plano y puede ser accesible ya que no está encriptado.

El archivo que contiene las passwords se encuentra en otro directorio, al cual solo el root tiene permisos para accederlo, éste es un **archivo shadow**, donde están encriptadas. Se usa encriptación *one way* (en un solo sentido), de manera que no es posible desencriptar. En el momento del logeo, se encripta la contraseña ingresada por el usuario y se compara ésta contraseña encriptada con el dato almacenado que también está cifrado, si ambos son diferentes el logeo será fallido. Para modificar las passwords, Linux accede a los datos simulando ser root, por lo que es posible la transacción.

3- SEGURIDAD DE LAS APLICACIONES

OBJETIVO DE AUDITORÍA: la Auditoría Informática deberá evaluar la seguridad de las aplicaciones utilizadas en La Empresa, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento, de acuerdo a los estándares propuestos.

3.1 SOFTWARE

En la Empresa hay dos servidores, con **sistema operativo** Linux Mandrake para el servidor de aplicaciones y Bea Linux para el de Internet. Como resultado de una auditoría se eligió este sistema operativo por las siguientes razones:

- Porque necesitaban migrar a un sistema con entorno gráfico,
- Por el bajo costo (y la diferencia de precio con Windows NT),
- Porque estaban utilizando un sistema operativo (C-Tos) que era muy similar al Unix y la migración resultaba fácil,
- Por la confiabilidad,
- Por la compatibilidad que tiene con Windows (en el explorador de Windows se pueden ver las carpetas compartidas de Linux por el uso de un emulador),
- Por el buen control de acceso y la buena generación de logs de auditoría,
- Por la posibilidad de conseguir actualizaciones,
- Por el software de aplicación gratis,
- Por una experiencia mala con Windows, y una buena experiencia con UNIX,
- Por buenos consejos de profesionales capacitados de la UTN.

Las **aplicaciones** en la Empresa estaban desarrolladas en Cobol y actualmente se están migrando a AcuCobol, en entorno gráfico. Hasta el momento esta reingeniería se encuentra en el 80% del desarrollo total del sistema. Los módulos del sistema que se han completado se encuentran funcionando desde hace aproximadamente un año y medio.

El 80% de las PC's usan el sistema operativo Windows 98, en el resto de ellas hay Windows Millennium y Windows XP. No usan software comprado, a excepción de los sistemas: Microsoft Office, StarOffice, Norton Antivirus, y demás utilitarios, y sistemas propietarios de las fábricas, como FIS (Ford Internet System) y uno similar de la VW.

3.2 SEGURIDAD DE BASES DE DATOS

En la empresa se utiliza el AcuCobol para el desarrollo y la administración de los datos, los cuales están almacenados en un **sistema de archivos indexados**, a pesar de que AcuCobol tiene soporte para bases de datos. Esta implementación se debe a que los datos anteriores se encontraban en un sistema de archivos y el sistema nuevo fue

implantándose en paralelo en la empresa, de manera que todavía existen usuarios (los del sector de contaduría) que siguen utilizando el sistema anterior. Entre los planes del centro de cómputos se encuentra hacer la **migración** de este sistema de archivos a uno de bases de datos.

Existe un control que restringe el acceso a ciertos datos críticos en las aplicaciones propias de la empresa, pero no hay una **clasificación formal de estos datos**.

No se realizan **controles de acceso lógico**, a las carpetas donde se almacenen los archivos indexados, ya que estos archivos están en una carpeta del servidor no compartida para el resto de la red, a lo que se agregan los controles de seguridad física del servidor.

Las únicas personas que pueden tener acceso a los archivos de la base de datos son los administradores y todo aquel que opere el servidor de aplicaciones (es decir las personas que tengan acceso físico al equipo). En este servidor hay instalado un editor SQL (usado para programar las impresoras fiscales), y el AcuServer, programas con los que es posible editar los archivos indexados.

Los aplicativos que administran la base de datos disponen de **recursos suficientes** para su funcionamiento, ya que aproximadamente solo el 30% de los recursos del servidor están en uso, el resto está ocioso.

Cuando algún usuario elimina registros de una base de datos, éstos **no se borran físicamente** sino que son marcados como borrados. De esta forma siempre permanecen los registros de las transacciones realizadas.

3.3 CONTROL DE APLICACIONES EN PC'S

No hay **estándares** definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la **instalación y actualización** de la configuración de las PC's. Solo hay una instalación básica de alguna versión del Windows, Internet Explorer, Norton Antivirus y una versión ejecutable de AcuCobol que inserta las librerías necesarias para que corran las aplicaciones desarrolladas.

En el caso de que una PC presente errores en su configuración, se utilizan **herramientas de reparación** de errores, como el Norton Disk Doctor, con el fin de evitar la reinstalación total del sistema y así causar una pérdida innecesaria de tiempo.

Tampoco se realizan **actualizaciones de los programas instalados**, como el Internet Explorer y el Microsoft Office. No se buscan Service Packs ni nuevas versiones. La política de actualización de programas que se lleva a cabo permite actualizar los programas solo si es necesario debido a algún mal funcionamiento o nuevo requerimiento, lo que facilita la continuidad de los programas.

Las únicas **versiones** que se actualizan y quedan documentadas son las de los programas desarrollados por la Empresa, a pedido de algún departamento. Estas versiones se actualizan directamente en el servidor, lo que evita hacer el control en cada una de las máquinas.

Solamente los administradores del centro de cómputos son los encargados de las **instalaciones** en las PC's, aunque para los usuarios no existen restricciones con respecto a la instalación de programas. Pueden bajar de la web cualquier aplicación e instalarla en su PC sin ningún control sobre las licencias ni autorización previa. Esto se debe a que, para controlar problemas de **licencias, virus o programas no**

permitidos, no hay ninguna herramienta en uso ni se realizan auditorías internas periódicas. En una sola oportunidad fue necesario el registro on line de un aplicativo de emisión de mails que solicitó la gerencia.

Cuando se hace un **cambio en la configuración del servidor**, se guardan copias de las configuraciones anterior y posterior al cambio, pero no se documentan los cambios que se realizan ni la fecha de las modificaciones.

3.4 CONTROL DE DATOS EN LAS APLICACIONES

En las aplicaciones desarrolladas en la empresa se implementan controles en los **datos de entrada** (archivos y datos ingresados manualmente) y de salida, que aseguran su integridad, exactitud y validez.

Con respecto a los **datos de salida**, existen diversas restricciones:

- se deshabilitan los portapapeles,
- se restringen las impresiones en ciertos sectores de la empresa (ventas), y de cierta información confidencial,
- se deshabilita la barra de herramientas de manera que no se puedan grabar ni imprimir los datos,
- se deshabilita el menú contextual (surgido del botón derecho del mouse), lo que impide solo permite que la información sea leída.

Se utiliza un programa freeware, cuya función es **sincronizar la fecha y hora** de cada una de las PC's de la red cada un minuto, de acuerdo al horario del servidor. De esta forma los logs y los datos siempre se generan con la fecha del servidor.

3.5 CICLO DE VIDA

La Empresa cuenta con **aplicaciones propias** desarrolladas para cada uno de los sectores que la componen, por su grupo de programadores internos. Este desarrollo no sigue una metodología estándar, pero se usa la misma nomenclatura para denominar variables, tablas, parámetros, etc. Durante el ciclo de vida no se priorizaron los requisitos de seguridad del sistema, debido a la urgencia que envestía el proceso de reingeniería de sistemas.

Análisis: debido a que se trata de una reingeniería de sistemas, no se realizó un relevamiento formal para el desarrollo. Los programadores tenían noción de los requerimientos y necesidades de los usuarios por el conocimiento del sistema anterior; y a este se lo mejoró implementando nuevas funciones que demandaban los jefes de cada sector.

Desarrollo: la implementación del sistema se está desarrollando en AcuCobol. Al comienzo del desarrollo se evaluaron las incidencias que podían representar los cambios en el sistema con respecto al sistema anterior, completándose así un análisis de riesgo preliminar. No se utilizaron métricas para la estimación ni durante el desarrollo.

Prueba: para el testeo del sistema se generan casos de pruebas, donde se definen tablas con valores de entrada al sistema. Cuando se hacen modificaciones en los programas, los casos de pruebas que se usan sobre el software modificado son los

mismos que se usaron antes, de manera de comprobar que los valores obtenidos en las últimas pruebas sean los mismos que los que surgieron de las primeras. Las pruebas se realizan por módulos, y al integrar los módulos se realizan pruebas de integración. Los resultados obtenidos en las pruebas son documentados en las carpetas relativas a cada uno de los módulos.

Instalación y modificaciones: una vez hecha la instalación, las únicas modificaciones que se realizan son a pedido del gerente del área correspondiente, pero sin la implementación de un formulario de solicitud de cambio. Antes de hacer las modificaciones solicitadas, se confecciona un análisis de riesgos, considerando el impacto que puede provocar el cambio, con el fin de decidir la implementación del mismo. No se lleva a cabo ningún control de versiones ni gestión de configuración de las modificaciones.

Documentación: cada módulo desarrollado posee una carpeta con diagramas y documentación sobre el mismo. Se han desarrollado manuales para el área de Gestoría y para el sector de Ventas de la empresa, aunque todavía no están confeccionados los manuales para la totalidad de los módulos. Una meta del equipo de desarrollo es documentar el sistema en su totalidad, e incluso modificar los manuales existentes para generar un manual de usuario completo que englobe todo el sistema de la empresa.

Terceros: con respecto a la participación de terceros en el desarrollo, existió un único caso, que consistió en el desarrollo de una página web dinámica, implementada por un programador externo. Ésta fue entregada a la Empresa, con su código fuente desarrollado en PHP, junto con los manuales de uso.

La página web fue diseñada para que todo el mantenimiento pueda desarrollarse desde el interior de la empresa, a excepción de las modificaciones que se llevan a cabo en la estructura de la página. Es una página dinámica en el área de consultas de usados, turnos del taller y consultas en general. La página se modifica desde el servidor de Internet, con un administrador desarrollado en HTML para este fin. Esta página se encuentra on line en un host externo, lo que resta una gran cantidad de riesgos a la empresa, debido a que permite que no se reciba ningún requerimiento del exterior vía web, lo que podría atentar contra la integridad de los datos.

4- SEGURIDAD FÍSICA

OBJETIVO DE AUDITORÍA: se evaluará que el centro de cómputos, los equipos, los dispositivos, los medios de almacenamientos y las personas que conforman el sistema informático de La Empresa cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos de la organización.

4.1 EQUIPAMIENTO

4.1.1 CARACTERÍSTICAS DE LOS SERVIDORES

En la casa central existen dos **servidores** iguales con las siguientes características:

- Servidores Hewlett Packard LC 2200, comprados en el año 2000. Uno de ellos es el servidor de aplicaciones y datos, y el otro es servidor de Internet. Cada uno contiene:
 - 2 Procesadores (redundantes) Pentium III 550 MHz
 - 2 Fuentes (redundantes)
 - 2 Placas de red (redundantes)
 - 1 GB de memoria RAM.
 - 3 discos con tecnología SCSI con 18 GB de capacidad cada uno.
- Sistema UPS de suministro alternativo de energía.
- Generador de energía eléctrica.

4.1.2 CARACTERÍSTICAS DE LAS PC'S

La empresa en su totalidad posee alrededor de 100 PC's, de las cuales 60 están en la casa central.

El 40% de estas PC's es de marca Unisys (60%) o Hewlett Packard PC 100 (40%). En sus principios no contaban con aplicaciones gráficas, sino con el sistema operativo CTOS basado en entorno caracter. Al ir migrando a aplicaciones y sistemas operativos gráficos, fueron adquiriendo clones con mayor capacidad, actualizando el motherboard, el procesador, el gabinete y la cantidad de memoria RAM, y conservando el resto del hardware.

La empresa ha tomado la decisión de **asegurar** su red, debido al gran costo que implicaba contratar un mantenimiento tercerizado permanentemente.

4.2 CONTROL DE ACCESO FÍSICO AL CENTRO DE CÓMPUTOS

En el momento de la instalación del centro de cómputos no se efectuó un **análisis de costo-beneficio** para determinar que controles de acceso físico sería necesario implementar.

Existe un circuito cerrado de **cámaras de video**. Este sistema no es exclusivo del centro de cómputos, ya que las cámaras están en toda el área administrativa de la

empresa, ubicadas en puntos estratégicos, como en la puerta de ingreso, pero ninguna de éstas cámaras apunta al centro de cómputos o a su puerta de ingreso.

La empresa cuenta con **guardias de seguridad**; en horarios laborales se ubican en el interior y exterior de la misma, y cuando se cierra la empresa solo quedan en el exterior, porque queda activado el sistema de alarma. No hay tarjetas magnéticas de entrada ni llaves cifradas en ningún sector del edificio.

El personal que tiene el **acceso permitido al centro de cómputos** es el de cómputos, administración y gerencia, que están en el mismo ambiente, separados del resto de la empresa por una doble puerta. Las demás áreas son gerencia, créditos, auto-ahorro y ventas, que no tienen permiso de acceso.

Esta **doble puerta** que separa este ambiente de administración gerencial del resto de la empresa tiene la función de evitar el acceso físico de cualquier persona no autorizada, sin identificación previa. De manera que las personas que pretenden entrar deben permanecer entre dos puertas, ya que no se puede abrir la segunda si no se cierra la primera, a partir de ahí un encargado debe autorizar el acceso mirando por un circuito cerrado de televisión.

Por más que siempre hay personal de sistemas en el interior del centro de cómputos, cualquier **persona ajena a la empresa** que necesite realizar una tarea de mantenimiento relativa al centro de cómputos deberá anunciarse en la puerta de entrada. El personal del centro de cómputos es el encargado de escoltarlo desde la puerta hacia el interior del edificio, acompañándolo durante el transcurso de su tarea, hasta que sea concluida.

4.3 CONTROL DE ACCESO A EQUIPOS

Todas las máquinas de la empresa disponen de **disqueteras y lectoras de CD**, aunque el 90% de los usuarios no las necesita. Solo algunas máquinas de administración que reciben disquetes de la Dirección General de Rentas o del Gobierno deben utilizarlas como medios de entrada de datos, a pesar de que se está empezando a utilizar Internet para el intercambio de información.

Estos **dispositivos** están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos. Nunca hubo robo de datos usando medios externos, solo fue necesario hacer bloqueos de las impresoras para restringir los datos de salida del sistema, previniendo posibles fraudes. En el centro de cómputos hay unidades de zip no utilizadas, guardadas sin llave ni control de acceso adicional. Esto implica que podrían ser fácilmente robados, o cualquier persona que disponga de los instaladores necesarios, podrá instalar dichas unidades en cualquier PC de la empresa.

Los **gabinetes** donde se ubican los switches de cada una de las sucursales, están cerrados con llave, para evitar que el personal de limpieza o cualquier persona desconecten las entradas, y como medida de precaución, debido a que hay bocas libres en estos dispositivos. Las llaves de todos los gabinetes están en el centro de cómputos de la casa central, en poder del administrador del sistema. Todos ellos están ubicados fuera del alcance del personal (a la altura del techo, o en espacios donde hay poca circulación de personal).

No se realizan **controles periódicos** sobre los dispositivos de hardware instalados en las PC's, de manera que alguien podría sacar o poner alguno. Una vez que se ha

completado la instalación de algún equipo, el administrador del sistema no realiza chequeos rutinarios o periódicos, solo revisa los equipos ante fallas en los mismos, o por un problema reportado por el usuario.

Los servidores del centro de cómputos no se apagan en **horarios no laborales**, permanecen prendidos las 24 horas del día, aunque durante la noche no se realizan trabajos, permanecen ociosos, debido a que no existen procedimientos en lote (todos los programas se ejecutan on line).

4.4 DISPOSITIVOS DE SOPORTE

En la empresa disponen de los siguientes **dispositivos para soporte** del equipamiento informático:

- **Aire acondicionado y calefacción:** la temperatura se mantiene entre 19°C y 20°C. Cuentan con un equipo de refrigeración central, y en el centro de cómputos hay un equipo adicional de aire acondicionado, solo para esta área, con el fin de mantener esta temperatura en verano. Estas especificaciones las sugirió el personal que provee los equipamientos.
- **Matafuegos:** son equipos químicos, manuales y están instalados y mantenidos por una empresa externa, quienes deciden el lugar en que van a estar ubicados, el centro de cómputos cuenta con uno propio, ubicado en la habitación de los servidores.
- **Alarmas contra intrusos:** existe una alarma en la empresa que se activa en los horarios no comerciales, generalmente de noche cuando se cierra la empresa.
- **Generador de energía:** en la empresa cuentan con un generador de energía debido a los frecuentes cortes de luz. Necesita de un breve tiempo de puesta en marcha, pero debido a que los cortes también son breves (5 minutos) pocas veces se utiliza.
- **UPS:** (Uninterruptible Power Supply) en el centro de cómputos hay dos UPS en serie que pueden mantener los servidores y las máquinas de desarrollo funcionando por 2 horas.
- **Estabilizador de tensión:** la corriente eléctrica proviene de un tablero independiente al que llega la línea de EPEC, esta línea va a tres estabilizadores de tensión de donde salen tres líneas. Se dividió la carga eléctrica en tres sectores para un mejor funcionamiento:
 - Un sector abarca el centro de cómputos y tres usuarios más.
 - Los demás usuarios de la empresa se reparten entre las otras dos líneas libres.
- **Descarga a tierra:** hay dos jabalinas que funcionan como descarga a tierra, una para el edificio y otra para el centro de cómputos.
- **Luz de emergencia:** en el centro de cómputos hay una luz de emergencia que permanece en carga las 24 horas del día y en el caso de un corte de luz se activa automáticamente.
- **Humidificador para la biblioteca de cintas y centro de cómputos:** no hay archivos en cintas por lo que no son necesarios estos dispositivos.
- **Piso aislante:** el personal que proveyó el equipamiento sugirió poner un piso aislante de goma, que se usaba para los centros de cómputos cuando las

máquinas generaban mucha inducción, pero debido a que los dispositivos actuales no generan ese nivel de inducción, no fue necesaria esta protección.

4.5 ESTRUCTURA DEL EDIFICIO

Cuando se construyó el edificio de la empresa, se tuvo en cuenta el **diseño del centro de cómputos** y sus condiciones de seguridad. Por este motivo se lo ubicó en el sector posterior del edificio, para restringir el acceso. Está ubicado en un piso elevado, ya que en los pisos superiores se encuentra el sector administrativo, mientras que en la planta baja se ubica el taller. Éste no produce ninguna interferencia ni ruidos, ya que esta es una restricción de las normas IRAM certificada por el taller de Ford.

Las **paredes externas** del centro de cómputos son elevadas (aproximadamente 6 mts.) y las ventanas tienen rejas soldadas y vidrios espejados que impiden la visibilidad desde el exterior del mismo.

En toda la empresa hay vidrios esmerilados, que **dividen los sectores** del área administrativa, por lo que solo se ven los monitores desde el interior de cada área.

El equipamiento informático fue provisto por una empresa que se encargó del **asesoramiento técnico**. A estos proveedores les consultaron cuáles eran los requisitos mínimos necesarios para que las garantías cubriesen los equipamientos (la instalación eléctrica necesaria, la refrigeración correcta del área, los métodos de aislamiento magnético, etc.) Para determinar qué medidas tomar en la instalación se realizó un análisis costo – beneficio donde se decidió, por ejemplo, no implementar un piso falso en el centro de cómputos para el aislamiento, debido a que la poca inducción que podía existir no representaba un gran riesgo para la empresa, y el costo era muy elevado.

El centro de cómputos se diseñó pensando en su futuro **crecimiento** y actualmente sus instalaciones se encuentran convenientemente ubicadas, con la posibilidad de expandirse sin inconvenientes.

4.6 CABLEADO ESTRUCTURADO

La instalación del cableado fue tercerizada, y se implementó un **cableado estructurado**, brindándole a la empresa una garantía escrita. Para diagramar los canales de red se tuvieron en cuenta los posibles desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos.

Se implementó un techo falso, por donde tendieron el **cableado**, de fácil accesibilidad ya que se sacan los paneles que lo componen. Desde allí los cables pasan por las columnas del edificio, desde las cuales bajan hasta los perfiles de aluminio de los paneles que dividen los boxes, y por estos llegan hasta el suelo. Estos paneles no son prácticos a la hora de hacer modificaciones en el cableado, debido a la cantidad de cables que pasan por ellos y al poco espacio con el que cuentan, pero resultaron económicos y son seguros en cuanto no es fácil desarmarlos. Por este motivo, y para facilitar la tarea de agregar cables en el interior de los paneles, hay tendido de cableado redundante. Estos cables no tienen bocas instaladas, pero sí están conectados al switch. En una de las sucursales hay cables en el techo protegidos por cable canal, fuera del alcance del personal. En el resto de la red no hay bocas libres, ni puertos disponibles para poder instalar nuevas PC's o equipos móviles.

En todo el trayecto del cableado se tuvo en cuenta la **distancia mínima** necesaria entre cables para no provocar interferencias, daños o cortes. Además no hay distancias grandes recorridas con cables UTP, para estas largas conexiones se utiliza fibra óptica o radio.

En el **switch** hay una boca dedicada para cada máquina, y bocas de sobra por una posible ampliación de la red. Además hay dos **hubs** que llegan al switch, los cuales conectan dos y tres máquinas respectivamente. Esto se configuró de esta manera porque la empresa disponía de los hubs y, aunque se disminuye la velocidad de la red, en el análisis de costo - beneficio no se justificaba el gasto de un cableado nuevo para cinco equipos.

Para que no haya interferencias se utilizó cableado UTP categoría 5, fibra óptica para conectar los edificios y enlaces de radio para enlazar las sucursales. Si se llega a caer la conexión radial en una de las sucursales, el sistema de radio queda inutilizable desde esa sucursal caída hasta la última. El mantenimiento de dichas antenas lo realiza una empresa externa.

Los cables en la patchera están numerados de manera que se los puede identificar fácilmente.

Detrás de cada máquina hay un **conector** triple que tiene:

- 1 Boca UTP
- 1 Potencia estabilizada
- 1 Boca de teléfono.

Todas estas líneas no producen **interferencias** debido a la calidad de los cables de red, y a que la línea eléctrica está estabilizada. Además, la empresa encargada de la instalación de la red midió la interferencia que hay en las bocas de red de las PC's encontrando que eran muy bajas y no representaban riesgos.

4.6.1 ANCHO DE BANDA DE LA RED

La empresa externa que instaló la red hizo una medición de la transmisión máxima que podía utilizarse, obteniendo un valor de 3,5 a 4MB en el caso que se utilicen todos los recursos de red disponibles (esto es ejecutando la aplicación e Internet al mismo tiempo). Este valor representaba un 70% de la capacidad de transmisión que garantizaba la empresa, ya que las antenas de transmisión radial tienen 12MB de ancho de banda, de los cuales se garantizan 6MB para la transmisión. Mientras que en el cableado hay UTP de 100MB.

4.6.2 FALLA EN LA RED

Por norma, cuando hay un **corte de luz** se graban los datos y se deja de trabajar on line. Si el corte supera la media hora de duración, entonces apagan los servidores como una medida de prevención y si es necesario, se enciende el generador de energía. Mientras tanto, las tareas continúan realizándose en forma manual.

En el caso de un corte en el servicio de red por falta de energía, **falla en las antenas o en el switch**, el área más crítica sería la de taller y repuesto, que hacen facturación en tiempo real. Si llega a haber un fallo, hay papelería para implementar las funciones en forma manual y una vez restaurado el sistema estas facturas se cargan al mismo.

5- ADMINISTRACIÓN DEL CPD

OBJETIVO DE AUDITORÍA: los auditores deberán evaluar la correcta organización y administración del área de sistemas (Centro de Procesamiento de Datos), así como la asignación de tareas y responsabilidades del personal que la conforma; a fin de que ésta brinde condiciones óptimas de operación que posibiliten un ambiente adecuado de control y permitan mejorar la disponibilidad de sus servicios, de acuerdo a las normas existentes que regulan esta actividad.

5.1 ADMINISTRACIÓN DEL CPD

5.1.1 RESPONSABILIDAD DEL EQUIPO DE SISTEMAS

No hay responsabilidades puntuales asignadas a cada empleado, tampoco hay un encargado de la seguridad. Existe un responsable general del área de sistemas, que es el administrador del centro de cómputos. Él es el que planifica y delega las tareas a los empleados del centro de cómputos, generalmente una vez por semana haciendo responsable a cada uno de sus propios tiempos. Además del administrador, hay una persona dedicada al mantenimiento de la página y cuatro desarrolladores del sistema.

El administrador es el encargado de reportar a los gerentes sobre las actividades en el centro de cómputos. Estos reportes generalmente se realizan a modo de auto evaluación ya que no son un pedido de ningún directivo.

5.1.2 PLANES DE SISTEMAS

No se han desarrollado **planes formales** del departamento de sistemas, solo se hace una distribución de tareas semanalmente entre el personal de esta área.

La reingeniería del sistema es el **proyecto** prioritario, luego tienen proyectos a futuro, como es la migración del sistema de archivos a una base de datos. Se van asignando prioridades a las tareas a medida que surgen. No hay normas, estándares o procedimientos en las que se basen para la planificación, el control y la evaluación de las actividades del área de sistemas de información.

5.1.3 PERMISOS DE LOS ENCARGADOS DEL CENTRO DE CÓMPUTOS

Cuando entra un nuevo empleado al centro de cómputos, no se le asignan los mismos permisos que al resto de los empleados. A modo de ejemplo: no se le otorgan permisos de acceso a Internet ni cuenta de mail mientras están capacitándose en el uso de la herramienta de desarrollo. A medida que le son asignadas más responsabilidades y sean necesarios más permisos, se va modificando su cuenta de usuario. Estos permisos son asignados por el administrador del centro de cómputos.

5.1.4 IMPORTANCIA DE LA SEGURIDAD

Los empleados de la gerencia y de los cargos más altos tienen plena conciencia de la importancia de la seguridad en la empresa, porque fueron ellos los que encargaron el sistema con los requerimientos que tiene actualmente, aunque pudimos comprobar que no siempre cumplen las disposiciones de seguridad impuestas. Los demás

empleados de la empresa tienen conocimientos de las normas pero no son conscientes de su importancia.

5.1.5 *MANTENIMIENTO*

- **Solicitud de mantenimiento:** cada vez que los usuarios necesitan asesoramiento o servicios del centro de cómputos, se comunican telefónicamente con el administrador explicando su situación. No queda ninguna constancia de las tareas desarrolladas por los empleados del centro de cómputos, ni de las solicitudes de los usuarios.
- **Mantenimiento preventivo:** en este momento en el centro de cómputos no se desarrolla ningún mantenimiento preventivo, debido al costo de contratar una persona más que se dedique a esto, ya que los empleados del centro de cómputos están ocupados en el desarrollo del sistema.
- **Clasificación de datos y hardware:** los equipos de la empresa no han sido clasificados formalmente según su prioridad, aunque se puede identificar que las máquinas que están en el sector de atención al público tienen mayor prioridad que el resto. En la escala siguen las de gerencia, y por último el resto de las PC's, en cuanto al orden de solución de problemas. Si llega a haber un cliente esperando en alguna máquina, entonces esa es la PC que tiene la mayor prioridad en ese momento.
- **Rótulos:** no hay procesos para rotular, manipular y dar de baja un equipo, sus periféricos o los medios de almacenamiento, solo las licencias de software están registradas. Las máquinas y dispositivos no se identifican entre ellas aunque hay un inventario de la cantidad de máquinas que existen pero no tiene detalles suficientes.

5.1.6 *INTERACCIÓN CON EL USUARIO*

- **Publicidad de normas:** normalmente los avisos cotidianos o de rutina se hacen a través de mail. Para el anuncio de una nueva norma o la modificación de un procedimiento existente se emplearía la misma metodología que en la capacitación de los usuarios, con mailing informativo y reuniones en la sala de reuniones.
- **Boletín informativo:** en la empresa utilizan un boletín informativo que se emite sin frecuencia fija, cada vez que es necesario informar al usuario, o para recordarles las tareas de mantenimiento de sus equipos que deben realizar, como por ejemplo actualizar el antivirus, hacer copias de respaldo de sus datos, defragmentar el disco, modificar y proteger sus password, borrar archivos temporales, entre otras.
- **Buzón de sugerencias:** no han implementado un buzón de sugerencias donde los usuarios puedan expresar sus inquietudes.

5.1.7 *INSTALADORES*

Los instaladores de las aplicaciones utilizadas en la empresa se encuentran en sus CD's originales almacenados en un armario del centro de cómputos, y no disponen de instaladores en disquetes.

Los instaladores de uso más frecuente, como los del Norton Antivirus o del Acrobat Reader, están on line en el servidor y se instalan desde carpetas compartidas. Otros

igualmente utilizados, como las distintas versiones de Windows, se ejecutan desde copias de los CD's originales, para evitar posibles daños en los discos originales.

5.1.8 LICENCIAS

Como ya enunciamos, en el centro de cómputos se mantiene un registro de los números de licencia de las aplicaciones instaladas en las PC's y los servidores de la empresa. Los programas de los que se disponen licencias son los siguientes:

- Windows 98, Millennium y XP en las PC's.
- Microsoft Office y StarOffice en las PC's.
- Norton Antivirus Corporativo.
- IncrediMail.

El resto de las aplicaciones son propietarias, por lo que no necesitan de licencias, o son freeware como el Acrobat Reader y los Linux de los servidores.

5.2 CAPACITACIÓN

La capacitación de los usuarios fue desarrollándose por áreas, a medida que se completaban los distintos módulos del sistema. Cuando ingresa un empleado nuevo a la empresa se lo capacita en el uso del sistema, de la misma forma en que han sido capacitados los empleados efectivos: en la sala de reuniones el encargado del departamento de sistemas le enseña el funcionamiento del sistema, aunque si el grupo de usuarios es reducido las charlas pueden darse en el centro de cómputos.

En estas charlas se les instruye sobre consideraciones de seguridad como:

- no usar password fáciles de descifrar,
- no divulgarlas,
- no escribirlas ni guardarlas,
- entender que la administración del password es el principal método de seguridad del sistema.
- no modificar la configuración de las PC's (configuración de red o del sistema),
- no abrir mails con asuntos en inglés ni de destinos desconocidos.

Estas charlas las da el administrador del sistema junto con dos personas del equipo, generalmente los que trabajaron en el desarrollo del módulo que está siendo presentado. Una vez que han sido instruidos con una capacitación teórica, el personal del departamento de sistemas se instala junto con los usuarios en los puestos de trabajo, para asistirlos hasta que adquieran práctica, comprobando que el manejo del sistema sea el adecuado.

En ningún momento, hay consentimiento por parte de los usuarios a que auditen sus actividades en el sistema, ni declaraciones de que conocen las normas de "buen uso" del sistema.

5.3 BACKUP

5.3.1 BACKUP DE DATOS EN EL SERVIDOR

Cuando se hace un **cambio en la configuración del servidor**, se guardan copias de las configuraciones anterior y posterior al cambio, pero no se documentan los cambios que se realizan ni la fecha de estas modificaciones.

No hay ningún procedimiento formal para la realización ni la recuperación de los backups. Además no se realizan chequeos para comprobar que el funcionamiento sea el correcto.

Los backups se hacen diariamente a última hora, a las 5 p.m. Es un proceso que no está automatizado, por lo que todos los días, antes de irse, cada desarrollador copia los archivos que ha modificado durante el día a una carpeta del servidor de aplicaciones. Luego se agregan los archivos de la empresa modificados por los usuarios. Una vez generada esta carpeta, el administrador del sistema la zipa y copia este archivo a un CD, proceso que demora 1 hora aproximadamente.

Estos backups son incrementales, es decir que se agregan a la carpeta los archivos modificados y se backupea todo lo que ésta contiene. Debido a que se realizan estos tipos de backup incrementales, es imposible recuperar versiones antiguas de aplicaciones desarrolladas y luego modificadas, ya que se sobrescriben con las versiones nuevas. No se hacen backups de cada una de las versiones del sistema por separado, se resguardan los datos a medida que van siendo modificados.

Los sábados y domingos la empresa permanece abierta y se generan datos, pero no se actualizan los backups hasta el lunes siguiente.

Para realizar el backup se utilizan cinco discos compactos, uno para cada día de la semana, y se regraba el disco que corresponde a ese día. Los 5 CD's se los lleva a su casa un empleado de la empresa designado por la Gerencia. Si este empleado no asistiera a trabajar, no hay asignado ningún reemplazante, en ese caso el administrador del centro de cómputos delegaría a alguien esta responsabilidad.

Los CD's regrabables usados en la empresa no han sido reemplazados por otros nuevos. No hay políticas de reemplazo de estos medios de almacenamiento, ni se les realizan controles para comprobar que están en buen estado y que su funcionamiento es el correcto.

No hay un responsable designado para realizar los backups, aunque generalmente los hace una sola persona, el responsable del área o administrador del centro de cómputos. Tampoco hay ninguna política en cuanto a asignar un responsable para la restauración de los datos de los backups, esta tarea también la realiza el administrador.

Se han hecho pruebas de la recuperación de los backups en CD, cuando comenzaron con este procedimiento, y estas pruebas resultaron satisfactorias, pero no hay políticas de recuperación ni chequeos periódicos de este proceso. Los backups que se generan sobre las bases de datos han sido recuperados dos veces por emergencias, obteniéndose resultados positivos.

5.3.2 BACKUP DE DATOS EN LAS PC'S

Los usuarios deben realizar sus propios backups de los datos almacenados en sus máquinas, ya que estos datos son propiedad de los empleados. Generalmente no los backupean, debido a que los archivos que almacenen son de soporte o de poca importancia para la empresa.

Los usuarios han sido instruidos a almacenar en la carpeta Mis Documentos todos los datos que ellos generen. Si hacen un backup deberían hacerlo en sus propias máquinas o en disquetes, aunque hay un usuario que tiene asignado un espacio del servidor para guardar allí sus copias de respaldo, debido a que sus datos son mas sensibles. Este backup se realiza a través de un archivo .bat que copia sus datos al servidor.

5.3.3 BACKUP DE LA PÁGINA WEB

El administrador del sistema realiza un backup de la página web completa en una PC del centro de cómputos, pero sin una frecuencia preestablecida.

5.3.4 BACKUP DE LOGS

No se hace ningún backup de los logs generados por las diferentes aplicaciones del servidor, solo se los almacena y se depuran mensualmente.

5.3.5 PROTECCIÓN DE LOS BACKUPS

Los archivos backupeados no están protegidos con ningún control de acceso ni encriptación. Esta situación puede resultar peligrosa ya que estos archivos contienen las bases de datos de la empresa y, ante cualquier incidente o extravío de los mismos, es fácil recuperar los datos en su formato original.

5.3.6 DOCUMENTACIÓN DEL BACKUP

No hay documentación escrita sobre los datos que se backupean, dónde se hace esta copia ni datos históricos referidos a la restauración de los mismos.

5.4 DOCUMENTACIÓN

5.4.1 DOCUMENTACIÓN DEL CENTRO DE CÓMPUTOS

En el centro de cómputos existe documentación sobre:

- Licencias del software, y en qué máquinas está instalado,
- Números IP de las máquinas y de los switches,
- Planos de la ubicación de los canales de red, desarrollados por la empresa que instaló la red,
- Gráficos de la ubicación física de los equipos de los distintos locales,
- Inventario de insumos,
- Documentación del desarrollo del sistema.

No hay backups de ninguno de estos datos, ya que son documentos impresos que se van modificando manualmente.

5.4.2 MANUALES

No hay ningún plan de contingencia a seguir, ni un plan de continuidad. No hay desarrollado ningún plan de seguridad ni procedimientos formales. Se comenzó a desarrollar un manual de usuario del sistema pero se completó solo un 30% del mismo, y ahora a quedado desactualizado. Además se desarrollaron los manuales para las áreas de Gestoría y Ventas, aunque éstos también están desactualizados.

Está en los planes del administrador del centro de cómputos desarrollar manuales de usuario explicando, para cada módulo del sistema (o área de la organización), el funcionamiento del mismo.

5.4.3 DOCUMENTACIÓN DEL DESARROLLO

Existe una carpeta con diagramas y documentación referente a cada módulo del sistema, y allí se registran los cambios que se producen durante el uso del sistema. Estos registros se generan durante las etapas de desarrollo y mantenimiento, pero no se actualizan los demás documentos o manuales cuando se hace una modificación del sistema, de manera que el cambio solo queda registrado en papel.

6- AUDITORÍAS Y REVISIONES

OBJETIVO DE AUDITORÍA: la Auditoría Informática deberá evaluar las metodologías de control, auditorías internas y revisiones que se lleven a cabo en forma periódica, con el fin de encontrar debilidades y proponer mejoras, con base en las normativas que asesoran en el buen desempeño de la auditoría interna en una Organización.

6.1 CHEQUEOS DEL SISTEMA

6.1.1 HERRAMIENTAS DE GENERACIÓN Y ADMINISTRACIÓN DE LOGS

En la empresa las siguientes **aplicaciones** o sistemas generan logs de auditoría:

- El kernel del sistema operativo de los servidores (Linux)
- El antivirus y el Proxy del servidor de Internet
- En AcuServer (o manejador de archivos del sistema de la empresa)

Cada una de las aplicaciones que genera los logs utiliza una carpeta diferente para su almacenamiento.

Para graficar los logs de auditoría se utiliza una aplicación llamada **Monitor**. Ésta lee los logs generados por las distintas aplicaciones cada cinco minutos, calcula las estadísticas y, cuando se llama al programa, grafica éstos valores. Este programa tiene la capacidad de no consumir gran cantidad de recursos.

Los procesos de rotación y eliminación de logs los realiza una aplicación llamada **CronTab**. Todos los registros (del sistema operativo, del Proxy, del antivirus y del AcuServer) se almacenan durante tres meses, y este programa se encarga de hacer la rotación mensual y eliminar los logs del mes saliente.

Los chequeos de logs se hacen manualmente ya que no hay una aplicación de administración de logs que genere reportes, ni hay alarmas en el sistema que avisen al administrador de la ocurrencia de un evento en particular.

Todos los **logs** contienen los siguientes campos:

- Fecha y hora
- Fuente (el componente que disparó el evento)
- ID del evento (número único que identifica el evento)
- Computadora (máquina donde se logeo el evento)
- Descripción (datos asociados con el evento o mensajes de error)

6.1.2 LOGS DE LOS SERVIDORES

El kernel de Linux monitoriza los servidores generando entre otros, **logs** sobre:

- los servicios de mail,
- servicios de red,
- configuración,
- utilización del CPU,

- reinicio de servidores.

No se han buscado nuevas herramientas de generación ni gráfico de logs, por falta de tiempo.

6.1.3 LÍNEA DE BASE

Existen valores que se recogen de los logs, son estadísticas generadas por el Monitor de red, en forma diaria, semanal, mensual y anual, con datos sobre tráfico de red, cantidad de archivos abiertos, uso de memoria, uso del disco y uso del swap. Todos estos datos no generan una línea de base ya que no están almacenados como tal, sino que son datos **estadísticos no persistentes** calculados por el Monitor para realizar los gráficos.

Al hacer alguna modificación en la configuración del sistema, se genera una nueva compilación de datos (**nueva línea de base**), que no queda documentada. Esto se presta a confusiones, ya que no se identifica si ha habido algún incidente o si la variación se debe a cambios realizados en el sistema.

6.1.4 AUDITORÍAS INTERNAS

En la empresa no se realizan **auditorías programadas**, ni **rutinas de chequeos de logs**, debido a que la política actual de la empresa es realizar controles solo cuando se presentan problemas o ante necesidades puntuales.

6.2 RESPONSABILIDADES DE LOS ENCARGADOS DE SEGURIDAD

El **encargado del centro de cómputos**:

- Administra, desarrolla e implementa los procedimientos de auditoría y revisión.
- Monitoriza y reacciona a los avisos (warnings) y reportes.
- Realiza chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad.
- Revisa los reportes de auditorías o logs cuando es advertido de anomalías.

El **encargado del mantenimiento** de los servidores determina qué logs se generan, qué eventos de seguridad se auditan y qué datos se recogen. Además se encarga de buscar nuevas herramientas que faciliten la auditoría.

6.3 AUDITORÍAS DE CONTROL DE ACCESO

6.3.1 CONTROL DE ACCESO A LOGS

Los logs se almacenan en el servidor de aplicaciones y en el de Internet, por lo que cuentan con el control de acceso físico al servidor, pero no hay ningún control de **acceso lógico a las carpetas** donde están almacenados. Éstos pueden ser accedidos desde cualquier máquina conectada a la red, conociendo la clave de administrador, a través del WebMin.

6.3.2 CONTROL DE ACCESO A INTERNET

Con respecto a las **conexiones a Internet**, existen registros con información sobre el número IP de la máquina conectada y la dirección de las páginas visitadas.

6.3.3 MODIFICACIÓN DE DATOS

El sistema operativo genera logs indicando qué datos se han modificado y en que momento, pero estos no son analizados por los administradores, solo se almacenan y se borran periódicamente. Existen logs sobre la mayoría de los **movimientos de los usuarios** en el sistema de la empresa, generados por el AcuServer, en lo que se refiere a acceso a archivos abiertos y modificados. Esta aplicación genera reportes sobre qué máquina se logea, la hora a la que ingresa, a qué archivos accede y la hora a la que se desconecta, pero no contiene datos sobre el usuario que se está conectando.

Se piensa desarrollar un **sistema de control de cambios** para los datos, de manera que cada archivo del sistema de archivos indexados se asocie a una tabla de auditoría con las altas, bajas, modificaciones y consultas realizadas en los datos; pero este sistema todavía no está operativo.

6.3.4 CAMBIO DE PASSWORD

No se generan logs cuando un usuario modifica su password, no se guardan las contraseñas anteriores (para evitar la repetición), no se determina que aplicación se ha usado para realizar el cambio ni, en caso que el cambio resulte fallido, el motivo del fallo.

6.3.5 LOGS DEL ADMINISTRADOR

No se chequean periódicamente para verificar que sean válidos, que no haya habido intrusiones, o que no se registren ningún tipo de problemas.

6.3.6 LOGIN FALLIDO

Tanto el login exitoso como el fallido generan un log en el AcuServer. El log generado no especifica el motivo del fallo, como por ejemplo si falló porque el password estaba mal, porque el usuario no existe, o porque tuvo dos intentos errados. Solo se identifica que hubo un error de conexión.

6.3.7 LOCKEO DE UN USUARIO

La única manera de lockear un usuario es porque ingresó mal el password dos veces consecutivas, pero no se genera un registro de este evento, sino que el usuario debe avisar al administrador del sistema.

6.3.8 PERFIL DE USUARIO

Con los logs que existen en la empresa sería posible generar perfiles de los requerimientos de cada usuario, pero no se hacen estas tareas, los datos se encuentran en bruto sin analizar.

6.3.9 LOGS DE IMPRESIÓN

En la empresa no hay **impresoras** en red, por lo que las impresiones se ejecutan en impresoras locales a las PC's. No hay generación de logs cuando se requiere una impresión de algún dato suministrado por el sistema de la empresa.

6.4 AUDITORÍAS DE REDES

6.4.1 REPORTES DE CORREO

De los logs del mail no se calculan estadísticas, no se sacan **líneas de base** ni se grafican. El administrador solo los lee cuando supone que puede haber algún problema, a pedido de los usuarios por una supuesta falla en el servicio de mail. En el caso que se llene el espacio en disco de alguna cuenta, se envía un mail al root indicando el problema, pero no se emiten alarmas ni se generan logs.

El **SendMail** genera logs del tráfico de mails, aunque estos no se leen ni auditan. Estos logs se guardan durante 30 días, y se eliminan mediante la rotación de logs. En la oportunidad en que no se realizó la rotación correctamente, los logs del SendMail superaron los 2GB de datos, por lo que fue necesario que el administrador los borre manualmente.

En estos logs se almacena el cuerpo del mail completo, pero no se guardan los archivos adjuntos, solo es posible consultar si contenía o no archivos, y los nombres de los mismos.

No se generan **estadísticas** sobre qué departamento o usuario de la empresa utiliza más el servicio de mail, o si a algún usurario le llegan más mail que la cantidad promedio, pero en los logs figuran los datos del usuario que sería necesario para realizar dichos cálculos.

El **antivirus** (PC Cillin para Linux) genera logs con datos sobre el correo entrante y saliente, la hora de envío, el contenido del mail, asunto del mail, archivos adjuntos, reporte de virus de cada parte del mail, máquina destino y fuente y direcciones IP de estas máquinas. Estos reportes se almacenan durante 15 días. Además, existe una herramienta en el servidor de hosting que tiene detalles como los usuarios que están activos, los que están inactivos, cuanto espacio tiene usado cada usuario de mail, cuanto espacio hay libre, entre otros.

6.4.2 ESTADÍSTICAS DE RED

Existen, como citamos anteriormente, gráficos sobre el **tráfico en la red**, proporcionados por el programa de administración de red denominado Monitor. Pero no existen datos detallados sobre el consumo de ancho de banda por terminal ni por sector de la empresa, de manera de tener la posibilidad de individualizar cuál de las terminales usa más tráfico de red o en qué parte de la línea el tráfico es más intenso. Solo existen datos indicando la cantidad de bytes entrantes y salientes, pero no se detalla desde dónde se generan, ni con qué aplicación (mail, datos, aplicaciones, mensajes, Internet, etc.).

El **Proxy** utilizado (Squid) genera logs muy detallados, con datos sobre las páginas visitadas, el usuario, los horarios de entrada y salida, aunque no se generan reportes

con datos relativos a los archivos descargados desde Internet. Esta aplicación tiene la capacidad de generar gráficos con los logs, aunque no se utilizan.

Tampoco existen reportes sobre las **aplicaciones** utilizadas por cada usuario, ni las prioridades de estas aplicaciones con el fin de discriminar qué cantidad de tráfico genera cada aplicación. Sería útil para ver qué aplicación usa más recursos, y restringir en el caso que sea necesario.

No hay datos estadísticos de los intentos de ataques. Cada vez que ocurre uno desde el exterior de la empresa el sistema operativo envía un mail al root advirtiéndolo de esta situación.

No se hace ningún seguimiento de los logs en busca de **cambios en las estadísticas** como un incremento en el uso de Internet, incremento en los ataques o la modificación en los permisos.

7- PLAN DE CONTINGENCIAS

OBJETIVO DE AUDITORÍA: basándose en el análisis de riesgos desarrollado en la presente auditoría¹, los auditores deberán determinar cuáles son los activos con mayor nivel de impacto y más vulnerables de la empresa, con el fin de asesorar en el futuro un posible desarrollo de un plan de contingencia y de continuidad de servicios críticos, teniendo en cuenta los riesgos más probables y considerando las distintas soluciones posibles.

7.1 PLAN DE ADMINISTRACIÓN DE INCIDENTES

En la empresa no hay **planes formales** para la administración de incidentes, como planes de contingencia, de recuperación de desastres o de reducción de riesgos. Pero se dispone de backups de hardware y de servicios que prestan terceros para garantizar la continuidad de los servicios ante alguna contingencia. Estos terceros son una aseguradora y personal técnico especializado de mantenimiento externo.

Actualmente las emergencias son administradas por el encargado del centro de cómputos aunque no hay **responsabilidades formales** asignadas a los empleados. Existen tres personas que generalmente se distribuyen las tareas a medida que se presentan, y esto se realiza sin ninguna planificación.

7.2 BACKUP DE EQUIPAMIENTO

7.2.1 EQUIPAMIENTO DE LOS SERVIDORES

En **cada servidor** existen 3 discos duros con tecnología SCSI, donde cada uno de ellos tiene una capacidad de 18 GB. Uno de ellos trabaja como disco raíz, un segundo disco funciona como disco espejo del primero, y el tercer disco es de respaldo (este disco no contiene datos).

Son discos tipo “hot swap”, es decir que pueden reemplazarse mutuamente sin la necesidad de reiniciar el equipo. Con esta metodología pueden caerse hasta dos discos simultáneamente sin inconvenientes para el funcionamiento del sistema, y al reponer el disco que falta el servidor actualiza los datos automáticamente.

El **servidor de Internet**, ante una contingencia, puede funcionar como servidor de aplicaciones, ya que sus estructuras físicas son idénticas. De esta manera es posible cambiar los discos duros y el servidor de Internet se convierte en el servidor de aplicaciones. Además el servidor de Internet posee un backup de los datos del servidor de aplicaciones exportados por el SAMBA. Esta copia se actualiza con un proceso del sistema operativo cada 1 hora. Este proceso no funciona en sentido inverso, es decir que el servidor de Internet no está respaldado en el servidor de aplicaciones.

En el caso de una rotura de disco, solo es necesario sacar el disco roto del servidor y cambiarlo por el disco espejado correspondiente, ya que existen 2 discos iguales.

¹ Anexo I - Análisis de Riesgo

Se realizaron **pruebas** de esta configuración cuando se instaló el sistema operativo por primera vez. Estas pruebas demoraron 4 minutos y sus resultados fueron satisfactorios; después de éstas no se realizaron pruebas posteriores.

7.2.2 *EQUIPAMIENTO DE RED*

No hay **backup de hardware** debido a que esta red se encuentra asegurada, de manera tal que ante una contingencia física en algún equipo, la aseguradora garantiza la reparación o el reemplazo del dispositivo. Se optó por esta alternativa basándose en un análisis costo / beneficio que abarcó la totalidad de la infraestructura de la empresa, teniendo en cuenta los costos de implementación, mantenimiento, entrenamiento técnico del personal, y de restauración en caso de una emergencia.

7.2.3 *CPD ALTERNATIVO*

Los datos de la empresa y los dos servidores se encuentran en la misma habitación física, ya que no hay ningún centro de procesamiento de datos alternativo, porque no se justifica esta inversión.

7.3 **ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES**

7.3.1 *ESTRATEGIA PREACTIVA*

- **Constitución del grupo de desarrollo del plan**

En el caso en que se genere un plan de emergencia, el responsable del desarrollo e implementación del plan debería ser el administrador del centro de cómputos. En cada área de la empresa existe un líder que sería el Jefe o Encargado del área, debido a la responsabilidad que tiene en el grupo. Éste debería sugerir al Administrador las medidas de seguridad a implementar en el plan que requiera su sector.

- **Sistemas de información**

No hay ningún responsable por la información de cada departamento, cada usuario es responsable de sus datos. Tampoco están identificados todos los sistemas de información, a modo de inventario, contemplando sus características principales, de manera que no es posible asignarles prioridades y así determinar qué sistema es más importante a la hora de recuperar la operatividad luego de un desastre.

- **Equipos de cómputos**

No hay inventarios de los equipos de hardware ni de software, ni documentación con respecto a los equipos de la red física, de manera que no se les asigna un orden de importancia. Pero en el caso de necesitar restaurar las PC's primero se deben asegurar las del sector de ventas de las sucursales, las de la Gerencia, las del área de Sistemas, y las de Contaduría.

- **Establecimiento del plan de acción**

En caso de una emergencia sería necesario desarrollar un plan de acción, en el cual el servidor de aplicaciones sería el activo con mayor importancia al momento de continuar con las tareas, debido a que en él se encuentran los sistemas propios de la empresa y sus datos. Todos estos sistemas tienen la

misma prioridad en el caso de una contingencia, aunque existe una alternativa manual para el desarrollo de todas las actividades.

Los **activos** más críticos a proteger serían:

- Datos:
 - o Base de datos, datos compartidos por el Samba, documentación del centro de cómputos y de los sistemas.
 - o Programas fuentes y ejecutables del sistema de la empresa.
- Hardware:
 - o Servidores, switch central y switches de las sucursales, equipos de radio, equipamiento del centro de cómputos y canales de fibra óptica.
 - o Soporte físico de backups.

▪ **Definición de niveles críticos de servicio**

Los servicios más críticos de la empresa son la atención al público, el taller y el departamento de Contaduría. Por posibles contingencias con la red, en el caso que se demore o se discontinúe el servicio, disponen de consultas con las listas de precios físicamente ubicadas en las máquinas de atención al público y el taller; y para el área de contaduría y demás sectores existen procedimientos manuales para todas las actividades de la empresa.

Un ejemplo de contingencias que ocurre en el sector de ventas sería que actualmente existen problemas con los archivos temporales que bloquean el acceso a programas del AcuServer. Para mitigar este riesgo es necesario que los usuarios no dejen abiertas las aplicaciones o las cierren correctamente. Para eliminar estos archivos los usuarios tienen una aplicación en los escritorios de sus PC's. En esta situación el riesgo está controlado, pero no hay documentación formal que determine los responsables a cargo de esta contingencia, las aplicaciones y equipos a los que afecta este problema.

No se hacen simulaciones de siniestros para el entrenamiento del personal, solo en el momento de instalar los servidores se hizo un simulacro de sustitución de discos, de manera de comprobar su funcionamiento.

7.3.2 *ESTRATEGIA DE ACCIÓN*

No hay funciones claras que debe realizar el personal durante una contingencia, ya que no hay responsabilidades asignadas. Las situaciones se resuelven a medida que transcurren, sin la implementación de una norma a seguir formalmente documentada.

7.3.3 *ESTRATEGIA REACTIVA*

▪ **Evaluación de daños**

Una vez que ha ocurrido una contingencia, los encargados de evaluar los daños son los responsables de cada una de las áreas de la empresa, reportando a un miembro de la Gerencia que actúa como coordinador, el cual evalúa los resultados obtenidos al aplicar la solución.

- **Ejecución de actividades**

Una vez ocurrido el siniestro, el administrador del sistema trata de llevar el sistema informático de la empresa a su funcionamiento normal, realizando las actividades de recuperación sin respaldarse en un plan o manual formal de procedimientos.

- **Retroalimentación del Plan de Acción**

No hay un plan de acción a seguir, pero se toman acciones correctivas una vez que ha ocurrido una emergencia, de manera de evitar la misma contingencia en el futuro y mejorar la eficacia de las directivas. Una vez que han ocurrido los desastres no se genera documentación con respecto a las modificaciones implementadas ni a las acciones correctivas que se llevaron a cabo.

INFORME DE DEBILIDADES Y RECOMENDACIONES

En este informe se presentan las debilidades halladas y las sugerencias que pueden implementarse ante la ausencia o la falla en los controles para el tratamiento de la seguridad de la información. Estas recomendaciones están avaladas por las normativas arriba enumeradas.

1- SEGURIDAD LÓGICA

1.1 IDENTIFICACIÓN – ID’S

- ❖ **Debilidad:** durante el proceso de auditoría pudimos comprobar que los ID’s de los usuarios en el sistema, que deberían corresponder a sus propios números de legajo, no existían como tales, sino que eran números al azar generados por el administrador del sistema.

Efectos: esto genera un inconveniente en el usuario al momento de memorizar su número de acceso al sistema, provoca errores de inconsistencia con la base de datos de recursos humanos y dificulta la manipulación de datos de usuarios en el sistema.

Recomendación: se podría comprobar con la tabla de personal que el número legajo existe, o bien se recomienda implementar otro sistema de identificación de usuarios, como puede serlo el nombre de dominio de la cuenta de mail (Ej. para el dominio jperez@laempresa.com utilizar jperez como ID de usuario).

- ❖ **Debilidad:** durante la inspección de auditoría verificamos que algunos usuarios no tenían asignado un grupo de la empresa, dejando este campo vacío en la base de datos.

Efectos: esta situación genera problemas en la identificación del sector de la empresa al que pertenecen los usuarios ya que en el caso de que el campo esté vacío, el sistema considera que el usuario no tiene restricciones y le da acceso completo a los datos. Esto genera una falla en la confidencialidad y posible divulgación de datos.

Recomendación: deberá tenerse en cuenta que no puede existir el valor NULL en el campo “grupo” de los datos de usuario, ya que de él dependen los futuros permisos que se le asignen.

- ❖ **Debilidad:** existen usuarios en el sistema para los cuales no estaba asignada una fecha de expiración del password.

Efectos: el principal problema de esta situación consiste en que el usuario no es obligado, en ningún momento, a modificar su clave de acceso, de manera que se facilita su revelación o robo.

Recomendación: el sistema no debe permitir que el campo donde se ingresa la fecha de expiación del password sea nulo, ya que de él depende el requerimiento de cambio de contraseña.

- ❖ **Debilidad:** cuando un usuario ingresa dos veces mal la contraseña de ingreso, éste usuario es bloqueado por el sistema y el administrador debe desbloquearlo.

Efectos: es posible que el usuario, al modificar varias veces su contraseña, olvide o confunda los passwords, de manera que puede ingresar erróneamente

la clave varias veces y bloquearse su cuenta en repetidas oportunidades, lo que genera molestias en el administrador y en el propio usuario.

Recomendación: suponemos que el sistema puede resultar más eficiente si el número de intentos fallidos se incrementa a cinco, así se generarían menos bloqueos de usuarios y menores interrupciones a las tareas del administrador.

- ❖ **Debilidad:** no hay en la empresa un procedimiento formal para efectuar las bajas de los empleados del sistema.

Efectos: es posible que los empleados próximos a desvincularse de la empresa (cualquiera sea el motivo de esta situación) emprendan acciones de vandalismo o sabotaje, por rechazo o insatisfacción con esta decisión, o bien para beneficios personales.

Recomendación: sería conveniente que el área de recursos humanos de aviso al administrador del sistema o Jefe del centro de cómputos, con un período de tiempo previo al despido, de esta manera es posible llevar a cabo una política de desvinculación del personal, a través de la cuál se quitan permisos al usuario en forma periódica. Con esto se disminuye el riesgo de vandalismo por insatisfacción con la decisión de la Empresa

- ❖ **Debilidad:** no se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.

Efectos: es posible que, por error, negligencia, fraude o algún otro motivo, la cuenta o los permisos de algún usuario sean modificados, permitiendo que usuarios no habilitados accedan a datos que no le están permitidos.

Recomendación: Periódicamente sería conveniente controlar las cuentas de usuarios, viendo que:

- Estén activas solo las cuentas necesarias.
- No se han creado ni borrado cuentas.
- Los datos del usuario son consistentes.
- Los permisos que le corresponden son los que tiene asignados.
- Los passwords no están expirados y han sido cambiados periódicamente.

- ❖ **Debilidad:** no existe en el sistema una lista de control de acceso, esto imposibilita relacionar los usuarios con los datos que les es posible acceder, y qué permisos tienen sobre estos datos (lectura, escritura, modificación, borrado.)

Efectos: la ausencia de esta relación dificulta la trazabilidad de las acciones, de manera que resulta complicado identificar los permisos de los usuarios con respecto a los datos, archivos y carpetas del sistema, en el caso que sea necesaria una auditoría o revisión de la actividad particular de un usuario.

Recomendación: recomendamos la generación de una lista de control de acceso donde se identifiquen a todos los usuarios habilitados en el sistema, los datos a los que pueden acceder y los tipos de permisos que los usuarios poseen

sobre los mismos. Con esta herramienta sería posible personalizar perfiles de usuarios, que no dependan exclusivamente del grupo al que pertenecen. Esta lista de control de acceso debería almacenarse en el servidor de aplicaciones cifrada, de manera que los permisos de los usuarios no sean revelados a personas no autorizadas, y así evitar la posibilidad de una modificación no autorizada.

Con esta configuración puede utilizarse una herramienta que genere automáticamente los accesos directos a los programas de acuerdo a cada usuario en particular al momento del logeo.

- ❖ **Debilidad:** los accesos directos a los que el usuario tiene acceso los genera el administrador del sistema a mano, una vez que el usuario fue dado de alta.

Efectos: esta práctica puede resultar poco práctica e ineficiente, debido a que una posible equivocación del administrador del sistema implicaría que usuarios no autorizados accedan a menús y datos que no le están permitidos. Además podría ocurrir que otra persona genere estos accesos directos (de la misma manera que lo hace el administrador), con la misma consecuencia descrita anteriormente.

Recomendación: es recomendable que, una vez que el usuario se ha logeado al sistema, éste cree (o haga visibles) los accesos directos que son necesarios de forma automática, de acuerdo al perfil que le corresponde.

- ❖ **Debilidad:** no se tiene en cuenta ninguna restricción horaria en el momento de permitir a un usuario el logeo al sistema.

Efectos: esta debilidad puede permitir que un usuario no autorizado intente ingresar al sistema en horario no laboral (desde el exterior de la empresa, por ejemplo), condición que se ve agravada por el hecho que los servidores no se apagan sino que permanecen prendidos las 24 horas del día.

Recomendación: debería discriminarse el horario en que puede ser utilizado el sistema informático de la empresa, de manera que:

- las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan (debido a que diferentes grupos pueden tener diferentes horarios).
- durante las vacaciones o licencias las cuentas de usuarios deben desactivarse.
- en días feriados las cuentas de usuarios administrativos, a excepción de los del Grupo Ventas, deben permanecer desactivados.

- ❖ **Debilidad:** no se tiene en cuenta ninguna restricción con respecto al equipo desde donde se logea cada usuario.

Efectos: al no controlar el dispositivo físico desde donde los usuarios acceden a la red, puede ocurrir que alguna persona no autorizada tenga acceso a un equipo que no le corresponde, permitiéndosele ver información para la que no tiene autorización.

Recomendación: se deberá tener en cuenta la localización del PC que se intenta logear, para así poder relacionar cada usuario con su propia PC, o con su propio

grupo de trabajo, de manera que un usuario de ventas solo podrá logearse en alguna de las PC's del departamento de ventas y un gerente solo pueda logearse en su propia PC.

- ❖ **Debilidad:** aunque el usuario permanezca un largo período de tiempo sin actividad el sistema no ejecuta ninguna acción; los administradores solo advierten a los usuarios sobre la necesidad de no dejar las máquinas logeadas e inactivas.

Esta situación pudo comprobarse también en los servidores, donde el administrador está logeado en el sistema permanentemente.

Efectos: el peligro en el que se incurre con esta debilidad radica en la posibilidad de que un usuario autorizado se logee en el sistema y abandone su puesto de trabajo. Si otro usuario no autorizado tiene acceso físico a esta PC, éste último también tendrá acceso a datos que le están prohibidos. Esta situación se ve agravada si los equipos a los que se hace referencia son los servidores de la empresa, debido a que no solo se tiene acceso a datos críticos sino también a opciones de configuración de los sistemas.

Recomendación: si el sistema permanece ocioso durante cinco minutos, el programa debería encargarse de deslogear al usuario del sistema, borrar la pantalla. Cuando el usuario regrese, se debería solicitar nombre de usuario y contraseña nuevamente.

Además, sería conveniente que las PC's utilicen algún protector de pantalla con contraseña.

Estas recomendaciones se deben tener presente en la administración de los servidores.

- ❖ **Debilidad:** las cuentas de usuarios no pasan a un estado de suspensión, aunque permanezcan varios días sin actividad.

Efectos: puede ocurrir que alguna persona no autorizada tenga acceso a una cuenta de usuario que no le corresponde, permitiéndosele ver información para la que no tiene autorización.

Recomendación: Sería conveniente que el sistema, en forma automática, suspenda la cuenta de un usuario que no se logea durante cinco días. Además, si un usuario se va de vacaciones, o solicita una licencia, su cuenta debería inhabilitarse hasta su regreso.

- ❖ **Debilidad:** los servidores permanecen logeados con el usuario root durante las 24 horas del día. De esta manera la seguridad de los datos de la empresa que residen en el servidor solo dependerá del acceso físico al equipo.

Efectos: debido a que no hay controles lógicos, cualquier persona que consiga ingresar al centro de cómputos podría acceder a los datos y a la configuración de los servidores.

Recomendación: el administrador solo debería utilizar este usuario del sistema en caso que fuera necesario realizar alguna tarea que así lo requiera. Para las demás actividades debería contar con otro usuario, con menos privilegios y por lo tanto menos riesgoso.

- ❖ **Debilidad:** los usuarios del departamento de ventas no son identificados en forma personal, sino que todos usan el mismo nombre y contraseña de ingreso al sistema informático.

Efectos: ante un posible error, fraude o robo de algún dato de este sistema, sería imposible identificar qué persona accedió a la información, en qué momento lo hizo, etc., es decir que no pueden rastrearse las acciones de los usuarios en el sistema.

Recomendación: todos los usuarios deben poder identificarse en el sistema de manera única para así poder seguirle los rastros a través de los logs de auditoría que se generen.

- ❖ **Debilidad:** los usuarios del sistema pueden tener abiertos, al mismo tiempo, todos los menús a los que están autorizados, y **varias sesiones** del mismo menú. No se hacen restricciones en cuanto a la cantidad de sesiones que los usuarios pueden utilizar.

Efectos: al abrir varias sesiones al mismo tiempo, existe la posibilidad que un usuario use la cuenta de otro para ingresar a los datos, complicando así la trazabilidad de las acciones de los usuarios. Además de no ser necesaria esta posibilidad de tener varias sesiones abiertas, ya que con una sola sesión el usuario dispone de toda la información que necesita.

Recomendación: consideramos necesario que solamente se pueda abrir una sesión de cada aplicación del sistema informático de la empresa con el mismo nombre de usuario, y así no se podrán abrir dos sesiones del mismo menú en diferentes terminales, posibilitando esto el control sobre las actividades desarrolladas por los usuarios, a través de logs donde se registre el usuario, la terminal en la que está logeado y la aplicación que está usando. De esta forma se podrá identificar si en algún caso hay intentos de intrusión, o si simplemente se ha dejado logeada una terminal por error.

- ❖ **Debilidad:** no se eliminan los usuarios que vienen por default en el sistema operativo, como las cuentas Guest del LINUX, estas cuentas permanecen en el sistema sin que ningún usuario las utilice.

Efectos: en el caso que una persona no autorizada conozca la existencia de estas cuentas puede llegar a utilizarlas para tener acceso al sistema operativo del servidor.

Recomendación: sería conveniente eliminar estos tipos de usuarios, no solo los que trae Linux por default sino también los usuarios de Windows XP. No deben existir en el sistema más usuarios que los necesarios para la empresa.

- ❖ **Debilidad:** en la empresa hay tres personas con el mismo perfil de administrador, cada una de ellas tiene una cuenta diferente con un password determinado, pero a fines prácticos, los tres conocen todas los passwords de las demás cuentas, ya que no hay una clara definición de tareas.

Efectos: con este esquema de acceso se imposibilita rastrear las acciones de cada uno de los administradores en el sistema operativo de los servidores, así no pueden asignarse responsabilidades individuales ante un posible error.

Recomendación: no es conveniente que varias personas accedan a la misma cuenta de usuario. Por este motivo sugerimos que no se revelen las contraseñas personales, de manera de diferenciar a los tres administradores del sistema.

Debería existir un administrador total del sistema (root); y sugerimos que éste usuario esté en estado de inhabilitación, cuyo nombre de usuario y contraseña se encuentran guardados en un sobre cerrado.

El segundo en responsabilidad (un súper-usuario) tiene permisos iguales al anterior, con una restricción que lo imposibilita de borrar el usuario root.

Además existiría una tercera cuenta de administrador, que tenga a su cargo un grupo de tareas de menor importancia y cotidianas del administrador.

En caso de que falte el administrador (el súper-usuario) por algún motivo, y el segundo requiera alguna tarea de mayor responsabilidad, este deberá recurrir a la cuenta de root, buscando los datos en el sobre. Una vez que esta cuenta ha sido usada, y el administrador retorna a sus tareas, deberá cambiar la contraseña de esta cuenta y guardarla en un nuevo sobre cerrado.

- ❖ **Debilidad:** el administrador puede logearse desde cualquier terminal de la empresa, además de tener la posibilidad de abrir varias sesiones del sistema al mismo tiempo.

Efectos: esta situación resulta riesgosa ya que el administrador podría dejar una terminal logeada con esta cuenta, lo que permitiría a cualquier usuario que acceda a esta terminal con perfil de administrador realizar cambios en los perfiles de usuarios y sus permisos, entre otras actividades.

Recomendación: Para evitar esta contingencia, el administrador debe poder logearse solamente desde ciertas terminales, las que se encuentren en el centro de cómputos, y en una terminal específica y habilitada por cada sucursal. Para poder realizar el mantenimiento del resto de las PC's sugerimos que se cree una cuenta *mantenimiento* donde el administrador tenga permisos que le permitan realizar sus tareas habituales.

- ❖ **Debilidad:** el mantenimiento técnico especializado externo utiliza la misma cuenta de administrador para hacer modificaciones en los sistemas operativos de los servidores vía Internet, y una vez finalizado el mantenimiento el administrador del sistema no cambia la contraseña.

Efectos: esta situación resulta inadmisibles, debido a que existe otra persona, ajena a la organización, que conoce la contraseña del administrador del sistema, de manera que se aumenta el riesgo de intrusión a los sistemas y divulgación o robo de datos.

Si esta contraseña es utilizada a través de Internet, el riesgo se hace todavía más grande debido a la posibilidad de escuchas o interceptaciones en la comunicación, que podrían resultar en el robo del password.

Recomendación: sugerimos que, para resolver esta situación, se cree una nueva cuenta de usuario para realizar el mantenimiento externo, con los permisos necesarios para dicha tarea.

Una vez finalizado el mantenimiento, el administrador del sistema podría modificar la contraseña, de manera de evitar entradas no autorizadas. De esta

manera, cada vez que sea necesario realizar un mantenimiento, el administrador del sistema debería proporcionar el nuevo password al personal externo.

Esta cuenta, por la peligrosidad que enviste, debería ser chequeada periódicamente por el administrador, comprobando las tareas que desde allí se realizan.

1.2 AUTENTICACIÓN

- ❖ **Debilidad:** una vez que algún usuario ha logrado logearse en el sistema se muestra solamente el nombre de usuario en la pantalla.

Efectos: si en una cuenta de usuario hubo un intento de intrusión, o se logró la intrusión, el usuario nunca se percatará de este ataque, como así tampoco lo hará el administrador del sistema.

Recomendación: en una pantalla intermedia se podría indicar, para un control personal del usuario, la siguiente información:

- Nombre de usuario
- Fecha y hora de la última conexión
- Localización de la última conexión (Ej. número de terminal)
- Intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.

Esto es posible ya que toda esta información está guardada en los logs del sistema, pero no se los analiza. De esta manera el usuario puede llevar un control sobre sus conexiones.

- ❖ **Debilidad:** la aplicación para administración de cuentas de usuarios del sistema informático, puede ejecutarse desde cualquiera de las terminales de la empresa, a través de la línea de comandos de Windows.

Efectos: es posible que el administrador olvide deslogearse del sistema, dejando la aplicación abierta en cualquier máquina. Además en la línea de comandos de Windows queda un historial de los últimos comandos ejecutados, de manera que si algún usuario identifica la contraseña de acceso del administrador, podría ingresar al sistema de modificación de perfiles.

Recomendación: sería conveniente que esta aplicación solo se pudiese ejecutar en las máquinas del centro de cómputos (específicamente las que son de uso cotidiano del administrador de sistema), sabiendo la extrema sensibilidad de los datos que administra.

- ❖ **Debilidad:** los datos de autenticación son almacenados y transmitidos sin ningún cifrado.

Efectos: al no existir encriptación en los datos de autenticación, puede ocurrir que alguien acceda al archivo de passwords del sistema de la empresa, y disponga de acceso a todas las cuentas de usuarios existentes, con todos los permisos posibles, y de esta forma no tendría ninguna restricción en el acceso a los menús del sistema.

Al no cifrar durante la transmisión de datos, puede ocurrir que alguien intercepte el canal de comunicaciones, consiguiendo las contraseñas y nombres de usuarios en texto plano.

Recomendación: el archivo con los datos de usuarios del sistema debería almacenarse en un formato no legible, es decir encriptado, y almacenado en el servidor de aplicaciones en una carpeta protegida por una contraseña gestionada por el administrador del centro de cómputos. Además, sería conveniente que los datos de autenticación viajen encriptados a través de la red, durante toda la transmisión.

El archivo que almacena los passwords de los usuarios no debería poder modificarse, sino solamente a través de la aplicación de gestión de cuentas. Otra opción que puede adoptarse es no desencriptar los passwords para su comparación cuando se realiza un logeo, sino directamente comparar los passwords encriptados en el archivo contra los ingresados por el usuario.

- ❖ **Debilidad:** en cuanto a los mensajes externos desde la Gerencia hacia las fábricas, que pueden revestir mayor importancia, podría utilizarse un sistema de firma digital.

Efectos: se reduciría la posibilidad de un ataque de Ingeniería Social, así como también contar con el beneficio del no repudio.

Recomendación: podría tenerse en cuenta la posibilidad de implementar un sistema de firmas digitales para así identificar fehacientemente al emisor; aunque esta recomendación solo sería conveniente en ciertos mensajes, aquellos que la Gerencia considere de mayor importancia.

1.3 PASSWORD

- ❖ **Debilidad:** los passwords no tienen una longitud mínima requerida por el sistema, solo tienen que respetar un largo máximo de 10 caracteres alfanuméricos.

Efectos: al no haber una longitud mínima, los usuarios pueden poner un password de un solo carácter (por ejemplo un espacio, o un solo número) lo que las hace fácilmente descifrables, generando vulnerabilidades importantes en los datos que éstas protegen.

Recomendación: es necesario que exista un número mínimo de caracteres (6) que conforman el password. Además puede requerirse que dicha contraseña está compuesta de datos alfanuméricos, numéricos y caracteres especiales.

- ❖ **Debilidad:** no se realiza ningún control sobre las cuentas de los usuarios, para comprobar que cambian el password asignado por primera vez.

Efectos: de ser así, el usuario permanecerá con un password fácilmente descifrable, facilitando la divulgación de esta contraseña y el robo de datos.

Recomendación: es necesario que, cuando el usuario se logea por primera vez al sistema, éste lo obligue a modificar su contraseña, impidiéndole el acceso hasta que éste procedimiento no haya terminado con éxito. Esto se logra

ingresando la fecha de expiración del password como vencida en el momento de realizar el alta de un nuevo usuario.

- ❖ **Debilidad:** pudimos ver que el password de un usuario era un número fácilmente imaginable.

Efectos: al ingresar al sistema con un password fácilmente descifrable, es posible que los demás usuarios lo obtengan y accedan a datos que les están prohibidos.

Recomendación: Deberán considerarse herramientas para controlar que el password no sea fácil de descifrar, como puede ser realizar comparaciones contra una lista de palabras reservadas, por ejemplo el nombre de la empresa, el nombre de cuenta del usuario, números o letras repetitivas, entre otras. Una buena forma de crear un buen password es elegir una frase fácil de recordar y luego usar las primeras letras de sus palabras, por ejemplo: "Nos los representantes del pueblo de la Nación Argentina" puede formar el password "NLRDPLNA".

- ❖ **Debilidad:** durante la auditoría pudimos comprobar que los password de acceso a los root de ambos servidores Linux son iguales.

Efectos: con una situación como esta se incrementa el riesgo de divulgación y robo de datos debido a que, si alguien tiene acceso al password del servidor de Internet, también podrá acceder al servidor de aplicaciones con los permisos del administrador.

Recomendación: sugerimos que los passwords sean diferentes en ambos servidores, y que sean modificados con mayor frecuencia que los passwords de los usuarios.

- ❖ **Debilidad:** no se controla si el usuario cambia su contraseña ingresando siempre el mismo password, simulando cambiarlo, pero este ingresa nuevamente la clave que ha estado usando siempre.

Efectos: las contraseñas que no se modifican por largos periodos de tiempo corren el riesgo de ser descubiertas, debido a que seguramente habrá más oportunidades de descifrarlas.

Recomendación: deberá controlarse que el usuario ingrese una clave nueva cada vez que la modifique, así como que las últimas 5 claves no se repitan. Esto puede hacerse utilizando una base de datos donde se acumulen las últimas cinco claves que ha empleado cada usuario.

- ❖ **Debilidad:** generalmente, los password no son actualizadas por los usuarios, permaneciendo iguales por largos periodos de tiempo, ya que tienen un plazo de expiración de 1 año.

Efectos: las contraseñas que no se modifican por largos periodos de tiempo corren el riesgo de ser descubiertas por más usuarios, debido a que seguramente habrá más oportunidades de descifrarlas.

Recomendación: consideramos que el período de vigencia del password no debería ser tan largo, suponemos que sería conveniente utilizar uno de 4 meses.

- ❖ **Debilidad:** en ambos casos, cuando un usuario se olvida su contraseña o es bloqueado por el sistema, recurre al administrador, el cual lee el password del usuario (en el sistema de gestión de cuentas de usuario), recordándoselo. Pero en ningún momento se lo intima a modificar el password revelado.

Efectos: en esta situación el administrador del sistema conoce el password del usuario, lo que genera divulgación de información innecesaria. Esto se agrava cuando ocurre el mismo suceso varias veces, de manera que el administrador conocerá el patrón de contraseñas utilizado por el usuario.

Recomendación: para resolver esto el administrador modificará la fecha de expiración del password, obligando así al usuario a cambiar su contraseña en el momento del logeo. La aplicación, en ningún momento, revelará la contraseña del usuario al administrador.

1.4 SEGREGACIÓN DE FUNCIONES:

- ❖ **Debilidad:** no se implementa ningún régimen de separación de tareas ni tampoco un sistema de rotación de personal.

Efectos: si un usuario tiene la capacidad (o los permisos) para realizar una tarea completa, pueden cometerse errores o fraude, sin que la irregularidad sea advertida.

Al no haber una rotación de personal, es más difícil controlar la productividad del empleado, evitar posibles fraudes en el desempeño de sus funciones, así como el reemplazo del empleado en caso de su ausencia.

Recomendación: sería recomendable implementar un régimen de separación de tareas, para que un usuario no pueda realizar el ciclo de vida completo de una operación, y necesite de la intervención de otros empleados para poder concretarla, de manera que para poder realizar un fraude es necesaria la participación de más de un empleado, y se agrega un control para evitar posibles errores. Para esto será necesario restringir permisos a los usuarios.

Sería bueno tener en cuenta otro control, como la rotación de personal para controlar el desempeño que los empleados han tenido durante un período de tiempo. Además sirve para tener una persona capacitada de respaldo, en caso de necesitar una suplencia. Para poder llevar a cabo este control es necesario cambiar el usuario de grupo, modificándole sus permisos.

Estas tareas deberían estar a cargo del Departamento de Recursos Humanos, junto con los directivos de la empresa o con los responsables de cada área.

2- SEGURIDAD DE LAS COMUNICACIONES

2.1 TOPOLOGÍA DE RED

No se hallaron debilidades significativas con respecto a este tema.

2.2 CONEXIONES EXTERNAS

- ❖ **Debilidad:** la comunicación con el depósito de las fábricas se realiza vía módem, utilizando PC's que no tienen ningún control especial con respecto a la conexión a Internet. Esta comunicación se realiza sin la supervisión del firewall.

Efectos: una conexión a Internet sin resguardo es peligrosa, ya que aumenta los riesgos de intrusiones, virus, entre otros sucesos no deseables.

Recomendación: es conveniente que se utilice un firewall en las PC's que utilizan conexiones con módem, como las destinadas a la comunicación con las fábricas.

2.3 CONFIGURACIÓN LÓGICA DE RED

- ❖ **Debilidad:** no hay ninguna medida tomada para que un usuario pueda proteger sus datos.

Efectos: algún usuario puede acceder a datos de otro usuario que no deberían ser divulgados.

Recomendación: el Samba podría utilizarse para el control de perfiles. Con esta aplicación podría gestionarse la protección de las distintas carpetas, incluyendo las de backup de la página Web y de los usuarios, con controles de acceso más fuertes que los que están funcionando actualmente en la red; esto se logra declarando la aplicación como controladora de dominios, para que administre las carpetas, con una funcionalidad similar a la de Linux.

- ❖ **Debilidad:** existen carpetas compartidas en los servidores.

Efectos: al haber carpetas compartidas en el servidor pueden generarse intrusiones, robos de información o infecciones de virus.

Recomendación: no deberían existir carpetas compartidas en los servidores. Si es necesario grabar un CD aconsejamos que el usuario tenga una carpeta compartida en su PC con una contraseña que conocerá el administrador del sistema. En el momento de grabar el CD el usuario avisará al administrador, y éste copiará los datos al CD.

En cuanto a la carpeta compartida en el servidor de Internet, para actualizar el antivirus sugerimos que una vez que la actualización sea descargada de Internet se copie a otra máquina y desde allí se ejecute, o bien que desde Internet se baje directamente a otra máquina que no sea servidor.

2.4 MAIL

- ❖ **Debilidad:** al instalar los Outlook Express en las PC's no se modifican las opciones de configuración por default, es decir que la vista previa y los controles ActiveX y Scripts están habilitados.

Efectos: la vista previa de los mails y la ejecución de controles ActiveX y Scripts son riesgosas ya que facilitan la infección con virus que se ejecutan automáticamente.

Recomendación: es conveniente exigir normas respecto a la habilitación y deshabilitación de dichas características y la configuración mínima que debe poseer el Outlook Express en las PC's. Debe deshabilitarse la vista previa de los mensajes y prohibirse la ejecución de controles ActiveX y Scripts.

- ❖ **Debilidad:** no se asocia una cuenta de correo a un equipo específico.

Efectos: un usuario, conociendo el nombre de cuenta y la contraseña de la cuenta de correo de otro usuario, puede configurarla en su máquina y así enviar y leer mensajes ajenos.

Recomendación: a pesar de que ya existe el control que ningún usuario conoce su propia contraseña (ya que el administrador las crea y configura las cuentas guardando las contraseñas en las máquinas), puede ser útil que el SendMail asocie una cuenta de mail a una PC determinada, de manera que solo pueda usarse ese equipo en particular para leer o enviar mails desde esa cuenta.

- ❖ **Debilidad:** los empleados no usan el mail solamente para funciones laborales, sino también con fines personales. Actualmente no se controla el envío, pueden usarlo para cualquier fin. No se hace ningún control de que los usuarios se suscriban a listas de correo, no hay prohibiciones en este sentido.

Efectos: al utilizarse el servicio de mail indiscriminadamente se baja la performance de la red y se incrementa el riesgo de infección con virus.

Recomendación: debería controlarse que el servicio de mails se use solo para fines laborales, notificando a los usuarios de esta norma. Además sería conveniente hacerles advertencias con respecto a la suscripción a listas de correo.

Se podría calcular una estadística del nivel medio de tráfico de red generado por el correo electrónico, de manera que aquel usuario que sobrepase la media será evaluado para controlar si el uso que le da a este servicio es el correcto. De no ser así deberían tomarse las acciones correctivas respectivas.

- ❖ **Debilidad:** la cuenta de mail asignada por la fábrica FORD a un miembro de la gerencia se satura ocasionalmente.

Efectos: al no hacerse la descarga de mensajes, la casilla de bloquee impidiendo la comunicación con la fábrica.

Recomendación: sería conveniente administrar esta cuenta con el SendMail, bajando los mensajes al servidor.

- ❖ **Debilidad:** no están prohibidos los programas de chateo ni los de file sharing.
Efectos: estas aplicaciones encierran incrementan el riesgo de ingreso de virus, troyanos e intrusos al sistema.
Recomendación: deberían restringirse este tipo de aplicaciones, deshabilitando los servicios que utilizan (como el SOCKS en el caso del MSN).
- ❖ **Debilidad:** no se implementa un sistema de **prioridades** de mail.
Efectos: podrían mejorarse el envío de los mails a destinos como fábricas, bancos, y otros que merezcan mayor consideración.
Recomendación: el SendMail podría configurarse para que aquellos mensajes enviados por la gerencia o los que tienen ciertos destinatarios, como fábricas o bancos, se envíen con prioridad alta.
- ❖ **Debilidad:** no se generan copias de seguridad de los mensajes.
Efectos: en el caso de una contingencia con el servidor de Internet, los usuarios perderían los mails que no hayan leído hasta el momento del incidente.
Recomendación: podrían realizarse backups solo los mensajes con prioridad alta que se almacenan en el servidor de Internet.
- ❖ **Debilidad:** no se utilizan firmas digitales ni encriptación en el correo electrónico a nivel gerencial.
Efectos: sin la utilización de firma digital se puede correr el riesgo de ataques de ingeniería social.
Recomendación: podría utilizarse firma digital o encriptación para los mensajes con prioridad alta de las cuentas de correo de la Gerencia, y así poder realizar un envío seguro al transmitir documentos confidenciales. Por ejemplo, podrían comprimirse la información de los mensajes para que no viaje en texto plano y protegerla con una contraseña para mayor seguridad.

2.5 ANTIVIRUS

- ❖ **Debilidad:** los usuarios son los responsables de actualizar sus propios antivirus.
Efectos: al no tener implantada una conciencia de seguridad, los usuarios no actualizan las listas de virus.
Recomendación: la actualización de las listas de virus debería ser responsabilidad del administrador o de un empleado del área de sistemas designado por él. Éste debería, además, realizar chequeos aleatorios verificando que las listas de virus estén actualizadas y que se realicen periódicamente escaneos en busca de virus. Estas tareas deben realizarse tanto en las PC's como en los servidores.
- ❖ **Debilidad:** no hay procedimientos formales a seguir en caso de infección de virus.

Efectos: al no utilizar un procedimiento como guía, puede ocurrir que el virus no sea eliminado completamente del equipo y se contagie a través de la red interna, además de la posibilidad de pérdida de datos en los equipos infectados.

Recomendación: debería haber un procedimiento documentado a seguir para el caso que se encuentre un virus en el sistema. Sugerimos las siguientes actividades:

- Chequear el disco con el escaneo de virus para determinar si hay un virus, y qué virus es. Eliminar el virus.
- Cerrar los programas, apagar la máquina y bootear la computadora desde el disco de rescate del antivirus.
- Hacer un nuevo chequeo de virus en el disco duro.
- Chequear el resto de los dispositivos de datos (disqueteras, disco removibles, etc.), para saber de donde vino el virus.
- Tratar de determinar la fuente del virus. La persona que hizo llegar el virus debe ser informada.
- Avisar a todos los usuarios del sistema que hayan intercambiado datos con la computadora infectada.
- Si el virus borró o modificó algún dato, tratar de restaurarlo desde los backups y restaurar los programas involucrados.
- Hacer un nuevo escaneo del disco, buscando virus en los datos restaurados.

2.6 FIREWALL

❖ **Debilidad:** no se encuentran restringidos los servicios y protocolos que no son necesarios para el funcionamiento del sistema.

Efectos: esta situación genera una exposición innecesaria aumentando la probabilidad de ataques o intrusiones.

Recomendación: sería conveniente restringir más los accesos en el interior de la red. Los siguientes servicios no son necesarios y pueden desactivarse:

- Los RSHELL, RLOGUIN y REXECUTE pueden remplazarse con los servicios del SSH, por lo que no deben habilitarse.
- No deberían habilitarse el TALK y el FINGER ya que brindan gran cantidad de información a cualquier persona que la solicite.
- Los APPLETS y los SCRIPTS no deberían poder ejecutarse en el servidor, aunque sí en las PC's ya que se dificultaría mucho la navegación si éstos no estuvieran.
- El SYSTAT no es necesario salvo cuando se requiere hacer un mantenimiento. Sugerimos que se habilite on demand para esta práctica.
- El puerto 22 (de SSH) puede restringirse más habilitándolo on demand, y desde alguna PC determinada, la que se usará para el mantenimiento de la red. Se puede hacer lo mismo con el FTP, permitiendo su uso solo desde una PC en particular y en un horario determinado.
- Además sería conveniente deshabilitar definitivamente todos los servicios de puertos bajos no necesarios, que están habilitados desde el interior de la red, ya que no deberían utilizarse (como el TELNET).

Es conveniente la utilización de herramientas de monitoreo de red. Puede ser conveniente la utilización de una aplicación (TCP WRAPPER) que habilita el uso de servicios como el FTP y el TELNET pero restringe el acceso de acuerdo a ciertas reglas de restricción, en función de la dirección (o el usuario) de origen. Así es posible permitir solamente que se utilice, por ejemplo el FTP, desde una determinada PC y con el fin de conectarse a la fábrica de FORD, con un destino fijo.

- ❖ **Debilidad:** el número IP del servidor de Internet se publica en una página WEB de manera que el encargado de mantenimiento tenga acceso a él cuando lo necesite, para realizar el mantenimiento a través de acceso remoto.

Efectos: es muy probable que el número IP sea hallado en Internet por intrusos, ya que solo está protegido por una contraseña. Esto puede provocar el acceso externo de posibles atacantes.

Recomendación: esto puede resultar cómodo para el encargado de mantenimiento externo pero resulta peligroso exponer el número IP del servidor de la empresa. Sería conveniente que el personal de mantenimiento solicite el número IP actual al administrador del sistema, junto con la contraseña de la cuenta de mantenimiento externo. Con esta metodología, el administrador posee pleno conocimiento de todas las tareas que se llevan a cabo en los servidores.

2.7 ATAQUES DE RED

- ❖ **Debilidad:** en la empresa no disponen de herramientas destinadas exclusivamente para la detección de intrusos.

Efectos: al no haber un sistema de detección de intrusos instalado en los servidores, los atacantes tienen una barrera menos en el momento de ingresar a los datos de la empresa.

Recomendación: se debería usar algún sistema de detección de intrusos, estos deberían ser tolerantes al fallo, y ejecutarse con los mínimos recursos posibles. Ejemplos: OmniGuard, RealSecure, Cisco Secure IDS.

- ❖ **Debilidad:** el archivo que contiene los datos de los empleados de la empresa se encuentra almacenado en el servidor, en texto plano, sin ningún control de acceso.

Efectos: ante el acceso indebido a datos del servidor, se divulgarían los datos de los empleados de la empresa.

Recomendación: este archivo debería estar encriptado, y la carpeta donde se almacena debería tener una clave de acceso.

3- SEGURIDAD DE LAS APLICACIONES

3.1 SOFTWARE

No se hallaron debilidades significativas con respecto a este tema.

3.2 SEGURIDAD DE BASES DE DATOS

- ❖ **Debilidad:** las aplicaciones utilizan un sistema de archivos indexados, para almacenar los datos de la empresa.

Efectos: al usar archivos indexados no poseen las ventajas de un sistema de base de datos relacionales, una de las más importantes es que no es necesario trabajar con los índices, los que no son del todo confiables al momento de trabajar con grandes volúmenes de datos. Otra desventaja es no asegurar la inexistencia de redundancia, cuando en las bases de datos relacionales esta es una de los principales beneficios.

La principal desventaja de archivo secuencial indexada es que el rendimiento baja al crecer el archivo, aunque esto se puede evitar reorganizando el archivo, no es conveniente realizar esta operación frecuentemente.

Recomendación: consideramos necesario que este sistema de archivos sea reemplazado por uno de bases de datos relacionales. Recomendamos que esta migración se realice una vez que el sistema de la empresa este desarrollado, probado e instalado en su totalidad. Para desempeñar este cambio es conveniente generar un plan de migración, evaluando las posibles contingencias y los planes de prueba necesarios para comprobar el buen funcionamiento de la operación.

- ❖ **Debilidad:** los datos de la empresa no se clasifican formalmente según su importancia.

Efectos: la clasificación de la información de acuerdo a su importancia permite asignar distintos niveles de controles de seguridad según la confidencialidad que sea necesaria, la falta de clasificación en los datos puede provocar la mala asignación de controles de acceso, y así posibilitar la divulgación de información.

Recomendación: sería conveniente que se clasifique la información en la Empresa, de acuerdo a la importancia de la misma, es decir teniendo en cuenta la confidencialidad y la disponibilidad que debe tener. Se podrían definir tres niveles de información: crítica (la no-disponibilidad de esta información ocasiona un daño en los activos de la empresa), confidencial (en poder de personas no autorizadas compromete los intereses de la empresa) y pública (información de libre circulación). Esta clasificación ser documentada e informada a todo el personal de la organización, y deberá evaluarse y actualizarse periódicamente.

- ❖ **Debilidad:** a la información de la empresa no se les asigna un responsable.

Efectos: al no haber un responsable encargado de la información, puede ocurrir que no se asignen los controles de acceso correctos, o alguien que responda ante los directivos en el caso de una contingencia (como puede ser pérdida o divulgación de información).

Recomendación: se recomienda asignar a la información un responsable, que asegure la confidencialidad, disponibilidad e integridad de dicha información. En base a la clasificación enunciada anteriormente, el Administrador del Centro de Cómputos y el responsable de la información deberían definir los controles de acceso a los datos.

- ❖ **Debilidad:** no se realizan controles de acceso lógico al sistema de archivos indexados que conformarían la base de datos de la Empresa, así como al aplicativo que edita dichos archivos.

Efectos: debido a que la seguridad del sistema de archivos indexados se centra solamente en el acceso físico a los servidores, cualquier persona que tenga acceso al centro de cómputos, podría acceder a los datos utilizando el editor.

Recomendación: sugerimos algún tipo de control de acceso lógico a la carpeta donde se almacenan los archivos indexados, y al editor. Consideramos que puede agregarse una contraseña de ingreso a la carpeta con los archivos indexados, así como también implementar un password de ejecución a la aplicación de edición.

3.3 CONTROL DE APLICACIONES EN PC'S

- ❖ **Debilidad:** no hay estándares definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la instalación y actualización de la configuración de las PC's.

Efectos: al no haber estándares en cuanto a la instalación de un puesto de trabajo, puede realizarse una configuración equivocada, incurriendo en una pérdida de tiempo y productividad. Además puede ocurrir que cada empleado del centro de cómputos instale puestos de trabajo con una configuración diferente, lo que dificultaría el mantenimiento de los mismos.

Recomendación: sugerimos desarrollar un procedimiento formal a seguir cada vez que sea necesario instalar un nuevo puesto de trabajo en la empresa, o reparar alguna PC con errores de configuración, con el fin de establecer un estándar. Podría utilizarse, como complemento, alguna herramienta de restablecimiento y copia de configuración (como el Norton Ghost por ejemplo). Sería recomendable documentar, no solo el procedimiento de instalación y reparación de puestos de trabajo, sino además cada uno de los mantenimientos que se les realizan, a modo de historial de cada PC. Con esto se logra una documentación de la configuración actual de cada una de las máquinas.

- ❖ **Debilidad:** para los usuarios no existen restricciones con respecto a la instalación de programas en sus respectivos puestos de trabajo, ya que están

habilitados los dispositivos externos y algunos disponen de conexión a Internet sin restricciones.

Efectos: la instalación indiscriminada de aplicaciones puede traer problemas en relación a las licencias de los programas y virus. Otro punto a tener presente es la pérdida de productividad del empleado y de recursos, ya que pueden instalarse juegos y demás programas que no hacen al funcionamiento de la empresa, arriesgando la integridad de los datos; y si el usuario posee conexión a Internet se pone en juego la confidencialidad de los mismos.

Recomendación: para evitar esta situación, es recomendable que, en el momento que el usuario ingresa a la empresa, se lo notifique y acepte que está prohibida la instalación de cualquier producto de software en los equipos. Con este requerimiento es posible tomar medidas a posteriori de la infracción, además de ayudar a generar una “cultura de la seguridad”.

Sugerimos que algún encargado del centro de cómputos designado por el administrador, realice chequeos periódicos de las PC's, identificando así los nuevos productos que han sido instalados. Además sería conveniente instalar una herramienta que audite en forma automática y constante las PC's en busca de modificaciones y genere reportes cada vez que suponga un problema, de esta manera no se necesitará realizar los chequeos con tanta frecuencia.

❖ **Debilidad:** la ventana de comandos del DOS está disponible para todos los usuarios de Windows.

Efectos: esta aplicación posee una gran cantidad de herramientas peligrosas para la estabilidad del sistema, tales como el *format* o el *deltree*, que pueden ser ejecutados por usuarios inexpertos o maliciosos.

Recomendación: este comando (command.com) debería eliminarse de los sistemas Windows y en el caso que el administrador necesite de esta aplicación, podría utilizarla a través de la red o de un dispositivo externo.

3.4 CONTROL DE DATOS EN LAS APLICACIONES

No se hallaron debilidades significativas con respecto a este tema.

3.5 CICLO DE VIDA

❖ **Debilidad:** no existe un plan de desarrollo de sistemas formal, ni se utilizan métricas durante el ciclo de vida del software.

Efectos: al no tener un plan de desarrollo, puede ocurrir que se administren mal las prioridades, lo que implica un atraso en el desarrollo del sistema. Además, genera un despilfarro de recursos y una administración de tiempos generalmente deficiente.

Al no utilizarse métricas con el objetivo de cuantificar los pasos del desarrollo, la estimación de los recursos a utilizar puede desviarse mucho de la realidad, generando más problemas en el desarrollo.

Recomendación: sería conveniente que el equipo de desarrolladores siguiera un plan detallado, generado por el administrador de sistemas, donde se definan

las asignaciones de recursos, el establecimiento de prioridades, la administración de tiempos y la utilización de métricas de software, con el objeto de garantizar en forma eficiente el cumplimiento de las tareas propuestas.

- ❖ **Debilidad:** no se aplica una gestión de configuración o un control de versiones durante el desarrollo.

Efectos: la gestión de la configuración se encarga de la administración de las modificaciones del sistema, si esta tarea del desarrollo no se aplica, entonces existirán inconsistencias en las modificaciones realizadas y en cada oportunidad se hará más difícil agregar nuevas modificaciones al sistema, además de no tener bien documentados los cambios realizados.

Recomendación: es imprescindible implementar una gestión de configuración o un control de versiones, para así documentar los cambios y poder analizarlos. Suponemos que una mejor administración de los cambios puede implementarse utilizando un documento formal de solicitud de cambio, donde quede reflejado el motivo del cambio y la solicitud requerida. Así quedará registrado dentro de la gestión de configuración y este mismo documento será utilizado para actualizar la documentación, tanto de las carpetas de los módulos como de los manuales de usuario.

Además sería conveniente tener en cuenta, durante el análisis de requisitos, evaluar los requerimientos de seguridad necesarios.

- ❖ **Debilidad:** no hay políticas formales definidas para la contratación de terceros en el desarrollo.

Efectos: el tercero, al no tener conocimiento de las normas de seguridad implementadas en la empresa, puede no cumplirlas poniendo en riesgo la seguridad de los activos.

Recomendación: se debe informar por escrito la importancia de la seguridad de la información a todo el personal contratado, terceros y consultores. El administrador del centro de cómputos, junto con los directivos, deberían ser quienes especifican los requerimientos de seguridad, los pasos a seguir en caso que no se respete lo establecido en el contrato y piden al tercero en cuestión que informe posibles brechas de seguridad existentes.

Adicionalmente, los contratos con terceros deberían contener una cláusula que indique “Derecho de auditar” para asegurar que el personal de la empresa o las autoridades representativas puedan evaluar su desempeño.

4- SEGURIDAD FÍSICA

4.1 EQUIPAMIENTO

No se hallaron debilidades significativas con respecto a este tema.

4.2 CONTROL DE ACCESO FÍSICO AL CENTRO DE CÓMPUTOS

- ❖ **Debilidad:** no hay control de acceso físico al centro de cómputos, ya que ninguna de las cámaras del circuito cerrado de video lo apunta a él o a su puerta de ingreso.

Efectos: al no haber un control de acceso especial en el centro de cómputos, cualquier persona que tenga acceso al área de administración y ante una distracción del personal, puede ingresar en él, con todo el riesgo que esto implica, debido a la sensibilidad crítica de los datos y activos que allí se encuentran.

Recomendación: sería conveniente que el área del centro de cómputos, donde se encuentran los servidores, el switch central y demás equipamiento crítico tenga una medida de seguridad extra, a través de la cuál solo se permita el acceso a los administradores. Esto podría implementarse con una llave, ya que no implica mucho gasto y pueden darse copias solo al personal necesario. Ó, en reemplazo de esta medida, puede agregarse una cámara extra de video que grabe el interior del centro de cómputos, o modificar la orientación de alguna existente hacia la puerta de ingreso al mismo.

- ❖ **Debilidad:** pudimos comprobar, durante al auditoría, que algún personal de mantenimiento técnico externo a la empresa ingresó al centro de cómputos y realizó sus actividades sin supervisión del personal de la empresa.

Efectos: esto situación puede resultar peligrosa ya que, como mencionamos anteriormente, en esta habitación se almacenan gran cantidad de equipos, corriendo el riesgo de robo de equipamiento o datos. Este incumplimiento de esta norma no ayuda a generar en los empleados una “cultura de la seguridad” sino que produce el efecto inverso, debilitándola.

Recomendación: cualquier persona ajena a la empresa que necesite realizar una tarea de mantenimiento relativa al centro de cómputos, debería anunciarse en la puerta de entrada. El personal del centro de cómputos debería escoltar a los visitantes desde la puerta hacia el interior del edificio, acompañándolos durante el transcurso de sus tareas, hasta que éstas sean concluidas.

4.3 CONTROL DE ACCESO A EQUIPOS

- ❖ **Debilidad:** las máquinas de la empresa disponen de disqueteras y lectoras de CD, aunque solo el 90% de los usuarios no las necesitan. Estos dispositivos están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos.

Efectos: debido a que cualquier usuario puede introducir un disquete o un CD con virus o intentar bootear desde estos dispositivos, esto implica un gran riesgo a la integridad del equipo y sus datos.

Recomendación: sería conveniente que las disqueteras y lectoras de discos se deshabilitaran desde el BIOS de cada máquina. Si llega a ser necesario, para realizar alguna tarea de mantenimiento, el administrador de sistemas puede ingresar al BIOS del equipo (utilizando la contraseña que él suministró), habilitar el dispositivo necesario y, una vez utilizado, deshabilitarlo nuevamente.

- ❖ **Debilidad:** no hay control de acceso a la configuración del BIOS de las PC's y de los servidores.

Efectos: de esta forma al momento del encendido de la máquina cualquiera podría modificar las opciones de configuración de los equipos.

Recomendación: sería conveniente que las máquinas tuvieran configurado un password de administrador en el acceso al setup (BIOS), para evitar que se modifiquen las configuraciones base de los equipos, esto podría aplicarse tanto a las PC's como a los servidores. Estas contraseñas deberían gestionarse el administrador del sistema, en todos los equipos de la red.

- ❖ **Debilidad:** no existe un control de acceso físico en el momento del encendido de los servidores.

Efectos: los servidores podrían ser encendidos por cualquier persona, sin que tenga que ingresar ninguna contraseña de ingreso.

Recomendación: sería conveniente que los servidores tengan implementado un sistema de llave de hardware, de manera que solamente el administrador del sistema, o la persona designada por él, pueda encenderlos.

- ❖ **Debilidad:** en el centro de cómputos hay unidades de zip no utilizadas, guardadas sin llave ni control de acceso adicional.

Efectos: estos dispositivos podrían ser fácilmente robados, o cualquier persona que disponga de los instaladores necesarios, podrá instalar dichas unidades en cualquier PC de la empresa.

Recomendación: consideramos que sería conveniente agregar otro control a esta clase de dispositivos, guardándolos en algún armario con llave.

- ❖ **Debilidad:** no se realizan controles sobre los dispositivos de hardware instalados en las PC's, una vez que se ha completado la instalación de algún equipo, el administrador del sistema no realiza chequeos rutinarios o periódicos.

Efectos: cualquier usuario podría sacar, poner o reemplazar algún dispositivo sin que se advierta la modificación.

Recomendación: sería conveniente que el administrador, o algún encargado de cómputos designado por él, realice chequeos periódicos para comprobar la correcta instalación de los dispositivos de los equipos, su buen funcionamiento y que sus números de series se correspondan con los datos registrados por el administrador al momento de la instalación.

- ❖ **Debilidad:** los servidores del centro de cómputos no se apagan en horarios no laborales, permanecen prendidos las 24 horas del día, aunque durante la noche no se realicen trabajos, permanecen ociosos.

Efectos: al permanecer prendidos sin justificación, se acorta el tiempo de vida útil del hardware y se predispone a que se produzcan posibles intrusiones en el momento en que no hay nadie en el centro de cómputos para mitigar el ataque.

Recomendación: debido a que no es necesario que los servidores permanezcan prendidos las 24 horas, podrían apagarse automáticamente a las 20:30, horario en que han cerrado todas las sucursales de la empresa.

4.4 DISPOSITIVOS DE SOPORTE

No se hallaron debilidades significativas con respecto a este tema.

4.5 ESTRUCTURA DEL EDIFICIO

No se hallaron debilidades significativas con respecto a este tema.

4.6 CABLEADO ESTRUCTURADO

- ❖ **Debilidad:** en el caso de ocurrir una contingencia con las antenas radiales, la sucursal queda imposibilitada de realizar transacciones on line.

Efectos: el sistema de radio queda inutilizable desde esa sucursal caída hasta la última, implicando que las tareas deben realizarse en forma manual.

Recomendación: en el caso de ocurrir esta contingencia recomendaríamos utilizar un sistema off line. Es decir, contar con un sistema isla de entrada de datos que, una vez reestablecido el servicio de red haga una actualización de los datos al sistema central. Hay que tener presente que este sistema de respaldo no reemplaza al sistema manual.

5- ADMINISTRACIÓN DEL CPD

5.1 ADMINISTRACIÓN DEL CPD

- ❖ **Debilidad:** no se asignan responsabilidades puntuales a cada empleado en cada tarea, ni hay un empleado del centro de cómputos designado como responsable de la seguridad de la organización.

Efectos: al no haber responsabilidades puntuales asignadas a cada empleado, pueden generarse malas interpretaciones con respecto a las tareas a desarrollar, lo que genera una pérdida de productividad.

Recomendación: deberían designarse responsabilidades claras y documentadas para cada empleado del centro de cómputos, las que deberán constar en los procedimientos formales que se desarrollen para cada actividad. De acuerdo a las funciones que desempeñen deberán distribuirse los permisos particulares de cada uno de los usuarios en sus respectivas cuentas del sistema.

Además debería haber un empleado a cargo de la seguridad del sistema, que coordine las tareas relativas a este tema, haciendo cumplir las políticas de seguridad en toda la empresa.

- ❖ **Debilidad:** no se han desarrollado planes formales del departamento de sistemas.

Efectos: sin planes de sistema se genera una deficiencia en la administración de tiempo, recursos humanos, costos, etc. lo que dificulta la productividad y eficiencia del área.

Recomendación: una medida de control útil sería desarrollar un plan de sistemas a corto plazo, que permita una supervisión continua y directa de las tareas que realiza el personal del centro de cómputos, y que contenga un cronograma de las actividades del área, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un periodo no muy prolongado de un año, debido a las cambiantes exigencias del sector.

Además podría considerarse el desarrollo de un plan estratégico a largo plazo, que contenga los proyectos principales y los cronogramas de su implementación, para un periodo de por lo menos 3 años.

- ❖ **Debilidad:** no hay, en los empleados de la empresa, plena conciencia con respecto a la importancia de la seguridad informática.

Efectos: al no existir una cultura de la seguridad implementada en la empresa, no se asegura el cumplimiento de normas y procedimientos.

Recomendación: a pesar de que existe una cierta conciencia sobre la seguridad de la información en el sector gerencial de la empresa, el equipo de sistemas debe hacer hincapié en la concienciación de todos los usuarios, haciéndolos más responsables y partícipes de las medidas de seguridad, ya que son los

principales involucrados, tanto los usuarios actuales como los que se incorporen en el futuro.

El proceso de concienciación debería ser renovado y transmitido a los usuarios en forma anual para asegurar que todos los usuarios que están afectados tengan acceso a las novedades sobre aspectos de seguridad.

- ❖ **Debilidad:** cada vez que los usuarios necesitan asesoramiento o servicios del centro de cómputos se comunican telefónicamente con alguno de los miembros del área.

Efectos: no queda ninguna constancia de las tareas desarrolladas por los empleados del centro de cómputos, ni de las solicitudes de los usuarios.

Recomendación: sería conveniente que los usuarios envíen mails al centro de cómputos, solicitando asesoramiento o servicios, o para reportar incidentes o problemas con sus equipos, de manera que quede constancia de la misma. Además debería llevarse un registro de los trabajos efectuados por los empleados del centro de cómputos, es decir tener algún tipo de mecanismo o historial de reportes.

Podría ser útil y eficiente la implementación de un buzón de sugerencias (por ejemplo una dirección de correo), donde los usuarios puedan recomendar mejoras o realizar cualquier tipo de comentarios, expresando sus inquietudes.

- ❖ **Debilidad:** en el centro de cómputos no se desarrolla ningún mantenimiento preventivo.

Efectos: al no tener implementado un mantenimiento preventivo de los equipos y sistemas de la empresa, será necesario esperar a que ocurran los desastres para arreglarlos, lo que ocasiona pérdida de efectividad de los empleados.

Recomendación: cuando finalice el desarrollo, alguno de los empleados podría asumir la responsabilidad de llevar a cabo un mantenimiento preventivo, monitorizando, chequeando y auditando las PC's y demás dispositivos que conforman la red.

- ❖ **Debilidad:** no existe un inventario donde se documenten todos los sistemas de información y sus características principales.

Efectos: al generar un inventario detallado es posible discriminar los responsables de la información que administra cada sistema, las áreas en la que interviene y el nivel de prioridad con que cuenta en caso de una emergencia.

Recomendación: es conveniente la generación de un inventario donde se detallen los sistemas de información utilizados en la organización, documentando las siguientes características:

- Nombre
- Lenguaje
- Departamento de la empresa que genera la información (dueño del sistema)
- Departamentos de la empresa que usan la información
- Volumen de archivos con los que trabaja

- Volumen de transacciones diarias, semanales y mensuales que maneja el sistema
- Equipamiento necesario para un manejo óptimo del sistema
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este sistema para la Institución (medido en horas o días en que la institución puede funcionar adecuadamente, sin disponer de la información del sistema).
- Relación de equipamiento mínimo necesario para que el sistema pueda seguir funcionando. Será necesario mantener esta relación siempre actualizada.
- Actividades a realizar para volver a contar con el sistema de información (actividades de restauración)

Puede ser útil disponer de un responsable a cargo de la actualización del mismo, que controle periódicamente estos dispositivos y la información almacenada.

- ❖ **Debilidad:** no hay inventarios de los equipos de hardware, ni documentación con respecto a los equipos de la red física.

Efectos: esta documentación facilita las actividades de los administradores del centro de cómputos, en el momento de realizar tareas de mantenimiento y para el desarrollo del plan de contingencias.

Recomendación: se debería implementar un inventario detallado de los equipos de cómputos, donde se incluya:

- Hardware: dispositivos instalados en cada máquina, número de serie, y demás datos sobre procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges, etc.
- Software en los equipos: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones, números de licencias, etc.
- Datos o principales archivos que contienen los equipos: durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, dueño designado de la información, etc.
- Configuración de los equipos (y sus archivos de configuración).
- Ubicación de los equipos.
- Nivel de uso institucional de los equipos.
- Etc.

Puede ser útil disponer de un responsable a cargo de la actualización del mismo, que controle periódicamente estos dispositivos y la información almacenada.

Sugerimos, además desarrollar procesos para rotular, manipular y dar de baja una computadora, sus periféricos y medios de almacenamiento removibles y no removibles.

- ❖ **Debilidad:** no se ha implementado un procedimiento que describa la manera de realizar la publicidad de las normas, directivas o modificaciones las mismas.

Efectos: en una organización es muy importante conocer las últimas modificaciones realizadas a los procedimientos o normas, de manera que nadie pueda excusarse de no conocer estos cambios.

Recomendación: debería existir un procedimiento describiendo la manera de realizar la publicidad de las modificaciones, incluyendo quién estará a cargo de la tarea. Esto puede llevarse a cabo mediante un mailing, por exposición en transparencias, por notificación expresa, o por otra vía de comunicación.

Es fundamental tener en cuenta este punto ya que un gran porcentaje de los problemas de seguridad proviene del desconocimiento de las normas y/o modificaciones a ellas por parte de los usuarios.

Esta metodología deberá emplearse para el anuncio de la política de seguridad que se desarrollará y para sus futuras modificaciones.

- ❖ **Debilidad:** los usuarios deben realizar tareas de mantenimiento, como actualizar el antivirus, **hacer copias de respaldo de sus datos**, defragmentar el disco, modificar y proteger sus password, borrar archivos temporales, entre otras.

Efectos: estas son tareas revisten gran importancia en el funcionamiento de los equipos de los puestos de trabajo, y una falla en su realización puede generar el mal funcionamiento de los mismos.

Recomendación: estas tareas de mantenimiento de las PC's de los puestos de trabajo deberían ser llevadas a cabo por el administrador del centro de cómputos, o por alguien designado por él.

- ❖ **Debilidad:** los instaladores de uso más frecuente están on line en el servidor y se instalan desde carpetas compartidas por éste.

Efectos: compartir carpetas en el servidor significa un gran riesgo para la administración de red ya que facilita la intrusión.

Recomendación: sería conveniente almacenar estos instaladores fuera del servidor, en particular recomendamos que los mismos se guarden en el mismo equipo que se utiliza para los demás backups de la empresa (detallado más adelante), en una carpeta protegida con contraseña, o podrían generarse CD's con estos instaladores.

5.2 CAPACITACIÓN

- ❖ **Debilidad:** en ningún momento hay consentimiento por parte de los usuarios a que auditen sus actividades en el sistema, ni declaraciones de que conocen las normas de "buen uso" del sistema.

Efectos: no hay un aval de que el usuario ha comprendido las normas de buen uso del sistema, y que está dispuesto a cumplirlas.

Recomendación: una vez que el usuario ha sido capacitado en la realización de sus tareas cotidianas y tenga una clara visión del manejo del sistema se le podría comunicar la política de seguridad de la información y los procedimientos establecidos por la empresa, además de un resumen por escrito

de las medidas básicas, junto con una copia que debería ser firmada por él y resguardada en el legajo del empleado. Esto implica que está de acuerdo con las normas impuestas, y es conciente de las consecuencias que acarrea el incumplimiento de estas normas.

5.3 BACKUP

- ❖ **Debilidad:** no se documentan los cambios que se realizan en la configuración de los servidores, ni la fecha de estas modificaciones.

Efectos: al no tener documentación actualizada de los cambios realizados, se dificulta conocer la configuración exacta y actual de cada servidor, y de esta forma se obstaculiza la tarea del mantenimiento.

Recomendación: sugerimos que se documente cada uno de estos cambios, para así tener un control y una identificación de los mismos, así se podrá generar un historial de modificaciones y calcular estadísticas de los mismos, y con éstas será posible hacer más eficiente la configuración de los servidores.

- ❖ **Debilidad:** no hay ningún procedimiento formal para la realización ni la recuperación de los backups de los datos almacenados en los servidores de la empresa.

Efectos: las copias de respaldo son el principal método de recuperación de datos del que dispone la organización y la ausencia de procedimientos para su implementación puede generar errores en el momento de un incidente.

Recomendación: consideramos necesario que exista un procedimiento escrito y formal de política de backup, que contenga las recomendaciones que se describen a continuación:

- Sería conveniente que el administrador del centro de cómputos designe a un *responsable* de la realización de las copias de seguridad y de su restauración, y un suplente de éste primero.
- El procedimiento de generación de backup debería estar *automatizado* con alguna herramienta de generación de copias de respaldo de datos.
- Las copias de respaldo deben realizarse en el *momento* en que se encuentre la menor cantidad posible de usuarios en el sistema.
- Debería realizarse un backup *incremental* diario, todos los días de la semana, mientras que una vez por semana sería conveniente realizar un backup completo de los datos más significativos.
- Deberían realizarse chequeos para comprobar que los procedimientos de *restauración* son eficientes.
- Los archivos de backup deberían tener una *contraseña* que los proteja, o bien encriptarse, ya que contienen información confidencial.
- Los backups diarios deberían *almacenarse en el exterior* de la empresa, ya que poseen un empleado designado, sería conveniente contar con un suplente.
- Sugerimos que este empleado se lleve el *último backup realizado*, mientras que los demás CD's deberían permanecer en el interior de la empresa resguardados en un lugar ajeno al centro de cómputos.

Consideramos necesario que el CD que es llevado al exterior sea transportado en un medio resistente que lo proteja.

- Deberían realizarse chequeos para comprobar el funcionamiento correcto de los *medios externos* donde se realizan las copias de respaldo.
- Debería existir una política de *reemplazo de CD's*, donde conste que deberían reemplazarse cada 6 meses, para evitar posibles fallas en el momento de la recuperación, debido al tiempo de vida útil del medio.
- Debería existir un *procedimiento de recuperación* de copias de respaldo, donde se incluya la metodología a seguir, quién tiene el permiso para realizarlo y en qué casos será permitido.
- Debería existir *documentación* de los backups generados, incluyendo:
 - qué datos contienen estas copias,
 - fechas de realización,
 - fechas de restauración,
 - errores obtenidos,
 - tiempo empleado en el proceso,
 - demás datos que se consideren necesarios en la administración de este procedimiento.

❖ **Debilidad:** los usuarios hacen backups de sus datos en sus propias máquinas o en disquetes.

Efectos: hacer un backup en la misma máquina donde están los archivos originales no es garantía, y hacerlos en disquetes tampoco sirve por la mala calidad del medio.

Recomendación: debido a que los usuarios no deberían tener habilitados dispositivos de almacenamiento externo (disqueteras) lo más conveniente sería que el administrador del sistema disponga de una máquina para la realización de backups. Allí debería generar todas las copias de respaldo de los datos de los usuarios. La carpeta donde se guarden estos backups deberá estar protegida con una contraseña gestionada por el administrador para restringir el acceso de otros usuarios.

❖ **Debilidad:** no hay ningún procedimiento formal para la realización ni la recuperación de los backups de la página Web de la empresa.

Efectos: las copias de respaldo son el principal método de recuperación de datos del que dispone la organización y la ausencia de procedimientos para su implementación puede generar errores en el momento de un incidente.

Recomendación: debería existir un procedimiento formal de backup de la página web, este backup debe contener toda la página completa, y debe hacerse cada vez que se modifique la estructura de la misma. Este backup debería almacenarse en el mismo equipo que los backup de los usuarios, en otra carpeta protegida con contraseña.

5.4 DOCUMENTACIÓN

❖ **Debilidad:** no hay un buen soporte de documentación en el centro de cómputos.

Efectos: al no poseer un buen soporte, la información puede ser incorrecta, inconsistente o desactualizada, lo que genera incertidumbre y dificulta la administración de incidentes.

Recomendación: sugerimos que la documentación posea mas detalles respecto a los siguientes datos:

- Diagrama de la distribución física de las instalaciones, identificación de PC's y equipos, y puestos de trabajo
- Número de serie de hardware
- Número de licencia del software
- Inventario de "hardware" y "software"
- Fallas en equipos y trabajos de mantenimiento
- Entrada del personal externo.
- Configuración de equipos y servidores.
- Cambios en la topología de red.
- Modificaciones de emergencia realizadas a sistemas y hardware.
- Procesos estándares del Sistema Operativo (en especial de Linux sobre las operaciones básicas)
- Métodos para compartir datos entre sistemas (por ejemplo con las fábricas, entre las sucursales o entre las PC's de la red)

Toda esta documentación debería generarse teniendo en cuenta tanto la casa central como las sucursales.

❖ **Debilidad:** no hay desarrollados planes de seguridad, procedimientos formales, ni demás manuales o documentos de soporte para la gestión de la seguridad en la red informática.

Efectos: al no poseer un buen soporte, la información puede ser incorrecta, inconsistente o desactualizada, lo que genera incertidumbre en el momento de llevar a cabo procedimientos o procesos, lo que dificulta la administración general.

Recomendación: sugerimos que la documentación posea mas detalles respecto a los siguientes datos:

- Plan de contingencia
- Política de seguridad
- Manual de procedimientos
- Manual de usuario (del software y del hardware)
- Manual de seguridad para el sistema: detalla las funciones y privilegios de la seguridad. Contiene: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc.
- Manual de seguridad para el usuario: asiste a los usuarios del sistema, describe como usar las protecciones, las responsabilidades de la seguridad del sistema.

❖ **Debilidad:** durante el desarrollo de sistemas, la documentación no es completa y las actualizaciones se realizan informalmente.

Efectos: por fallas en la gestión de la documentación pueden producirse errores en el desarrollo del sistema, así como una mala administración de recursos y falencias en la estimación de tiempos.

Recomendación: sugerimos la realización de los siguientes documentos para mejorar la documentación existente y así lograr una organización eficiente:

- objetivos,
- alcances,
- diagramas general y de funciones o de procesos,
- DER,
- diagrama de flujo,
- archivos de entrada-salida,
- responsable del módulo (analista que lo desarrolló),
- registro de modificaciones,
- lenguaje de programación,
- problemas o limitaciones conocidas,
- sectores de la organización a los que afecta,
- descripción del "hardware" y "software" utilizados,
- características de seguridad,

Consideramos necesario que cada vez que se produzca una modificación en algún módulo del sistema, se modifique toda la documentación correspondiente. Las modificaciones deben hacerse de acuerdo a un procedimiento formal definido en la gestión de configuración.

6- AUDITORÍAS Y REVISIONES

6.1 CHEQUEOS DEL SISTEMA

- ❖ **Debilidad:** no cuentan con una aplicación que genere alarmas o avisos cuando ocurre un evento que revista un determinado grado de riesgo.

Efectos: para que el administrador tome conocimiento de la ocurrencia de algún incidente problemático, debe leer los registros generados por las aplicaciones, analizarlos y tratar de encontrar problemas en un gran archivo de textos. Esta situación no resulta práctica, y puede ocurrir que la notificación del problema llegue tarde, cuando el error ya está avanzado.

Recomendación: aplicación para generar reportes y alarmas, ya que la lectura de los logs es tediosa y poco práctica, sería conveniente generar alarmas o algún otro mecanismo de alerta cuando ocurra algún evento en particular. Usar una aplicación que administre los logs, teniendo en cuenta la severidad de los eventos, e identificando el usuario asociado al evento.

- ❖ **Debilidad:** no se buscan nuevas herramientas de generación ni gráfico de logs.

Efectos: puede perderse efectividad y eficiencia con el uso de herramientas poco prácticas y desactualizadas, que no poseen generación de reportes ni alarmas, para que el administrador esté siempre al tanto de las situaciones riesgosas.

Recomendación: sería conveniente actualizar continuamente las herramientas que se usan para graficar la información generada en los logs. Debería asignarse la responsabilidad de esta tarea a una persona específica.

- ❖ **Debilidad:** no existe una línea de base definida, solo disponen de los datos almacenados en los logs.

Efectos: no es posible comparar medias o promedios generados en la empresa en situaciones normales con los valores actuales obtenidos de los logs, e identificar actividades inusuales.

Recomendación: sería conveniente generar líneas de base, en vez de un conjunto de datos históricos, para poder tener información sobre las PC's, los servidores y el sistema en general con detalles sobre, por ejemplo:

- qué usuario, sector o tarea utiliza más recursos de CPU (para calcular este dato dispongo de los logs generados por el AcuServer),
- qué datos son los que consumen más tráfico de red, memoria o CPU,
- qué datos se utilizan o se modifican con mas frecuencia,
- qué archivos tienen mayor índice de crecimiento (en los logs que genera el AcuServer hay información sobre quién accede a cada dato, en que momento accede y en qué momento libera los archivos),
- qué aplicaciones son más utilizadas,
- qué aplicaciones consumen más recursos,

- quién utiliza más memoria del servidor,
- en qué momento surgen cuellos de botella y en qué recursos,
- en qué momento o por cuánto tiempo la memoria o el CPU permanecen usados en un 100% de su capacidad.

❖ **Debilidad:** al hacer alguna modificación en la configuración del sistema, se genera una nueva compilación de datos (nueva línea de base), que no se documenta.

Efectos: esta situación genera confusiones, ya que no se identifica si se han modificado los valores debido a algún incidente o si la variación se debe a cambios realizados en el sistema.

Recomendación: sería conveniente documentar las nuevas líneas de base cuando se hace alguna modificación en el sistema, generando así un histórico de líneas de base y sus variaciones por incidentes. Esto se debe a que pequeños cambios en las configuraciones pueden producir grandes impactos en la performance.

❖ **Debilidad:** los logs se eliminan sin generar un backup de sus datos.

Efectos: al no hacer backup de los datos de los logs no es posible obtener datos estadísticos para la generación de las líneas de base.

Recomendación: sería recomendable, antes de eliminar los logs con el CronTab, generar un resumen de líneas de base y estos resultados guardarlos en CD's.

❖ **Debilidad:** en la empresa no se realizan auditorías programadas, ni rutinas de chequeos de logs.

Efectos: al no realizar controles aleatorios resulta difícil verificar el cumplimiento de los requerimientos y procedimientos de seguridad.

Recomendación: sería conveniente que se programen auditorías y chequeos aleatorios, para controlar las áreas o funciones críticas con respecto a la seguridad de los datos de la empresa, documentando la ejecución y los resultados de dichas pruebas.

Debe tenerse en cuenta la recomendación sobre separación de tareas, ya que la persona que realice dichas revisiones no debería estar comprometida con la tarea a auditar. Además, si el tamaño de la auditoría lo justifica, sería conveniente que la lleve a cabo un grupo de dos o más personas, para disminuir las tentativas de corrupción.

6.2 RESPONSABILIDADES DE LOS ENCARGADOS DE SEGURIDAD

No se hallaron debilidades significativas con respecto a este tema.

6.3 AUDITORÍAS DE CONTROL DE ACCESO

- ❖ **Debilidad:** los logs se guardan en el servidor de aplicaciones y en el de Internet, sin controles de acceso lógico a las carpetas donde están almacenados. Además pueden ser accedidos desde cualquier máquina conectada a la red, por usuarios o administradores, utilizando el WebMin, conociendo la clave de administrador.

Efectos: la modificación del contenido de los logs es considerada de alta criticidad debido a que usuarios, administradores o intrusos mal intencionados pueden borrar las pistas de auditoría correspondientes a violaciones del sistema.

Recomendación: sería conveniente reforzar con un password las carpetas donde se almacenan los logs para que los usuarios o administradores no puedan borrar o modificar los logs. Debe tenerse presente que, incluso para el administrador del sistema, este password debe ser desconocido, por lo que sugerimos que lo conserve algún miembro de la gerencia.

- ❖ **Debilidad:** la información que se almacena en los logs con respecto a las conexiones a Internet no es suficiente, ya que solo se almacena el número IP de la máquina conectada y la dirección de las páginas visitadas.

Efectos: al no disponer de la información necesaria, no será posible conocer las actividades de los usuarios en la red, como por ejemplo identificar la procedencia de posibles virus.

Recomendación: sería útil poseer información más detallada sobre:

- Cookies guardadas
- Archivos descargados
- Servicios utilizados
- Aplicaciones utilizadas

- ❖ **Debilidad:** no se identifican los usuarios que acceden a datos.

Efectos: no puedo identificar qué usuario accede a los datos, debido a que tengo información sobre la máquina que ingresa al sistema pero no del usuario que accede a los datos y cualquier usuario podría utilizar cualquier máquina.

Recomendación: es conveniente que se identifique al usuario, y no a la máquina que accede a los datos y así será posible rastrear las acciones de cada usuario en el tiempo.

- ❖ **Debilidad:** no se generan reportes relativos a las actividades de los usuarios sobre los datos.

Efectos: para el administrador del sistema resulta muy complicada la revisión de las actividades de los usuarios basándose en un estudio de los logs, debido a la cantidad de tiempo que implica esta tarea.

Recomendación: podría utilizarse una herramienta de generación de reportes de manera automática con datos sobre:

- Cantidad de usuarios que acceden simultáneamente a la base de datos (cantidad de conexiones activas),
- Estadísticas de entrada-salida para cada usuario,
- Tiempo y duración de los usuarios en el sistema,
- Usuarios que no han ingresado al sistema por un largo período de tiempo.
- Ocurrencias de deadlock con la base de datos,
- Generación de nuevos objetos de bases de datos,
- Modificación de datos,
- Número de intentos fallidos de conexiones a bases de datos.

Se deberán generar estadísticas o líneas de base de estos datos, a fin de utilizarse para el control de los datos de la base de datos.

- ❖ **Debilidad:** no se realizan chequeos periódicos a los logs generados con el usuario administrador del sistema

Efectos: al no generarse reportes sobre las actividades del usuario administrador, se corre el riesgo de que algunas acciones de intrusos o no permitidas pasen inadvertidas.

Recomendación: deberían realizarse controles sobre estos logs, comprobando que las acciones realizadas por el administrador se correspondan con los datos que en ellos figuran, de manera de identificar posibles intrusiones o anomalías. El estudio de estos reportes no debería ser realizado por el administrador, sino por su superior. Para que esta recomendación tenga validez, deberá cumplirse la sugerencia que imposibilita a los usuarios y administradores la modificación de los logs.

- ❖ **Debilidad:** no se generan logs cuando un usuario modifica su password.

Efectos: deben poder rastrearse todas las actividades del usuario en el sistema.

Recomendación: sugerimos que se generen logs cuando un usuario modifica su contraseña, agregando datos como la aplicación desde la que se realizó el cambio y en caso que el cambio resulte fallido, el motivo del fallo.

- ❖ **Debilidad:** los logs generados por un login fallido no especifica el motivo del fallo.

Efectos: al no incluir el motivo del fallo en los logs, no será posible determinar si hubo un error en el sistema, intento de intrusión o el usuario confundió su contraseña, entre otras.

Recomendación: detallar el motivo del login fallido en el contenido del log.

- ❖ **Debilidad:** no se genera un registro cuando la cuenta de un usuario ha sido bloqueada, ni tampoco un sistema de alerta ante este bloqueo.

Efectos: no poseer registros de los bloqueos de los usuarios, imposibilita la generación de estadísticas al respecto. Al no tener un sistema de alerta que ponga en conocimiento del administrador de esta situación, no le será posible identificar los intentos de intrusión en el momento en que ocurren.

Recomendación: sería conveniente que se generen logs cuando ocurra un evento de este tipo, y que se avise al administrador por medio de un sistema de alerta. Con este sistema podrían detectarse anticipadamente intentos de intrusión.

- ❖ **Debilidad:** no se generan perfiles de los usuarios con respecto a sus actividades.

Efectos: sin estos perfiles no se pueden identificar anomalías por grupos de usuarios.

Recomendación: sería conveniente generar estos perfiles con el objeto de saber que uso le dan a Internet, el tráfico de mails, tráfico de red que genera cada usuario o sector de la empresa, que terminales utilizan, las horas de acceso, etc., para así determinar qué acciones son inusuales y deban ser investigadas.

- ❖ **Debilidad:** no se generan logs cuando se requiere una impresión de algún dato suministrado por el sistema de la empresa.

Efectos: al no generar logs no se tiene un control sobre los datos de la empresa impresos, ni de los usuarios que solicitan esta tarea.

Recomendación: cuando un usuario solicita una impresión de algún dato del sistema de la empresa, debería generarse un log de dicho evento.

6.4 AUDITORÍAS DE REDES

- ❖ **Debilidad:** no poseen un plan de monitorización general de la red.

Efectos: al no tener un plan organizado de monitorización, puede ocurrir que baje la performance del sistema debido a cuellos de botella en los recursos.

Recomendación: generar un plan de monitorización, teniendo en cuenta que la monitorización tiene un impacto directo en la performance del sistema. Se podría utilizar, por ejemplo, alguna herramienta para monitorizar el tráfico y rendimiento de red, como un escáner de seguridad integral (Overall Security Scanner).

- ❖ **Debilidad:** no se auditan regularmente ni se generan estadísticas sobre los logs referentes al correo electrónico.

Efectos: al no tener estas estadísticas no se calculan ni se grafican líneas de base y al no realizar monitoreos periódicos no se puede alertar al administrador sobre anomalías o posibles errores.

Recomendación: el administrador o un encargado del centro de cómputos debería ser responsable de la monitorización de éstos logs, generando reportes diarios o mensuales, con los siguientes datos:

- poco espacio libre de cuotas asignadas al correo,
- disminución en la performance del correo,
- demasiados mensajes entrantes o salientes fuera de lo normal,

- departamento o usuario de la empresa que utiliza más el servicio de mail,
- warnings o advertencias ante la aparición de un virus,
- estadísticas sobre mails infectados con virus, períodos de mayor infección, máquinas más afectadas, direcciones fuentes que mas mails infectados envían, cantidad de archivos infectados por extensión (Ej. Los archivos de Word se infectan más que los de Excel),
- entre otras.

❖ **Debilidad:** no se auditan regularmente ni se generan estadísticas sobre los logs referentes a la administración de red. Además no se hace ningún seguimiento de los logs en busca de cambios en las estadísticas o en las líneas de base.

Efectos: al no tener estas estadísticas no se calculan ni se grafican líneas de base y al no realizar monitoreos periódicos no se puede alertar al administrador sobre anomalías o posibles errores, en lo respectivo al tráfico de red o utilización de recursos del servidor. Además pueden generarse nuevos cuellos de botella en algún recurso del sistema, y el administrador puede no notarlo hasta que algún usuario se lo advierta.

Recomendación: el administrador o un encargado del centro de cómputos debería ser responsable de la monitorización de estos logs. Podrían generarse gráficos y estadísticas diarios o mensuales compuestos por datos suministrados por las distintas aplicaciones que se utilizan en la empresa y que generen logs. Así podría obtenerse un reporte más detallado con datos y estadísticas como los siguientes:

- consumo de ancho de banda por terminal o por sector de la empresa o cuellos de botella en el tráfico de red,
- cantidad de tráfico genera cada aplicación utilizada por cada usuario
- cantidad de recursos que utilizan las aplicaciones.
- el estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta, etc.),
- intentos de intrusión,
- estadísticas del uso de los protocolos
- páginas de Internet más visitadas, con información sobre los archivos descargados, los usuarios conectados, el horario, etc.

El seguimiento de estadísticas puede ser automatizado por medio de herramientas para Linux que realicen las tareas y sólo informen de las desviaciones con respecto a las líneas de base, a través de un mail o alerta. Podrían generarse avisos cuando exista:

- incremento en el uso de Internet o del servicio de correo,
- tráfico excesivo de red, sectores o PC's que superan el promedio de ancho de banda,
- incremento en los ataques o sospecha de intrusión,
- poco espacio en disco de servidores o de PC's,
- poca disponibilidad de CPU, memoria o algún recurso en los servidores,
- violaciones a las reglas de servicios de red, modificación en los permisos de los servicios o mala utilización de servicios

- entre otros.

❖ **Debilidad:** no se hicieron **pruebas de auto-hackeo**, escaneos o intentos de intrusión o de escucha en la red informática. Tampoco se hacen testeos periódicos de puertos o de los servicios que están habilitados.

Efectos: al no hacer pruebas o chequeos pueden pasar inadvertidas situaciones que solo serán reveladas utilizando casos prácticos.

Recomendación: sería conveniente programar chequeos periódicos de la red, incluyendo los siguientes controles:

- los servicios, su configuración y su buen funcionamiento;
- tratar de escuchar o hacer un ataque de intrusión periódicamente, para comprobar que la red sigue siendo inaccesible desde el exterior,
- realizar pruebas de auto-hackeo:
 - a los servidores, desde dentro del servidor,
 - a los servidores, desde la red interna,
 - a la intranet desde dentro de ella,
 - accesos desde el exterior y/o Internet.

Podrían utilizarse herramientas que permiten hacer estas inspecciones en la red en forma automática, para comprobar en qué estado está y determinar si existen vulnerabilidades en algunos sectores de acuerdo a líneas de base ingresadas por el administrador (como COPS, NOCOL, SATAN, SNORK o TRIPWIRE). Además sería posible hacer auto-escaneos para verificar los recursos compartidos, y auto-hackeos para prevenir ataques de intrusión. Sugerimos documentar las pruebas y sus resultados cada vez que se realicen.

7- PLAN DE CONTINGENCIAS

7.1 PLAN DE ADMINISTRACIÓN DE INCIDENTES

No se hallaron debilidades significativas con respecto a este tema.

7.2 BACKUP DE EQUIPAMIENTO

- ❖ **Debilidad:** no se realizan pruebas periódicas de los mecanismos de respaldo de los servidores.

Efectos: ante una emergencia, puede ocurrir que estos mecanismos no funcionen correctamente o que los responsables del centro de cómputos no desempeñen sus funciones correctamente por falta de práctica.

Recomendación: deberían realizarse planes de prueba periódicas, comprobando todos los mecanismos de respaldo con los que cuentan los servidores de la empresa.

- ❖ **Debilidad:** los dos servidores de la empresa se encuentran en la misma habitación física.

Efectos: ante un incidente, se puede utilizar un servidor en reemplazo del otro. Pero en el caso que la habitación donde se encuentran los servidores resulte afectada por una emergencia, ambos equipos quedarían inutilizados.

Recomendación: podría ser útil que alguno de los dos servidores, cuyas características son idénticas, se ubique en otra habitación o en otro edificio de la empresa, junto con un switch que actualmente se encuentra ocioso en el centro de cómputos. Esta situación puede resultar beneficiosa ante cualquier contingencia ocurrida en el centro de cómputos de la casa central.

Esta modificación no resultaría tan costosa ya que solo sería necesaria una habitación libre a la cual se le realizarían modificaciones mínimas de manera que funcione como un centro de cómputos alternativo con las mismas condiciones de seguridad sugeridas para el CPD principal.

De esta manera, ante cualquier contingencia, por ejemplo si se produce una rotura del panel de control de energía independiente del centro de cómputos de la casa central, el sistema informático no se vería afectado, debido a que se contaría con un servidor alternativo en otro lugar físico, específicamente en otro edificio.

7.3 ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES

7.3.1 ESTRATEGIA PREACTIVA

- ❖ **Debilidad:** no se asignan prioridades a los sistemas de información ni a los equipos de hardware de la red física.

Efectos: al no asignar niveles de prioridad a los sistemas o equipamientos no es posible determinar cuáles son los que deberían recuperarse de inmediato en caso de una emergencia.

Recomendación: se debería asignar un orden de importancia a cada uno de los sistemas de información y de los equipos de la red, de acuerdo al análisis de riesgo y al impacto que representaría para la empresa su ausencia. La prioridad mayor la tendrá aquel sistema que es más importante a la hora de recuperar la operatividad luego de un desastre. Los equipos podrían estar señalizados o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.

- ❖ **Debilidad:** no se han identificado las funciones más críticas para las actividades de la empresa.

Efectos: al no identificar las funciones que interrumpen la productividad de la empresa debido a su criticidad, se corre el riesgo de no tenerlas en cuenta en el momento de la restauración del sistema.

Recomendación: sería conveniente definir las funciones o servicios de la empresa que sean más críticos. Cada jefe o encargado de área debe interactuar con el administrador y definir estos servicios junto con los recursos mínimos necesarios para su funcionamiento, y asignarles una prioridad en el plan de restauración.

Además, sería conveniente identificar las contingencias que podrían ocurrir para cada nivel de servicio determinando, considerando:

- Cuáles serían los peores problemas a los que se puede ver sometida la empresa, cuáles serían las peores contingencias
- Cuáles serían las más probables
- Cuáles son las que ocurren más a menudo
- Cuáles son las que no ocurren nunca

- ❖ **Debilidad:** no se hacen simulaciones de siniestros.

Efectos: sin estas simulaciones no será posible comprobar que los empleados hayan comprendido las tareas a su cargo y será imposible predecir su comportamiento ante una emergencia.

Recomendación: para el entrenamiento del personal deberían generarse simulacros de siniestros y así evaluar la efectividad del plan.

7.3.2 *ESTRATEGIA DE ACCIÓN*

- ❖ **Debilidad:** en la empresa no hay planes formales para la administración de incidentes ni funciones claras que deba realizar el personal durante una contingencia, ya que no hay responsabilidades asignadas.

Efectos: al no haberse designado claramente las responsabilidades de los empleados frente a una emergencia, las acciones que se tomen en caso de contingencia resultarán caóticas, comprometiendo la integridad de los datos y equipos.

Recomendación: debería conformarse un plan de emergencias, determinando los procedimientos a llevar a cabo para cada contingencia identificada en la estrategia preactiva. Estas tareas deberían estar claramente definidas y documentadas, y tener asignado un responsable para su ejecución, considerando los distintos escenarios posibles (por ejemplo durante el día o la noche). Ejemplos de las tareas a desarrollar pueden ser:

- En caso de incendio:
 - Identificar las vías de salida
 - Generar un plan de evacuación del personal
 - Desarrollar un plan de puesta a buen recaudo de los activos
 - Ubicación y señalización de los elementos contra el siniestro
- En caso de intrusión interna o externa:
 - Desconectar los servidores
 - Cerrar todos los accesos a los datos
 - Rastrear al intruso

Deberían contemplarse las siguientes características:

- Debería estar documentado y testeado antes de su puesta en práctica.
- Debería basarse en un análisis de riesgo, determinando que acciones merecen estar incluidas.
- Debería abarcar toda la empresa, no solo el área de cómputos.
- Debería entrenarse a los responsables y a los usuarios
- Debería mantenerse actualizado de acuerdo a nuevos puestos de trabajos y funciones.
- Debería ser retroalimentarlo después de cada incidente.
- Debería ser probado frecuentemente.
- Debería contener la siguiente información:
 - Objetivo del plan.
 - Modo de ejecución.
 - Tiempo de duración.
 - Costes estimados.
 - Recursos necesarios.
 - Evento a partir del cual se pondrá en marcha el plan.

7.3.3 *ESTRATEGIA REACTIVA*

❖ **Debilidad:** no se documentan los acontecimientos ocurridos durante las emergencias, ni se hacen evaluaciones formales de los daños sufridos.

Efectos: al no documentarse los acontecimientos ni daños acontecidos, se corre el riesgo de no hacer las correcciones necesarias para que no ocurran las mismas contingencias. Puede ocurrir también que durante el incidente se realicen modificaciones de urgencia en alguna parte del sistema y éstas no queden documentadas.

Recomendación: sugerimos que se documente la realización de las siguientes actividades después de que ha ocurrido algún desastre:

- Determinar la causa del daño.
- Evaluar la magnitud del daño que se ha producido.
- Que sistemas se han afectado.

- Qué modificaciones de emergencia se han realizado.
- Que equipos han quedado no operativos,
- Cuales se pueden recuperar y en cuanto tiempo.

Se debería actualizar la documentación del centro de cómputos con las modificaciones implementadas y las acciones correctivas que se llevaron a cabo como consecuencia del incidente.

- ❖ **Debilidad:** Una vez ocurrido el siniestro, el administrador del sistema realiza las actividades de recuperación sin respaldarse en un plan o manual formal de procedimientos.

Efectos: al no tener una guía es muy probable que se cometan errores u omisiones en las acciones de restablecimiento.

Recomendación: se debería asignar el papel de coordinador a un empleado, que se encargará de las operaciones necesarias para que el sistema funcione correctamente después de la emergencia. Ésta persona debería determinar las acciones a seguir de acuerdo al tipo de emergencia que ha ocurrido, basándose en el plan de emergencias. Un ejemplo de acciones principales a seguir en el caso de la caída del sistema serían:

- Setup e instalación de los componentes de hardware necesarios.
- Carga del software del sistema.
- Instalación del software de aplicación.
- Provisión de los datos necesarios (backup), incluyendo archivos de configuración.
- Re-arrancar el equipo.
- Se debe asegurar que se empieza a auditar una vez que se reinicia.

- ❖ **Debilidad:** debido a que no hay implementado un plan de acción en caso de desastres, no se realiza una retroalimentación con los datos obtenidos luego de una emergencia.

Efectos: si no se aprende del resultado de estas acciones, no será posible evitar la misma contingencia en el futuro ni mejorar la eficacia de las directivas.

Recomendación: se debería tener en cuenta la experiencia que se obtiene luego de una contingencia para retroalimentar el plan, y así obtener uno de mayor eficiencia. Esto se logra generando una lista de recomendaciones para minimizar los riesgos de futuros incidentes similares. En base a la experiencia obtenida, evaluar:

- El desempeño del personal inmerso en la emergencia, y reordenar la lista.
- Si algún elemento o tarea tenía asignada una prioridad que no le correspondía, se deberían modificar estas prioridades.
- La introducción de actividades que no se contemplaron en el plan de emergencia.
- La generación de sugerencias y posibles mejoras.

CONCLUSIÓN

El equipo de auditoría concluye que el estado de la seguridad de la información en la organización puede denominarse como

FAVORABLE CON SALVEDADE

Considerando los elementos de juicio obtenidos durante las tareas efectuadas, se ha determinado que si bien existen prácticas tendientes a garantizar un adecuado nivel de seguridad del sistema informático y de comunicaciones, las mismas no son suficientes ni se encuentran ordenadas en un cuerpo normativo.

Atento a las debilidades mencionadas anteriormente, la organización debe analizar la situación planteada a los efectos de determinar si corresponde la iniciación de acciones pertinentes.

Llevar a cabo las recomendaciones expuestas permitirá:

- ~ Reducir el ambiente de riesgo vigente,
- ~ Disponer de las medidas de control interno necesarias,
- ~ Disminuir el grado de exposición de los sistemas que se procesan,
- ~ Incrementar la confiabilidad, integridad y disponibilidad de la información,
- ~ Y optimizar los procesos orientados al cumplimiento de los objetivos de la empresa.

En este sentido, las medidas sugeridas para corregir las debilidades relevadas deberán analizarse a la luz del estudio de riesgos² a fin de conseguir disminuir el riesgo actual a su nivel mínimo.

En otro orden, consideramos necesario destacar la buena predisposición y colaboración puesta de manifiesto por el personal de la empresa durante la auditoría.

Córdoba, Octubre de 2002

² Anexo I: Análisis de riesgo.

PLAN DE SEGURIDAD INFORMÁTICA

El propósito de establecer este Plan de Seguridad Informática para La Empresa S.A. es proteger la información y los activos de la organización, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que debe asumir cada uno de los empleados mientras permanezcan en la organización.

Estas políticas emergen como el instrumento para concienciar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de tal forma que permitan a la empresa cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso de la institución, agudeza técnica para establecer fallas y deficiencias, y constancia para renovar y actualizar dicha política en función de un ambiente dinámico.

LA EMPRESA S.A.**PLAN DE SEGURIDAD INFORMÁTICA****OBJETIVO GENERAL**

El objetivo general consiste en la realización de un **Plan de Seguridad Informática** para **La Empresa S.A.**, en donde se definen los lineamientos para promover la planeación, el diseño e implantación de un modelo de seguridad en la misma con el fin de establecer una cultura de la seguridad en la organización. Asimismo, la obliga a redactar sus propios procedimientos de seguridad, los cuales deben estar enmarcados por este plan.

ANTECEDENTES

A iniciativa de la Gerencia de La Empresa S.A., se llevó a cabo una **Auditoría de Seguridad** y con base en ella, se establece la presente política.

ALCANCE

Este documento se aplica para todos los empleados de La Empresa S.A., así como a los proveedores y personal externo que desempeñen labores o le proporcionen algún tipo de servicio o producto.

VIGENCIA

El presente Plan de Seguridad Informática es de aplicación a partir del 1 de noviembre de 2002.

AUTORIDAD DE EMISIÓN

Este documento es emitido por alumnos de la Universidad Católica de Córdoba a ser presentado como Trabajo Final de la carrera de Ingeniería de Sistemas.

CONTENIDO

Este Plan presenta las **Políticas de Seguridad Informática** cuyo contenido se agrupa en los siguientes aspectos:

1. Seguridad Lógica.
2. Seguridad en las Comunicaciones.
3. Seguridad de las Aplicaciones.
4. Seguridad Física.

5. Administración del Centro de Cómputos.
6. Auditorías y Revisiones.
7. Plan de Contingencia.

DESARROLLO

En este Plan de Seguridad Informática se desarrollan normas y procedimientos que pautan las actividades relacionadas con la seguridad informática y la tecnología de información. Este deberá ser aprobado por los directivos de La Empresa S.A. para su implantación.

Estas políticas de seguridad informática y las medidas de seguridad en ellas especificadas deben ser revisadas periódicamente, analizando la necesidad de cambios o adaptaciones para cubrir los riesgos existentes y auditando su cumplimiento.

1- SEGURIDAD LÓGICA

1.1 IDENTIFICACIÓN – ID’S

- Deberá existir una herramienta para la administración y el control de acceso a los datos. Debe existir una **política formal de control de acceso** a datos donde se detalle como mínimo:
 - el nivel de confidencialidad de los datos y su sensibilidad,
 - los procedimientos de otorgamiento de claves de usuarios para el ingreso a los sistemas,
 - los estándares fijados para la identificación y la autenticación de usuarios.
- Para **dar de alta un usuario** al sistema debe existir un procedimiento formal, por escrito, que regule y exija el ingreso de los siguientes datos:
 - identificación del usuario, deberá ser única e irrepetible,
 - password, debe ser personal e ingresado por el usuario,
 - nombre y apellido completo,
 - sucursal de la empresa donde trabaja,
 - grupo de usuarios al que pertenece,
 - fecha de expiración del password,
 - fecha de anulación de la cuenta,
 - contador de intentos fallidos,
 - autorización de imprimir,
 - autorización de ingreso al área de usados.
- Deben asignarse los **permisos mínimos** y necesarios para que cada usuario desempeñe su tarea.
- Debe existir una manera de **auditar (lista de control de acceso)** todos los requerimientos de accesos y los datos que fueron modificados por cada usuario, y si este tiene los permisos necesarios para hacerlo.
- Deberá restringirse el acceso al sistema o la utilización de recursos en un **rango horario definido**, teniendo en cuenta que:
 - las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan,
 - durante las vacaciones o licencias las cuentas de usuarios deben desactivarse,
 - en días feriados las cuentas de usuarios administrativos, a excepción de los del departamento de ventas, deben permanecer desactivadas.
- Deben restringirse las conexiones de los usuarios sólo a las **estaciones físicas autorizadas**.

- El **administrador debe poder logearse** solamente desde las terminales que se encuentren en el centro de cómputos y en una terminal específica y habilitada por cada sucursal.
- El administrador del sistema deberá realizar un **chequero mensual de los usuarios** del sistema, comprobando que existen solo los usuarios que son necesarios y que sus permisos sean los correctos.
- El área de recursos humanos deberá comunicar al administrador los **cambios de personal** que se produzcan.
- Para **dar de baja un usuario** deberá existir un procedimiento formal por escrito, a través del cual los datos del usuario no se eliminarán sino que se actualizará la fecha de anulación de su cuenta, quedando estos datos registrados en el histórico.
- Además, se debe llevar a cabo una **política de desvinculación del personal**, a través de la cual se quitan permisos al empleado paulatinamente, evitando un posible acto de vandalismo por insatisfacción con la decisión de la Empresa.
- El sistema deberá **finalizar toda sesión interactiva** cuando la terminal desde donde se esté ejecutando no verifique uso durante un período de cinco minutos, deberá desloguear al usuario y limpiar la pantalla.
- Las PC's deben tener instalado un **protector de pantalla con contraseña**.
- Se debe bloquear el perfil de todo usuario que **no haya accedido al sistema** durante un período razonable de tiempo a determinar por el Directorio.
- Los usuarios del sistema solamente podrán abrir **una sesión de cada aplicación**, y no podrán abrir dos sesiones del mismo menú en diferentes terminales ni en la misma terminal.
- Se deberá impedir la existencia de **perfiles de usuarios genéricos**, en todos los sistemas operativos y en el sistema informático de la Empresa.
- Se deberá minimizar la generación y el uso de perfiles de **usuario con máximos privilegios**. Todos los usos de estas clases de perfiles deberán ser registrados y revisados por el administrador de seguridad.
- Deberá existir un **administrador total del sistema** (root), que deberá estar resguardado en un sobre cerrado bajo adecuadas normas de seguridad. En caso que sea necesaria su utilización se deberá proceder de acuerdo con un procedimiento de autorización estipulado a tal fin.
- Un **segundo** administrador (un súper-usuario) debe ser creado con privilegios similares al anterior. Se creará un **tercer** perfil de administrador del sistema, con los permisos mínimos necesarios para la realización de tareas cotidianas del administrador. Ninguno de estos usuarios tendrá permitida la eliminación del usuario root.

- Los administradores que realizan tareas de mantenimiento, deberán tener otro perfil, con un nivel de acceso menor, denominado **mantenimiento**, para ser utilizado en tareas cotidianas que no requieran privilegios de súper usuario.
- Si se realiza **mantenimiento externo**, deberá crearse una cuenta de usuario especial para esta tarea, con los permisos mínimos necesarios para desempeñar las funciones; una vez finalizado el mantenimiento el administrador del sistema deberá modificar la contraseña de esta cuenta. Cada vez que sea necesario realizar mantenimiento, el administrador deberá proporcionar esta clave al personal externo.
- Periódicamente el administrador del sistema deberá **chequear** las acciones desempeñadas con las cuentas de administradores y de mantenimiento.

1.2 AUTENTICACIÓN

- La **pantalla de logeo** del sistema deberá mostrar los siguientes datos:
 - nombre de usuario,
 - password,
 - opción para cambiar la clave.
- Mientras el usuario está **ingresando su contraseña**, esta no debe ser mostrada por pantalla.
- Cuando el **usuario logra logearse** al sistema deberán mostrarse los siguientes datos:
 - nombre de usuario,
 - fecha y hora de la última conexión,
 - localización de la última conexión (Ej. número de terminal),
 - cantidad de intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.
- La **aplicación para administrar los datos de usuarios** solo deberá ejecutarse en máquinas designadas del centro de cómputos.
- Deberán **encriptarse**:
 - la lista de control de accesos,
 - los passwords y datos de las cuentas de usuarios,
 - los datos de autenticación de los usuarios mientras son transmitidos a través de la red.

1.3 PASSWORD

- Los passwords deberán tener las siguientes **características**:
 - conjunto de caracteres alfa-numérico,
 - longitud mínima de 6 y máxima de 10 caracteres.
- El password deberá **inicializarse como expirado** para obligar el cambio.

- La **fecha de expiración** del password deberá ser de cuatro meses. El sistema exigirá automáticamente el cambio, una vez cumplido el plazo.
- El password **no deberá contener** el nombre de la empresa, el nombre del usuario, ni palabras reservadas.
- Bloquear el perfil de todo usuario que haya intentado **acceder al sistema en forma fallida** por más de **cinco** veces consecutivas.
- El usuario debe poder **modificar su password** cuantas veces considere necesario, sin seguir ningún procedimiento formal de aviso.
- Controlar que el password ingresado sea **diferente a los últimos cinco utilizados**.
- El password deberá tener un **período de duración mínimo** de 5 días. El sistema no permitirá el cambio de password si este período no se ha cumplido.
- Si un usuario **olvida el password**, la aplicación no deberá mostrarle el password al administrador, y permitirá que el usuario ingrese uno nuevo desde su terminal, la próxima vez que intente logearse.

1.4 SEGREGACIÓN DE FUNCIONES

- Debe existir una adecuada y documentada **separación de funciones** dentro del centro de cómputos.
- El área de sistemas debe encontrarse ubicada en el **organigrama** de la empresa en una posición tal que garantice la independencia necesaria respecto de las áreas usuarias.
- Deberá realizarse una **rotación en las tareas del personal** del centro de cómputos para controlar el desempeño que los empleados han tenido durante un período de tiempo. Para esto se deberán establecer períodos de vacaciones anuales obligatorios para el personal del área, entre otras medidas.

2- SEGURIDAD DE COMUNICACIONES

2.1 TOPOLOGÍA DE RED

- Se deberá asegurar la **integridad, exactitud, disponibilidad y confidencialidad** de los datos transmitidos, ya sea a través de los dispositivos de hardware, de los protocolos de transmisión, o de los controles aplicativos.
- Deberá existir **documentación** detallada sobre los diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos.
- Deberán existir **medios alternativos de transmisión** en caso de que alguna contingencia afecte al medio primario de comunicación.

2.2 CONEXIONES EXTERNAS

- Asegurar la definición e implementación de procedimientos pertinentes para el **control de las actividades de usuarios externos** del organismo a fin de garantizar la adecuada protección de los bienes de información de la organización.
- La conectividad a Internet será otorgada para propósitos relacionados con el negocio y mediante una **autorización de la Gerencia**. Los usuarios no autorizados deberán estar imposibilitados de conectarse al exterior.
- Los usuarios de la organización que utilicen Internet deben recibir **capacitación específica** respecto a su funcionalidad y a los riesgos y medidas de seguridad pertinentes.
- Debe asegurarse que la totalidad del tráfico entrante y saliente de la red interna, sea filtrado y controlado por un **firewall** prohibiendo el pasaje de todo el tráfico que no se encuentre expresamente autorizado.
- Todas las conexiones a Internet de la empresa deben traspasar un servidor **Proxy** una vez que han traspasado el firewall.
- Deben documentarse los **servicios provistos** a través de Internet y definirse las responsabilidades en cuanto a su administración. No se publicarán en Internet datos referidos a las cuentas de correo de los empleados, deberán exhibir cuentas especiales asignadas a cada área de la empresa.
- Cada vez que se establezca una vía de comunicación con **terceros** (personal de mantenimiento externo, fábricas, proveedor de servicios de Internet, etc.), los mecanismos de transmisión y las responsabilidades de las partes deberán fijarse por escrito.

- La información enviada a través de equipos de comunicaciones de la empresa se considera **privada**. Cabe aclarar que la información no es pública, a menos que en forma expresa se indique lo contrario.
- El uso de Internet debe ser **monitoreado** periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada, la compañía puede revisar el contenido de las comunicaciones de Internet.
- El acceso casual a los mensajes de correo electrónico por los administradores y similares, se considera una violación a la política de seguridad de la información. Sin embargo, la Gerencia tiene el **derecho de examinar** cualquier información, sin previo consentimiento o notificación del empleado, en caso que se considere que se está utilizando inadecuadamente el equipamiento de la compañía.
- De ser necesario realizar **mantenimiento remoto** a los servidores, se utilizarán protocolos y servicios de comunicación que garanticen la seguridad de los datos que se transmiten a través de la red, utilizando encriptación. Deberán documentarse cada una de las actividades que el personal externo realice sobre los equipos utilizando acceso remoto. Para llevar a cabo estas tareas, el encargado del mantenimiento deberá solicitar formalmente la dirección IP del servidor de Internet y el password de la cuenta de mantenimiento al administrador del centro de cómputos.

2.3 CONFIGURACIÓN LÓGICA DE RED

- El riesgo aumenta con el número de conexiones a **redes externas**; por lo tanto, la conectividad debe ser la mínima necesaria para cumplir con los objetivos de la empresa.
- El esquema de direcciones de la **red interna** no debe ser visible ante las conexiones externas.
- Deberá asegurarse que la **dirección IP** de la empresa sea un número variable y confidencial.
- Los **recursos lógicos** o físicos de los distintos **puestos de trabajo** no deben ser visibles en el resto de la red informática. Los recursos de los **servidores** serán visibles solo en los casos necesarios y con las medidas de seguridad correspondientes.
- Deben tomarse los recaudos necesarios para restringir todo tipo de aplicaciones que no ayudan al cumplimiento de los objetivos de la organización, tales como herramientas de **chateo** o **“file sharing”**.

2.4 MAIL

- La Gerencia determinará que empleados deben contar con una **cuenta** de correo electrónico, según lo amerite su tarea.

- Deberá existir un **procedimiento** formal para dar de alta y de baja las cuentas de correo electrónico en el sistema informático.
- La empresa deberá contar con un sistema de **mail externo y uno interno**, con diferentes dominios. De esta manera, las comunicaciones entre el personal de la empresa se realizarán sin exponer los mensajes a Internet.
- Los **aplicativos** de correo electrónico deben brindar las condiciones de seguridad necesarias para evitar los virus informáticos o la ejecución de código malicioso, deben brindar la facilidad de impedir que un usuario reciba correos de un remitente riesgoso para los recursos de la empresa.
- Todas las cuentas de correo que pertenezcan a la empresa deben estar gestionadas por una misma aplicación. Esta debe asociar una cuenta de correo a una **PC en particular** de la red interna.
- El administrador de mail no debe ser utilizado para enviar correo basura (**SPAM**).
- Los mensajes de correo electrónico deben ser considerados como **documentos formales** y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
- El correo electrónico no debe ser utilizado para enviar **cadenas de mensajes**, no debe relacionarse con actividades ilegales y no éticas o para mensajes no relacionados con los propósitos de la empresa.
- Los datos que se consideraron “confidenciales” o “críticos” deben **encriptarse**.
- Debe existir un procedimiento de **priorización** de mensajes, de manera que los correos electrónicos de prioridad alta sean **resguardados**.
- Deberá asignarse una **capacidad de almacenamiento** fija par cada una de las cuentas de correo electrónico de los empleados.

2.5 ANTIVIRUS

- En todos los **equipos** de la empresa debe existir una herramienta antivirus ejecutándose permanentemente y en continua actualización.
- Deberá utilizarse más de una herramienta antivirus en los **servidores**, para así disminuir el riesgo de infección.
- Deberán existir **discos de rescate** de los antivirus, tanto para los servidores como para los puestos de trabajo, que sean capaces de realizar escaneos de virus a bajo nivel y restaurar los sistemas.
- La **actualización** de los antivirus de todos los equipos de la empresa deberá realizarse a través de un procedimiento formal y, si es posible, automático, a cargo de un empleado del centro de cómputos designado por el administrador.

- Deberán programarse **escaneos** periódicos de virus en todos los equipos de la empresa; esta tarea estará a cargo de personal designado por el administrador del centro de cómputos.
- Deberá existir un **procedimiento formal** a seguir en caso que se detecte un virus en algún equipo del sistema.

2.6 FIREWALL

- El firewall de la empresa debe presentar una postura de negación preestablecida, configurado de manera que se prohíban todos los **protocolos y servicios**, habilitando los necesarios.
- Los servicios o protocolos que solo sean necesarios esporádicamente deberán habilitarse **on demand**. Aquellos que sean considerados riesgosos deberán habilitarse bajo estrictas limitaciones de uso, considerando el equipo desde el que se utilizará, hacia qué destino, las fechas y los horarios para dichas conexiones. A modo de ejemplo, esto puede aplicarse a la utilización del protocolo FTP para la comunicación con las fábricas.
- El **encargado de mantenimiento** debe controlar periódicamente la configuración del firewall y los servicios de red, documentando los resultados de dichas pruebas.
- De haber una falla en el firewall, debe ser una “**falla segura**”, lo que significa que todos los accesos al servidor de Internet deben bloquearse.

2.7 ATAQUES DE RED

- Toda la información que se considere confidencial deberá **encriptarse** durante la transmisión, o viajar en formato no legible.
- Deben existir **procedimientos** formalmente documentados destinados a prevenir los ataques de red más frecuentes.
- Se deberá usar algún sistema de detección de intrusos (**IDS**), tolerantes al fallo, utilizando los mínimos recursos posibles.
- Deberá utilizarse una herramienta que monitoree la red, con el fin de evitar el ataque de denegación de servicio (**DoS**).
- Para disminuir el riesgo de **sniffing**, la red de la empresa deberá segmentarse física y/o lógicamente.
- Con el fin de disminuir la posibilidad de **spoofing** el firewall deberá denegar el acceso a cualquier tráfico de red externo que posea una dirección fuente que debería estar en el interior de la red interna.
- Los **archivos de passwords** y datos de usuarios no deberán almacenarse en el directorio por default destinado a tal fin. Además deberán estar encriptados

utilizando encriptación en un solo sentido (“one way”), con estrictos controles de acceso lógico, de manera de disminuir la posibilidad de ataques.

3- SEGURIDAD DE LAS APLICACIONES

3.1 SOFTWARE

- El **sistema operativo** de los servidores deberá presentar las siguientes características:
 - alta confiabilidad,
 - equilibrio en costo y beneficio,
 - compatibilidad e interoperatividad con los sistemas operativos de las PC's y demás sistemas usados en la empresa,
 - escalabilidad,
 - disponibilidad de software de aplicación y actualizaciones,
 - buena administración y generación de logs,
 - buena performance,
 - cumplir con los requerimientos funcionales impuestos por la empresa,
 - amigable con el usuario,
 - disponibilidad de documentación.
- Además deberá presentar las siguientes características en lo relativo a la **seguridad**:
 - identificación y autenticación,
 - control de acceso,
 - login,
 - incorruptibilidad,
 - fiabilidad,
 - seguridad en la transmisión,
 - backup de datos,
 - encriptación,
 - funciones para preservar la integridad de datos,
 - requerimientos sobre privacidad de datos.

3.2 SEGURIDAD DE BASES DE DATOS

- El administrador de sistemas deberá confeccionar un **Plan de Migración** desde archivos indexados a bases de datos relacionales, una vez que el sistema esté desarrollado en su totalidad.
- Los archivos indexados de la empresa, las carpetas donde se encuentran almacenados y las aplicaciones que los administran deberán tener **controles de acceso**, de forma tal que la única persona que pueda tener acceso a estos recursos sea el administrador del centro de cómputos.
- Debe existir una aplicación que registre las siguientes **ocurrencias**:

- tiempo y duración de los usuarios en el sistema,
 - número de conexiones a bases de datos,
 - número de intentos fallidos de conexiones a bases de datos,
 - ocurrencias de deadlock con la base de datos,
 - estadísticas de entrada-salida para cada usuario,
 - generación de nuevos objetos de bases de datos,
 - modificación de datos.
- Deberán hacerse **chequeos regulares** de la seguridad de la base de datos, en los que se deberá verificar que:
 - se hacen y son efectivos los backups y los mecanismos de seguridad,
 - no haya usuarios de la base de datos que no tengan asignado una contraseña,
 - se revisen los perfiles de los usuarios que no han usado la base de datos por un período largo de tiempo,
 - nadie, además del administrador de datos, ha accedido a los archivos del software de base de datos y ha ejecutado un editor de archivos indexados,
 - solo el administrador de datos tiene acceso de lectura y escritura en los archivos de programa,
 - la base de datos y las aplicaciones que la administran tiene suficientes recursos libres para trabajar eficientemente.
- Deben mantenerse registros de todas las transacciones realizadas en la base de datos, de manera que éstas puedan revertirse en caso de surgir un problema. Los registros de la base de datos **no se borrarán** físicamente, sino que deberán marcarse como eliminados.
- Deberá existir una **clasificación de los datos** en base a su sensibilidad para definirlos como críticos y así determinar controles específicos. Se deberán definir tres niveles de información:
 - Crítica:
 - ~ la no-disponibilidad de esta información ocasiona un daño en los activos de la empresa;
 - ~ se considera recurso crítico a aquel recurso interno que debe estar disponible solamente para un conjunto determinado de personas, debe ponerse un cuidado especial en información que por ley o que por políticas de la empresa debe permanecer confidencial; la clasificación de un recurso como crítico deberá incluir los criterios para determinar quienes tienen acceso a él. De ser necesaria su transmisión por redes externas o su almacenamiento en sistemas de la red perímetro, deberán tomarse medidas de seguridad extremas, la información deberá encriptarse;
 - Confidencial:
 - ~ en poder de personas no autorizadas compromete los intereses de la empresa;

- ~ Se considera recurso confidencial a todo aquel que solo deberá utilizarse y ser del conocimiento de miembros de la empresa y por defecto todo aquel recurso que no haya sido explícitamente clasificado como disponible al público;
- Pública:
 - ~ información de libre circulación;
 - ~ se considera recurso disponible al público aquel que no requiere permanecer como de uso interno y que explícitamente se ha clasificado como un recurso público.

Esta clasificación deberá ser documentada e informada a todo el personal de la organización, y deberá evaluarse y actualizarse periódicamente.

- Deberá existir un **responsable** en cada área de la empresa, que responda por la información que se maneja en dicho sector. Deberá definir la clasificación de los datos y los controles de acceso que son necesarios, junto con el administrador del sistema.

3.3 CONTROL DE APLICACIONES EN PC'S

- Deberán existir **estándares de configuración** de los puestos de trabajo, servidores y demás equipos de la red informática.
- En base al estándar se deberá generar un **procedimiento** donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.
- Las **aplicaciones solo se actualizarán** debido al reporte de algún mal funcionamiento o a un nuevo requerimiento por parte de los usuarios o del personal del centro de cómputos.
- Antes de hacer un cambio en la configuración de los servidores se deberá hacer un **backup de la configuración existente**. Una vez que el cambio ha resultado satisfactorio deberá almacenarse la configuración modificada.
- Se deberá establecer un **procedimiento de emergencia** para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores en el caso de generarse problemas.
- Se deberán **documentar** no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se les realicen. Deberán generarse historiales y así calcular datos estadísticos de los cambios realizados y los errores reportados.
- En el momento en que un nuevo usuario ingrese a la empresa, se lo deberá **notificar y deberá aceptar** que tiene prohibida la instalación de cualquier producto de software en los equipos.
- Se deberán realizar **chequeos periódicos** en las PC's, los servidores y demás equipos, en búsqueda de aplicaciones instaladas no autorizadas o innecesarias.

3.4 CONTROL DE DATOS EN LAS APLICACIONES

- Los **datos de entrada y salida** del sistema deberán poseer controles donde se verifique su integridad, exactitud y validez.
- Los datos de salida del sistema de la empresa deben restringirse con **controles lógicos**, de acuerdo a los permisos de acceso.
- Deberán protegerse con **controles de acceso** las **carpetas** que almacenen los archivos de las aplicaciones, y solo el administrador de sistemas tendrá acceso a ellas.
- Se deberá utilizar un programa de **sincronización horaria** en todo el entorno de red, para asegurar la consistencia de los datos de las aplicaciones.

3.5 CICLO DE VIDA

- Deberá utilizarse un **plan detallado de sistemas**, donde se definan las asignaciones de recursos, el establecimiento de prioridades y responsabilidades, la administración de tiempos y la utilización de métricas de software. Esta norma deberá aplicarse tanto para el desarrollo de las aplicaciones como para las modificaciones que se realicen.
- Antes de realizar alguna modificación en el sistema, deberá realizarse un **análisis del impacto** de este cambio.
- Se deberá implementar una **gestión de configuración**, y deberán documentarse los cambios desarrollados en las aplicaciones.
- Deberá existir un **documento formal de solicitud de cambios**, donde quede reflejado el motivo y la solicitud del cambio, allí se agregarán los requerimientos de seguridad necesarios, definidos por el responsable de la información y el administrador de sistemas. La documentación de los cambios debe incluir:
 - sistema que afecta,
 - fecha de la modificación,
 - desarrollador que realizó el cambio,
 - empleado que solicitó el cambio,
 - descripción global de la modificación.
- El formulario anterior se utilizará para actualizar la **documentación del desarrollo** y de los distintos manuales generados.
- Deberán realizarse **pruebas del software** desarrollado, para esto se generarán planes y escenarios de prueba y se documentarán los resultados.
- Todo nuevo desarrollo o modificación deber estar **probado y aprobado** por los usuarios del mismo antes de su instalación en el ambiente de trabajo.

- La metodología para el desarrollo y mantenimiento de sistemas debe contemplar una **revisión de post-implantación** del sistema en operación, que deberá determinar si se han logrado los objetivos previstos, y si se ha alcanzado la satisfacción de las necesidades planteadas por los usuarios.
- Se deberá informar por escrito la importancia de la seguridad de la información a todo el personal contratado, **terceros** y consultores. El administrador del centro de cómputos, junto con los directivos, serán quienes:
 - especifiquen los requerimientos de seguridad,
 - determinen los pasos a seguir en caso que no se respete lo establecido en el contrato,
 - establezcan cláusulas sobre confidencialidad de la información,
 - exijan al tercero en cuestión que informe posibles brechas de seguridad existentes.
- Los **contratos con terceros** deberán contener una cláusula que indique “Derecho de auditar el desempeño del contratado”.
- Con respecto a la contratación de terceros para el desarrollo de aplicaciones, éste deberá **entregar** a la empresa:
 - aplicación ejecutable,
 - código fuente de la aplicación,
 - documentación del desarrollo,
 - manuales de uso.
- Antes de realizar la **compra** de una aplicación de software, deberá:
 - realizarse un análisis de costo – beneficio,
 - comprobar la adaptabilidad a los sistemas existentes en la empresa,
 - verificar la compatibilidad con los sistemas operativos de la empresa,
 - evaluar las medidas de seguridad que posee,
 - asegurar un servicio post-venta apropiado,
 - solicitar la misma documentación que se exige a los terceros.

4- SEGURIDAD FÍSICA

4.1 EQUIPAMIENTO

- Deberá existir una adecuada protección física y mantenimiento permanente de los equipos e instalaciones que conforman los activos de la empresa.

4.2 CONTROL DE ACCESO FÍSICO AL CENTRO DE CÓMPUTOS

- Se deberá restringir el acceso físico a las **áreas críticas** a toda persona no autorizada, para reducir el riesgo de accidentes y actividades fraudulentas.
- Se deberá asegurar que todos los **individuos** que entren a áreas restringidas se identifiquen y sean autenticados y autorizados para entrar.
- Cualquier **persona ajena a la empresa** que necesite ingresar al centro de cómputos deberá anunciarse en la puerta de entrada, personal de sistemas designado deberá escoltarlo desde la puerta hacia el interior del edificio, acompañándolo durante el transcurso de su tarea, hasta que éste concluya.
- Se deberán utilizar **sistemas de monitoreo** automáticos o manuales, que controlen el centro de cómputos y su ingreso constantemente.
- El **área del centro de cómputos** donde se encuentran los servidores, el switch central y demás equipamiento crítico solo debe tener permitido el acceso a los administradores.
- El personal de los centros de procesamiento así como el personal contratado sólo podrá permanecer en las instalaciones de las empresas durante el **horario autorizado**. Se deberá establecer un procedimiento de autorización para el personal que deba permanecer fuera de su horario habitual de trabajo.
- Deberán existir **guardias de seguridad** en permanente monitorización, durante el horario laboral. Se deberán ubicar en el exterior y el interior de la empresa.
- Se debe realizar un adecuado mantenimiento y **prueba de los procedimientos** para la restricción de acceso físico, así como de los dispositivos de seguridad para la prevención, detección y extinción del fuego.

4.3 CONTROL DE ACCESO A EQUIPOS

- Las **disqueteras y lectoras de CD** deberán deshabilitarse en aquellas máquinas en que no se necesiten.
- Las PC's de la empresa deberán tener un password de administrador en el **BIOS**, que deberá gestionar el administrador del sistema.

- Los servidores deberán tener una **llave de bloqueo** de hardware.
- Cualquier **dispositivo externo** que no se encuentre en uso, deberá permanecer guardado bajo llave dentro del centro de cómputos.
- Los **gabinetes** donde se ubican los switches de cada una de las sucursales, deberán permanecer guardados bajo llave, y fuera del alcance de personal no autorizado.
- El administrador o algún encargado de cómputos designado por él, deberá realizar **chequeos periódicos** para comprobar:
 - la correcta instalación de los dispositivos de los equipos,
 - su buen funcionamiento,
 - sus números de series corresponden con los datos registrados por el administrador al momento de la instalación.
- Los **servidores deberán apagarse** automáticamente una vez que han cerrado todas las sucursales de la empresa.

4.4 DISPOSITIVOS DE SOPORTE

- Deberán existir los siguientes **dispositivos de soporte** en la empresa:
 - **Aire acondicionado y Calefacción:** en el centro de cómputos la temperatura debe mantenerse entre 19° C y 20° C.
 - **Matafuegos:** deberán ser dispositivos químicos y manuales que cumplan las especificaciones para extinguir incendios en equipos eléctricos de computación,
 - ~ deberán estar instalados en lugares estratégicos de la empresa,
 - ~ el centro de cómputos deberá contar con uno propio ubicado en la habitación de los servidores.
 - **Alarmas contra intrusos:** deberán contar con una alarma que se active en horarios no comerciales. Ésta deberá poder activarse manualmente en horarios laborales ante una emergencia.
 - **Generador de energía:** deberá existir un generador de energía que se pondrá en marcha cada vez que haya problemas con el suministro de energía eléctrica o avisos de cortes de luz.
 - **UPS:** (Uninterruptible power supply) deberá existir al menos un UPS en el centro de cómputos que atienda a los servidores, con tiempo suficiente para que se apaguen de forma segura.
 - **Luz de emergencia:** deberá existir una luz de emergencia que se active automáticamente ante una contingencia.
 - **Estabilizador de tensión:** deberá existir al menos un estabilizador de tensión que atienda la línea de energía eléctrica independiente del centro de cómputos.
 - **Descarga a tierra:** deberán existir métodos de descarga a tierra para el edificio y otra independiente para el centro de cómputos.

- Todos estos dispositivos deberán ser **evaluados periódicamente** por personal de mantenimiento.
- Deberá existir una **llave de corte de energía general** en la salida de emergencias del edificio.
- Deberán existir procedimientos detallados a seguir por el personal en **caso de emergencias**, indicando responsables, quiénes deben estar adecuadamente capacitados.

4.5 ESTRUCTURA DEL EDIFICIO

- El centro de cómputos deberá ubicarse en un **piso superior** del edificio. Debe tener protecciones contra ruidos e interferencias electromagnéticas y visuales.
- Todas las **salidas hacia el exterior** del centro de cómputos deberán estar protegidas con rejas y métodos que impidan la visión.
- En el diseño del centro de cómputos deberá tenerse en cuenta el **futuro crecimiento** de la empresa, permitiendo la expansión del mismo y predisponiéndolo a reinstalaciones, conservando siempre recursos redundantes.
- Los **sectores** de la empresa deberán estar divididos entre sí, con un medio que restrinja la visión.

4.6 CABLEADO ESTRUCTURADO

- El cableado debe seguir las normas del **cableado estructurado**, que garantizan el funcionamiento eficiente de la red.
- Si el tendido del cableado se **terceriza**, la empresa encargada debe prestar garantías escritas sobre su trabajo.
- Se deberá **documentar** en planos los canales de tendidos de cables y las bocas de red existentes.
- Debe existir tendido de **cableado redundante** para futuros puestos de trabajo. Estos cables no deben tener bocas de red instaladas.
- Deberá medirse periódicamente el **nivel de interferencia** que existe en la red. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.
- Deberá medirse periódicamente **nivel de ancho de banda** de red ocupado. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.
- En el caso de ocurrir esta contingencia con la continuidad del servicio de red, deberá existir un **sistema informático off line** para los sectores críticos de la empresa.

- Deberá existir un **procedimiento manual** de respaldo para realizar las tareas cotidianas.
- Ante un **corte del suministro de energía** eléctrica deberán apagarse los equipos del centro de cómputos de forma segura, como medida de prevención.

5- ADMINISTRACIÓN DEL CPD

5.1 ADMINISTRACIÓN DEL CPD

- La empresa deberá asegurar la correcta **organización y administración** del área de sistemas a fin de que ésta brinde condiciones generales de operación que posibiliten un ambiente adecuado de control.
- Se deberá designar en la dirección del área un **profesional** que acredite experiencia en el manejo de los recursos informáticos y comprenda los riesgos y problemas relativos a la tecnología y sistemas de información. Es su obligación y responsabilidad el mantener seguros los sistemas que operan.
- Deberá designarse un **encargado de la seguridad** del sistema, que coordine las tareas correspondientes, haciendo cumplir las políticas de seguridad en toda la empresa.
- Deberá existir una **planificación** formalizada y completa de las actividades que se desarrollan normalmente. Deberán designarse responsabilidades claras y documentadas para actividad.
- Deberá desarrollarse un plan de sistemas a **corto plazo**, con contenga un cronograma de las actividades, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un periodo de un año.
- Deberá desarrollarse de un plan estratégico a **largo plazo**, que contenga los proyectos principales y los cronogramas de su implementación, para un periodo de por lo menos 3 años.
- **Ambos planes** deben tener objetivos concordantes con los de la organización, y deben supervisarse continuamente permitiendo su actualización en caso de ser necesario.
- Deberán generarse **reportes** trimestrales dirigidos al Directorio de la empresa, informando sobre las actividades en el centro de cómputos, el progreso de los planes propuestos y el cumplimiento de las políticas impuestas.
- El equipo de sistemas debe hacer hincapié en la concienciación de todos los usuarios, generando una **cultura de la seguridad**, haciéndolos partícipes de las medidas de seguridad, tanto los usuarios actuales como los que se incorporen en el futuro. El proceso de concienciación debe ser renovado y transmitido a los usuarios en forma anual.
- Los usuarios solicitarán **asesoramiento** o servicios al centro de cómputos a través de mails, de manera que se genere un registro de los trabajos efectuados por los empleados del centro de cómputos y de las solicitudes de los empleados.

- Deberá implementarse un **buzón de sugerencias** donde los usuarios recomienden mejoras o realicen comentarios, expresando sus inquietudes.
- Deberá existir un procedimiento para realizar la **publicidad** de políticas, planes o normas de la empresa y sus modificaciones.
- Deberá existir un encargado de llevar a cabo el **mantenimiento preventivo** el equipamiento informático de la empresa, monitorizando, chequeando y auditando las PC's y demás dispositivos que conforman la red.
- Los administradores deberán informar en tiempo de **suspensiones** en el servicio necesarias por mantenimiento, especificando fecha, hora y duración de la suspensión.
- Deberá generarse un **inventario** detallado donde se describan los sistemas de información y de los equipos de cómputos utilizados en la organización. Deberá asignarse un responsable de mantenerlo actualizado y de realizar controles periódicos.
- Deberán existir procesos para **rotular**, manipular y dar de baja el equipamiento informático.
- Los **medios de instalación originales** del software deberán respaldarse y resguardarse adecuadamente, en caso de que no sean de solo lectura, siempre se mantendrán con las protecciones contra escritura que estén disponibles para el medio. En la medida de lo posible se evitará instalar el software directamente de los medios originales.
- Debe existir un procedimiento para controlar que en el organismo solamente se utilicen productos de **software** adquiridos por vías oficiales.

5.2 CAPACITACIÓN

- El **personal del centro de cómputos** debe mantenerse capacitado respecto de las tecnologías utilizadas en la organización.
- Debe **impartirse capacitación** a los usuarios finales a efectos de que puedan operar adecuadamente los recursos informáticos.
- El personal debe ser entrenado respecto al cumplimiento de lo especificado en la **política de seguridad** informática. Se debe entregar una copia de la misma a cada empleado.
- Se debe obtener un **compromiso firmado** por parte del personal respecto al cumplimiento de las medidas de seguridad definidas en la política de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad de las claves de acceso, la no-divulgación de información de la organización, el cuidado de los recursos, la utilización de software sin licencia y el reporte de situaciones anormales. Debe confirmarse este compromiso anualmente o cada vez que se produzcan cambios en las funciones asignadas al personal.

- Asegurar que los empleados reciban **capacitación continua** para desarrollar y mantener sus conocimientos competencia, habilidades y concienciación en materia de seguridad informática dentro del nivel requerido a fin de lograr un desempeño eficaz.

5.3 BACKUP

- Se deberá asegurar la existencia de un **procedimiento** aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la organización, donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.
- La **periodicidad** de la generación de los resguardos debe ser acorde a la criticidad de la información y la frecuencia de cambios.
- La **ubicación** de los backups debe contar con adecuadas medidas de seguridad, sin estar expuestos a las mismas contingencias que el centro de cómputos, es decir que deberán almacenarse en el exterior de la empresa, y ser transportados en un medio resistente que los proteja. Debe designarse un **responsable** y un suplente encargados de su custodia, y se generará un registro de los **movimientos** de estos medios.
- Los archivos de backup deben tener un **control de acceso** lógico de acuerdo a la sensibilidad de sus datos, además de contar con protección física.
- El administrador del centro de cómputos debe designar un **responsable** de la realización de las copias de seguridad y de su restauración, y un suplente de éste primero.
- El procedimiento de generación de backup deberá estar **automatizado** con alguna herramienta de generación de copias de respaldo de datos.
- Deberán realizarse chequeos para comprobar el funcionamiento correcto de los **medios externos** donde se realizan las copias de respaldo. Además debe existir una política de reemplazo de medios externos de almacenamiento de backups, de manera de sustituirlos antes de su degradación física, y deberán poseer rótulos identificatorios.
- Deberá existir un **procedimiento de recuperación** de copias de respaldo, donde se incluya la metodología a seguir y el responsable de la realización. Deberán realizarse **chequeos** para comprobar que los procedimientos de restauración son eficientes.
- Debe existir una **política de documentación** de copias de respaldo, donde se registren todos los datos necesarios para la gestión del procedimiento de backup. Se deberá llevar un **inventario** actualizado de las copias de respaldo.
- Deben generarse copias de respaldo de las **configuraciones de los servidores**, documentando las modificaciones realizadas para identificar las distintas versiones. Se deberá establecer un procedimiento de emergencia para dejar sin

efecto los cambios efectuados y poder recuperar las **versiones autorizadas anteriores**.

- No deberán utilizarse los **servidores** de la empresa como medios de almacenamiento de las copias de respaldo de ningún sistema.
- Se deberá generar una copia de respaldo de toda la **documentación** del centro de cómputos, incluyendo el hardware, el software, y el plan de contingencias, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento.

5.4 DOCUMENTACIÓN

- Deberá generarse un **soporte** de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en el centro de cómputos.
- Deberán existir una documentación y un registro de las **actividades** del centro de cómputos (procesos normales, eventuales y excepcionales) que se desarrollan diariamente, que incluya como mínimo el detalle de los procesos realizados.
- Deberá desarrollarse documentación detallada sobre el equipamiento informático, que consista en diagramas y distribución física de las instalaciones, **inventarios** de hardware y software, diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos. Esta documentación comprende tanto al centro de procesamiento de datos principal, como a los secundarios y las redes departamentales.
- Deberá existir un registro de los eventos, **errores** y problemas del hardware y el software utilizados en las operaciones de procesamiento de datos.
- La metodología para el **desarrollo** y mantenimiento de sistemas debe incluir estándares para la documentación de las aplicaciones y las actividades. Esta documentación deberá mantenerse actualizada y abarcar todas las fases del ciclo de vida del desarrollo de los sistemas.

6- AUDITORÍAS Y REVISIONES

6.1 CHEQUEOS DEL SISTEMA

- La empresa debe asegurar que los sistemas provean las herramientas necesarias para garantizar un correcto control y auditabilidad de forma de asegurar la integridad, exactitud y disponibilidad de la información. Para ello deben existir:
 - **Herramientas que registren** todos los eventos relacionados con la seguridad de la información procesada por los centros de cómputos de la empresa.
 - **Herramientas que analiza los registros** generando reportes, estadísticas, gráficos con relación a los datos recogidos, con distintas frecuencias (diarios, semanales, mensuales y anuales). Deberá tener la capacidad de generar alarmas teniendo en cuenta la severidad de los eventos acontecidos.
 - **Procedimientos de revisión** de los eventos registrados, a cargo de un empleado designado por el administrador, de forma de detectar anomalías y tomar las acciones correctivas necesarias.
- Se deberán **registrar**, mediante logs de auditoría, aquellos eventos relacionados con la seguridad de la información. Dichos registros deberán contener como mínimo:
 - fecha y hora del evento,
 - fuente (el componente que disparó el evento),
 - ID del evento (número único que identifica el evento),
 - equipo (máquina donde se generó el evento),
 - usuario involucrado,
 - descripción (acción efectuada y datos asociados con el evento).
- Se deberán registrar como mínimo los siguientes **eventos respecto a los servidores**:
 - los servicios de mail,
 - servicios de red,
 - configuración de los servidores,
 - utilización del CPU,
 - reinicio de servidores.
- Deberán **actualizarse continuamente las herramientas** de análisis de logs, asignándole la responsabilidad de esta tarea a una persona en particular.
- Deberá existir un proceso encargado de la **rotación y eliminación** de logs. Se deberá conservar esta información al menos durante tres meses.
- Deberán generarse **líneas de base** que contengan información sobre las PC's, los servidores y el sistema informático en su totalidad, con datos históricos obtenidos

de los registros de auditoría, que sirvan para el cálculo de estadísticas y la generación de reportes diarios, semanales, mensuales y anuales.

- Estas líneas de base deben ser **resguardadas** en medios de almacenamiento externo no reutilizables, antes de la eliminación de los logs.
- Deberán **actualizarse** las líneas de base cada vez que se modifique la configuración del sistema.
- Deben programarse **auditorías periódicas y chequeos aleatorios**, para controlar las áreas o funciones críticas con respecto a la seguridad de los datos de la empresa, documentando la ejecución y los resultados de dichas pruebas.
- Se deberán **analizar periódicamente** los siguientes eventos específicos como mínimo:
 - controles de acceso y permisos de los usuarios,
 - uso de recursos informáticos,
 - operaciones de borrado o modificación de objetos críticos,
 - intentos de ingreso al sistema fallidos.
- Se deberán **documentar** las revisiones y controles efectuados, y **comunicar** las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

6.2 RESPONSABILIDADES DE LOS ENCARGADOS DE SEGURIDAD

- El administrador del sistema o un **encargado de auditorías** designado por él, deberá:
 - determinar qué logs se generarán,
 - determinar qué eventos de seguridad se auditarán,
 - determinar qué datos se recogerán de estas auditorías,
 - administrar, desarrollar e implementar los procedimientos de auditoría y revisión,
 - monitorizar y reaccionar a los avisos (warnings) y reportes,
 - chequear aleatoriamente para verificar el cumplimiento de los requerimientos y procedimientos de seguridad,
 - revisar los reportes de auditorías cuando es advertido de anomalías.
- El **encargado del mantenimiento** de los servidores debe encargarse de actualizar las herramientas de análisis de logs.

6.3 AUDITORÍAS DE CONTROL DE ACCESO

- Los **logs** deben almacenarse en carpetas de los servidores protegidas con contraseña. Esta contraseña debe ser desconocida para todos los usuarios del

sistema, incluso para el administrador, por lo que debe conservarla un miembro del Directorio.

- Deberán generarse logs referidos al **acceso a datos**, identificando los archivos abiertos por usuario.
- Deberán generarse logs referidos a la **modificación de datos**, identificando los datos modificados por cada usuario y el valor anterior de dicho dato.
- Deben generarse logs cuando un usuario **modifica su contraseña**, con datos sobre la aplicación desde la que se realizó el cambio y, en caso que el cambio resulte fallido, el motivo del fallo.
- Deben realizarse controles más frecuentes sobre los **logs del usuario administrador**. El estudio de estos reportes debe ser realizado por un superior y no por el administrador.
- Deben generarse logs cuando hubo un **fallo en el logeo** de un usuario, indicando el motivo del fallo.
- Debe generarse un logs cuando se produzca el **bloqueo de un usuario** avisando al administrador por medio de un sistema de alerta.
- Debe generarse **perfiles de los usuarios** en base a algunos de los siguientes datos:
 - uso de Internet,
 - tráfico de mails,
 - tráfico de red que genera cada usuario o sector de la empresa,
 - terminales utilizadas,
 - las horas de acceso.

6.4 AUDITORÍAS DE REDES

- Debe generarse un **plan de monitorización de red** utilizando algún escáner de seguridad integral (Overall security scanner).
- Con respecto a las **conexiones a Internet** deben almacenarse datos sobre:
 - número IP de la máquina conectada,
 - dirección de las páginas visitadas,
 - cookies guardadas,
 - archivos descargados,
 - servicios utilizados,
 - aplicaciones utilizadas.
- Con respecto a la utilización del **correo electrónico** deben almacenarse datos sobre:
 - correo entrante y saliente,
 - hora de envío,

- contenido del mail,
 - asunto del mail,
 - archivos adjuntos,
 - reporte de virus de cada parte del mail,
 - direcciones de máquina destino y fuente,
 - tamaño del mensaje.
- Con respecto a la utilización de la **red informática** deben almacenarse datos sobre:
 - ancho de banda utilizado y cuellos de botella en el tráfico de red,
 - tráfico generado por las aplicaciones,
 - recursos de los servidores que utilizan las aplicaciones,
 - el estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta),
 - intentos de intrusión,
 - uso de los protocolos,
 - solicitudes de impresión de datos de la empresa.

7- PLAN DE CONTINGENCIAS

7.1 PLAN DE ADMINISTRACIÓN DE INCIDENTES

- Se deberá asegurar la continuidad de la recolección de datos y su procesamiento ante cualquier contingencia que afecte a los centros de procesamiento. Para ello se deberá:
 - generar **procedimientos manuales** de respaldo para cada una de las actividades desarrolladas en la empresa,
 - preparar, probar y mantener actualizado un **plan de contingencias**, coordinando el mismo con los procedimientos de copias de respaldo y almacenamiento externo. Dicho plan deberá ser desarrollado de forma tal que cubra las distintas áreas de riesgo,
 - definir y asignar claramente las **responsabilidades** de las tareas detalladas en el plan,
 - prever un programa de **entrenamiento** para el personal involucrado en el plan de contingencias.
- Deberá almacenarse una **copia del plan** de contingencias en el exterior de la empresa, protegiéndola contra su divulgación y actualizándola permanentemente.

7.2 BACKUP DE EQUIPAMIENTO

- El equipamiento informático de la empresa debe contar con **dispositivos de respaldo**, ante cualquier tipo de incidente.
- Los **mecanismos de recuperación** de los dispositivos de respaldo deben ser probados periódicamente comprobando su buen funcionamiento.
- El sistema informático no deberá verse afectado ante una contingencia en el centro de cómputos, por lo que el equipamiento informático debe distribuirse en **lugares físicos diferentes**, contando ambos con las medidas y condiciones de calidad y seguridad especificadas en esta política, distribuyendo de esta manera el equipamiento redundante.
- En el caso que ocurra alguna **contingencia con el servidor** de aplicaciones, el servidor de Internet, se utilizará como servidor de aplicaciones. Este proceso no funcionará en sentido inverso, es decir que el servidor de aplicaciones no reemplazará al servidor de Internet.

7.3 ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES

- Debe conformarse un **grupo de desarrollo** encargado de concebir, probar e implementar el plan de contingencias. Éste debe estar a cargo del administrador del centro de cómputos, e integrado por los líderes de cada área de la organización.

- Debe asignarse un **orden de importancia** a los sistemas de información y a los equipos de la red informática, de acuerdo al análisis de riesgo y al impacto que representaría para la empresa su ausencia.
- Los equipos deberán estar **señalizados** o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.
- Deberán definirse las funciones o **servicios críticos** de la empresa, junto con los recursos mínimos necesarios para su funcionamiento, asignándoles una prioridad en el plan de contingencia.
- Deberán identificarse las **contingencias** que podrían ocurrir para cada nivel de servicio crítico definido.
- Deberá conformarse un **plan de emergencias**, determinando los procedimientos a llevar a cabo para cada contingencia identificada, considerando los distintos escenarios posibles. Cada procedimiento deberá estar claramente definido, y tener asignado un responsable para su ejecución.
- Para el desarrollo del plan de contingencias deben contemplarse las siguientes pautas:
 - Deberá estar **documentado y testeado** antes de su puesta en práctica.
 - Deberá basarse en un **análisis de riesgo**, determinando que acciones merecen estar incluidas.
 - Deberá **abarcar** la totalidad de la empresa.
 - Deberá mantenerse **actualizado** de acuerdo a nuevos puestos de trabajos y funciones.
 - Deberá ser **probado** frecuentemente.
 - Deberá **contener** la siguiente información:
 - ~ objetivo del plan,
 - ~ modo de ejecución,
 - ~ tiempo de duración,
 - ~ costes estimados,
 - ~ recursos necesarios,
 - ~ evento a partir del cual se pondrá en marcha el plan.
- Debe definirse hasta cuanto tiempo se aceptará estar en **condición de emergencia**.
- Debe documentarse la realización de las siguientes actividades **después de un incidente**:
 - determinar la causa del daño,
 - evaluar la magnitud del daño que se ha producido,
 - que sistemas se han afectado,
 - qué modificaciones de emergencia se han realizado,
 - que equipos han quedado no operativos,
 - cuales se pueden recuperar y en cuanto tiempo.

Cada una estas actividades deberán ser reportadas por los líderes de cada área a un miembro de la Gerencia.

- Deberá asignarse el papel de **coordinador** a un empleado, que se encargará de las operaciones necesarias para que el sistema funcione correctamente después de la emergencia. Éste deberá determinar las acciones a seguir basándose en el plan de emergencias.
- Deberá **retroalimentarse** el plan luego de una contingencia, ajustando las directivas en consecuencia.
- Deben establecerse planes de prueba periódicos que incluyan **simulacros de siniestros** para evaluar la eficacia y eficiencia del plan.

CONCLUSIÓN

A lo largo del presente trabajo pudimos comprender que la seguridad en cómputos es un conjunto de recursos destinados a lograr que la información y los activos de una organización sean confidenciales, íntegros y disponibles para todos sus usuarios.

Somos conscientes de que no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos, sin embargo se debe estar preparado y dispuesto a reaccionar con rapidez ya que las amenazas y las vulnerabilidades están cambiando constantemente.

Disponer de una política de seguridad es importante, pero entendemos que hacer de la política de seguridad una parte del entorno de trabajo diario es esencial. La comunicación con los usuarios del sistema es la clave para hacer que esta política sea efectiva y se genere una “cultura de la seguridad”.

Acordamos que la implantación de una política de seguridad informática en una empresa implica un gran desafío, pero sabemos además que es imprescindible, sobre todo si se tiene en cuenta que cada vez se produce un mayor número de ataques.

Ponemos de manifiesto que los resultados obtenidos fueron muy satisfactorios. Una vez concluido el desarrollo del presente trabajo, la empresa auditada se mostró muy conforme con las recomendaciones sugeridas, y reveló su intención de poner en práctica el plan de seguridad generado.

Asimismo podemos afirmar que las expectativas personales también fueron cubiertas con éxito. Nos fue posible aprender nuevos conceptos, desarrollando un trabajo de investigación sobre temas vigentes y volcar toda la teoría asimilada a un caso práctico.

Por último, esperamos con este trabajo generar en el lector una inquietud que incite a futuras investigaciones o proyectos que profundicen en el campo de la seguridad informática.

Córdoba, Octubre de 2002

ANEXO I – ANÁLISIS DE RIESGOS

1- INTRODUCCIÓN

El presente análisis de riesgo fue desarrollado con el propósito de determinar cuáles de los activos de la empresa tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos, identificando las causas potenciales que faciliten o impidan alcanzar los objetivos, calculando la probabilidad de su ocurrencia, evaluando sus probables efectos, y considerando el grado en que el riesgo puede ser controlado.

Para generar esta información se desempeñaron las siguientes actividades:

1. Listado de los activos de la empresa: se evaluaron los distintos activos físicos y de software de la organización, generando un inventario de aquellos que son considerados como vitales para su desenvolvimiento seguro.
2. Asignación de prioridades a los activos: los activos fueron clasificados según el impacto que sufriría la organización si faltase o fallara tal activo.
3. Definición de factores de riesgos: acto seguido se listaron los factores de riesgo relevantes a los que pueden verse sometidos cada uno de los activos arriba nombrados.
4. Descripción de consecuencias: teniendo presente el listado anterior, se generó una descripción de las consecuencias que podría sufrir la empresa si los activos son afectados por sus respectivos factores de riesgo, detallando la manera en que se protege al activo contra ese ataque en particular, y puntualizando en qué grado son efectivas estas medidas.
5. Asignación de probabilidades de ocurrencia de los factores de riesgo: teniendo en cuenta los datos arriba mencionados fue posible estimar la probabilidad de ocurrencia que cada uno de los factores de riesgo representaba con respecto a los activos listados, considerando para esta estimación las medidas tomadas por la empresa para mitigar su acción.
6. Cálculo de niveles de vulnerabilidad: una vez identificados los riesgos, se procedió a su análisis. Con toda la información recolectada, se determinó el nivel de vulnerabilidad que se asocia con cada activo listado.
7. Conclusiones: a partir de las actividades anteriormente descritas se pudo evaluar la situación actual de la empresa en relación a los incidentes que pueden afectarla, calculando el porcentaje de los riesgos cubiertos y descubiertos, y un análisis sobre la escala de importancia de los activos.
8. Consecuencias: luego de identificar, estimar y cuantificar los riesgos, los directivos de la empresa deben determinar los objetivos específicos de control y, con relación a ellos, establecer los procedimientos de control más convenientes, para enfrentarlos de la manera más eficaz y económica posible.

En general, aquellos riesgos cuya concreción esté estimada como de baja frecuencia, no justifican preocupaciones mayores. Por el contrario, los que se estiman de alta frecuencia deben merecer preferente atención. Entre estos extremos se encuentran casos que deben ser analizados cuidadosamente, aplicando elevadas dosis de buen juicio y sentido común.

2- ACTIVOS Y FACTORES DE RIESGOS

Presentamos los distintos activos reconocidos en La Empresa, asignando un valor a la importancia que tienen en la organización, ponderada en una escala del 1 al 10. Esta importancia es un valor subjetivo que refleja el nivel de impacto que puede tener la empresa si un incidente afecta a los activos, sin considerar las medidas de seguridad que existan sobre los mismos.

A continuación se listan los factores de riesgo que pueden afectar a dichos activos, indicando la probabilidad de que estas contingencias ocurran, en una escala del 1 al 3. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en la organización.

Activos a proteger	Imp.
Servidores y switch central.	10
Bases de datos.	10
Software de aplicación, programas fuente, sistemas operativos.	9
Backup.	9
Datos en tránsito, datos de configuración, datos en medios externos.	8
Administrador de sistemas (Departamento de sistemas).	7
Cableado, antenas, switch, hubs, módems.	6
Red.	6
Usuarios.	5
Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	4
Hardware (teclado, monitor, unidades de discos, medios removibles, etc.).	3
Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	2
Datos de usuarios.	1

Factores de riesgo	Prob.
Abuso de puertos para el mantenimiento remoto	1
Acceso no autorizado a datos (borrado, modificación, etc.)	2
Administración impropia del sistema de IT	1
Almacenamiento de passwords negligente	2
Ancho de banda insuficiente	1
Aplicaciones sin licencia	2
Ausencia o falta de segmentación	1
Base de datos compleja	2
Borrado, modificación o revelación desautorizada o inadvertida de información	1
Browsing de información	1
Complejidad en el acceso a las redes de sistemas de IT	1
Condiciones de trabajo adversas	1
Conexión de cables inadmisibles	1
Conexiones todavía activas	3
Configuración impropia del SendMail	1
Configuración inadecuada de componentes de red	2

Factores de riesgo	Prob.
Conocimiento insuficiente de los documentos de requerimientos en el desarrollo	2
Copia no autorizada de un medio de datos	2
Corte de luz, UPS descargado o variaciones de voltaje.	1
Daño de cables inadvertido	1
Deficiencias conceptuales en la red	1
Descripción de archivos inadecuada	1
Destrucción negligente de equipos o datos	1
Destrucción o mal funcionamiento de un componente	1
Documentación deficiente	3
Documentación insuficiente o faltante, Funciones no documentadas	3
Denial of service	1
Entrada sin autorización a habitaciones	2
Entrenamiento de usuarios inadecuado	2
Errores de configuración y operación	1
Errores de software	1
Errores en las funciones de encriptación	1
Factores ambientales	1
Falla de base de datos	1
Falla del sistema	1
Falla en la MAN	1
Falla en medios externos	1
Falta de auditorías	3
Falta de autenticación	1
Falta de compatibilidad	1
Falta de confidencialidad	1
Falta de cuidado en el manejo de la información (Ej. Password)	2
Falta de espacio de almacenamiento	1
Ingeniería social - Ingeniería social inversa	1
Interferencias	1
Límite de vida útil - Máquinas obsoletas	1
Longitud de los cables de red excedida	1
Mal interpretación	2
Mal mantenimiento	1
Mal uso de derechos de administrador	3
Mal uso de servicios de mail	2
Mala administración de control de acceso (salteo del login, etc.)	1
Mala configuración del schedule de backups	1
Mala evaluación de datos de auditoría	3
Mala integridad de los datos	1
Mantenimiento inadecuado o ausente	2
Medios de datos no están disponibles cuando son necesarios	1
Modificación de paquetes	1
Modificación no autorizada de datos	1
No-cumplimiento con las medidas de seguridad del sistema	2
Penetración, interceptación o manipulación de líneas	1
Pérdida de backups	2
Perdida de confidencialidad en datos privados y de sistema	1

Factores de riesgo	Prob.
Pérdida de confidencialidad o integridad de datos como resultado de un error humano en el sistema	1
Pérdida de datos	1
Perdida de datos en tránsito	1
Desvinculación del personal	1
Poca adaptación a cambios en el sistema	1
Portapapeles, impresoras o directorios compartidos	1
Prueba de software deficiente	1
Recursos escasos	1
Reducción de velocidad de transmisión	1
Reglas insuficientes o ausencia de ellas	2
Riesgo por el personal de limpieza o personal externo	1
Robo	1
Robo de información	1
Robo por uso de laptops	1
Rótulos inadecuados en los medios de datos	1
Sabotaje	1
Seguridad de base de datos deficiente	1
Sincronización de tiempo inadecuada	1
Software desactualizado	1
Spoofing y sniffing	1
Transferencia de datos incorrectos o no deseados	1
Transporte inseguro de archivos	1
Transporte inseguro de medios de datos	1
Uso de derechos sin autorización	2
Uso descontrolado de recursos (DoS)	1
Uso impropio del sistema de IT	1
Uso sin autorización	1
Virus, gusanos y caballos de Troya	3

3- POSIBLES CONSECUENCIAS Y MEDIDAS EXISTENTES

En el presente cuadro se listan los activos de la organización, los factores de riesgos que los afectan directamente y las consecuencias que puede acarrear la ocurrencia de estos factores. Se agrega información referida a las medidas que ha tomado la empresa para mitigar estas consecuencias. Por último los auditores han evaluado estas medidas, indicando si son deficientes, mejorables o eficientes.

(Deficiente - Mejorable - Eficiente)

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Servidores y switch central.	Acceso no autorizado	Robo, modificación de información.	s	Seguridad física y control de acceso lógico	m
	Corte de luz, UPS descargado o variaciones de voltaje.	Falta de sistema.	s	Generador, UPS, estabilizador, tres líneas independientes.	e
	Destrucción de un componente	Pérdida de tiempo por necesidad de reemplazo.	s	Redundancia de los componentes del servidor.	e
	Error de configuración	Aumento de vulnerabilidades e inestabilidad en el sistema.	s	Contratación de mantenimiento por especialistas.	e
	Factores ambientales	Falta de sistema y destrucción de equipos.	s	Seguridad física y buen diseño del edificio.	e
	Límite de vida útil - Máquinas obsoletas	Deterioro en la performance del sistema.	s	Equipamiento actual y asesoramiento permanente.	e
	Mal mantenimiento	Interrupciones en el funcionamiento del sistema.	s	Mantenimiento interno y mantenimiento tercerizado en manos de especialistas.	e
	Modificación no autorizada de datos	Inconsistencia de datos, mala configuración, fraude.	s	Controles de acceso físico y lógico al servidor.	m
	Robo	Pérdida de equipamiento o información.	s	Controles de acceso físicos, guardias de seguridad, alarmas.	e
	Virus	Fallas generales del sistema y en la red.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Bases de datos.	Base de datos compleja	Desarrollo complejo de sistemas.	n		m
	Copia no autorizada de un medio de datos	Divulgación de información.	s	Deshabilitación del portapapeles y controles lógicos.	e
	Errores de software	Inconsistencias en los datos.	s	Controles internos y backup de los datos.	m
	Falla de base de datos	Inconsistencias en los datos.	s	Controles internos y backup de los datos.	e
	Falla en medios externos	Perdida de backup.	s	Redundancia de los mismos.	m
	Falta de espacio de almacenamiento	Falla en la aplicación.	s	Recursos abundantes.	e
	Mala configuración del schedule de backups	Datos sin backup.	s	Organización de scheduler.	e
	Mala integridad de los datos	Inconsistencias y redundancia de datos.	s	Controles en las aplicaciones desarrolladas.	m
	Medios de datos no están disponibles cuando son necesarios	Pérdida de tiempo y productividad.	s	Aplicación de la empresa que trabaja en tiempo real (on-line)	e
	Pérdida de backups	Incapacidad de restauración	s	Backups redundantes.	e
	Perdida de confidencialidad en datos privados y de sistema	Divulgación de información.	s	Controles físicos y controles de accesos lógicos a datos críticos.	m
	Perdida de datos en tránsito	Inconsistencia de datos y divulgación de información.	s	Políticas de configuración de red.	m
	Portapapeles, impresoras o directorios compartidos	Divulgación de información.	s	Deshabilitación del portapapeles y controles lógicos.	e
	Robo	Divulgación de información.	s	Deshabilitación del portapapeles y controles lógicos.	e
	Robo por uso de laptops	Divulgación de información.	s	Ausencia de información crítica en laptops.	e
	Sabotaje	Pérdida o modificación de datos, pérdida de tiempo y productividad.	s	Backups redundantes y controles físicos y lógicos.	e
	Spoofing y sniffing	Divulgación y modificación de información.	n		d
	Transferencia de datos incorrectos	Inconsistencia de datos.	s	Controles lógicos.	e
	Virus	Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Software de aplicación, programas fuente y sistemas operativos.	Acceso no autorizado a datos (borrado, modificación, etc.)	Modificación del software en desarrollo.	s	Controles físicos y controles de accesos lógicos a desarrollo de software.	e
	Aplicaciones sin licencia	Multas y problemas con Software Legal.	n		m
	Conocimiento insuficiente de los documentos de requerimientos en el desarrollo	Sistema inestable y excesivos pedidos de cambios.	s	Metodología de análisis y diseño estructurada.	m
	Error de configuración	Mal funcionamiento de los sistemas.	s	Existen herramientas de análisis y personal de mantenimiento.	e
	Errores en las funciones de encriptación	Problemas en la recuperación de archivos encriptados o divulgación de información.	s	Personal de mantenimiento especializado.	e
	Falla del sistema	Falta de sistema y posibles demoras.	s	Backup y sistemas de respaldo.	m
	Falta de compatibilidad	Datos erróneos e inestabilidad del sistema.	s	Herramienta de comunicación entre sistemas operativos diferentes.	e
	Falta de confidencialidad	Divulgación de información.	s	Deshabilitación del portapapeles y controles lógicos.	e
	Mala administración de control de acceso (salteo del login, etc.)	Divulgación y modificación de información.	s	Controles de acceso lógico, reforzados en datos críticos.	e
	Pérdida de datos	Divulgación de información.	s	Backup de respaldo.	e
	Poca adaptación a cambios del sistema	Sistema inestable y de difícil modificación.	s	Metodología de análisis y diseño estructurada.	e
	Prueba de software deficiente	Sistema poco confiable.	s	Metodología de análisis y diseño estructurada.	e
	Software desactualizado	Probabilidad incremental de vulnerabilidades y virus.	s	Mantenimiento por especialistas y constante evaluación de las aplicaciones.	m
	Virus	Inestabilidad y mal funcionamiento de sistemas.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Backup.	Copia no autorizada a un medio de datos	Robo de información.	s	Controles de seguridad física en el ingreso al centro de cómputos y controles de acceso lógicos al servidor.	m
	Errores de software	Error en la generación o en la copia de backups a medios externos.	n		m
	Falla en medios externos	Pérdida de backups.	s	Backups redundantes en distintos medios de almacenamiento.	m
	Falta de espacio de almacenamiento	Falla en la generación del backup.	s	Existencia de discos redundantes para la copia.	e
	Mala configuración del schedule de backups	Falta de copias de respaldo de datos.	s	Agenda de backups eficiente.	e
	Mala integridad de los datos resguardados.	Errores durante la restauración de datos.	s	Numerosas copias de respaldo por posibles errores.	m
	Medios de datos no están disponibles cuando son necesarios	Pérdida de backup y retraso del sistema.	s	Numerosas copias de respaldo por posibles errores.	e
	Pérdida de backups	Falta de datos, incapacidad de restaurarlos y divulgación de información.	s	Backups redundantes	e
	Robo	Incapacidad de restaurarlos y divulgación de información.	s	Controles de acceso físicos, guardias de seguridad, alarmas.	e
	Rótulos inadecuado en los medios de datos	Errores durante la restauración de datos.	s	Rótulos capaces de diferenciar cada medio de datos como único.	e
	Sabotaje	Pérdida o robo de información.	s	Controles de acceso físicos, guardias de seguridad y copias de respaldo redundantes.	e
	Spoofing y sniffing	Divulgación, modificación y robo de información.	n		d
	Virus	Pérdida de datos de backup.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Datos en tránsito, datos de configuración, datos en medios externos.	Copia no autorizada de un medio de datos	Robo de información.	s	Controles de seguridad física, controles de acceso lógicos a los sistemas.	m
	Errores en las funciones de encriptación	Divulgación de información (passwords)	s	Utilización de protocolos seguros en la transmisión.	e
	Falla en medios externos	Pérdida de datos en medios externos.	s	Copias de respaldo redundantes	e
	Mala integridad de los datos	Inconsistencia de información.	s	Controles de integridad en la transmisión, en el ingreso de datos.	e
	Medios de datos no están disponibles cuando son necesarios	Pérdida de tiempo y productividad por falta de datos.	s	Copias de respaldo redundantes	e
	Perdida de confidencialidad en datos privados y de sistema	Divulgación de información.	s	Controles de acceso lógico y físico a los medios de almacenamiento de datos, reforzados en datos críticos.	m
	Perdida de datos en tránsito	Divulgación de información.	s	Utilización de protocolos seguros en la transmisión.	m
	Portapapeles, impresoras o directorios compartidos	Divulgación o robo de información.	s	Prohibición de la impresión y de la utilización del portapapeles.	e
	Robo por uso de laptops	Divulgación o robo de información.	s	Laptops de usos personales, sin datos críticos de la empresa.	e
	Sabotaje	Pérdida o robo de información.	s	Utilización de protocolos seguros en la transmisión.	m
	Spoofing y sniffing	Divulgación, modificación y robo de información.	n		d
	Virus	Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Administrador de sistemas (Departamento de Sistemas).	Administración impropia del sistema de IT (responsabilidades y roles del personal de sistemas)	Asignación de responsabilidades impropia.	n		m
	Almacenamiento de passwords negligente	Divulgación de password y uso indebido de derechos de usuarios.	s	El sistema operativo encripta las password de sus usuarios, y se ha modificado el directorio de almacenamiento por default.	m
	Configuración impropia del SendMail	Divulgación de mensajes, uso del servidor para enviar SPAM, fallas en la administración de cuotas de discos.	s	La configuración del SendMail la realiza y mantiene un especialista en la aplicación.	e
	Errores de configuración y operación del sistema.	Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades.	s	El mantenimiento diario lo realiza el administrador de sistemas, ayudado por un especialista contratado.	e
	Falta de auditorías en sistema operativo	Imposibilidad del seguimiento de usuarios y de la generación de reportes.	s	Existen logs generados automáticamente por el sistema operativo y por sus aplicaciones principales.	e
	Mala evaluación de datos de auditoría	No se analizan los logs y por lo tanto no hay evaluación de los resultados.	n		d
	Mal uso de derechos de administrador	Mala distribución de los permisos y de las cuentas de administrador.	n		d

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Cableado, antenas, switch, hubs, módem.	Ancho de banda insuficiente	Transmisión pesada en la red o imposibilidad de utilizar el sistema on-line.	s	Recursos abundantes en ancho de banda.	e
	Conexión de cables inadmisibles	Pinchaduras de cables, robo de datos, spoofing y sniffing.	s	Cableado estructurado aplicado en el tendido de la empresa.	e
	Daño o destrucción de cables o equipamiento inadvertido	Pinchaduras de cables, robo de datos, spoofing y sniffing.	s	Cableado estructurado aplicado en el tendido de la empresa.	e
	Factores ambientales	Interferencias o daños de equipamiento.	s	Utilización de UPS y buen diseño del edificio	e
	Interferencias	Errores en los datos de transmisión o imposibilidad de utilizar el sistema on-line.	s	Cableado estructurado en la red de la empresa y mantenimiento de sistema radial tercerizado.	e
	Límite de vida útil de equipos.	Equipos obsoletos e imposibilidad de utilizar el sistema.	s	Equipamiento actualizado y mantenimiento tercerizado del cableado.	e
	Longitud de los cables de red excedida	Transmisión lenta o con interferencias, o imposibilidad de utilizar el sistema on-line.	s	Cableado estructurado y mantenimiento tercerizado del cableado.	e
	Mal mantenimiento	Errores de transmisión o interrupción del servicio de red.	s	Mantenimiento tercerizado por especialistas en cableado estructurado.	e
	Reducción de velocidad de transmisión	Pérdida de tiempo de los usuarios, o imposibilidad de utilizar el sistema on-line.	s	Recursos abundantes en ancho de banda.	e
	Riesgo por el personal de limpieza o personal externo	Daño en cables o equipos, interrupción del sistema on-line.	s	Cables y equipos protegidos, fuera de la vista y el alcance de terceros.	e

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Red.	Abuso de puertos para el mantenimiento remoto	Posibles intrusiones y robo o divulgación de información.	s	Política de configuración de puertos restringida y herramientas de monitoreo de puertos.	m
	Ausencia o falta de segmentación	Tramos de red extensos y dificultades en la comunicación.	s	Red segmentada física y lógicamente por sectores.	e
	Complejidad en el diseño de las redes de sistemas de IT	Dificultad en la administración y en el mantenimiento.	s	Diseño de red simple con topología de bus.	e
	Conexiones todavía activas	Intrusión de usuarios no autorizados al sistema.	n		d
	Configuración inadecuada de componentes de red	Errores de transmisión, interrupción del servicio de red.	s	Equipamiento de red configurado por empresa tercerizada.	e
	Denial of service	Interrupción de todos o algunos de los servicios de red.	n		m
	Errores de configuración y operación	Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades.	s	El mantenimiento diario lo realiza el administrador de sistemas, ayudado por un especialista contratado.	e
	Falla en la MAN	Una o más sucursales incomunicadas.	n		m
	Falta de autenticación	Posibles intrusiones y robo o divulgación de información.	s	Controles de acceso a datos y a equipos, y firewall.	m
	Mal uso de servicios de mail	Disminución de la performance del ancho de banda	s	Concienciación de los usuarios sobre el buen uso del mail.	m
	Sincronización de tiempo inadecuada	Inconsistencia en datos.	s	Aplicativo que actualiza el horario permanentemente.	e
	Spoofing y sniffing	Divulgación, modificación y robo de información.	n		d
	Transporte inseguro de archivos	Divulgación de información.	n		m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Usuarios.	Acceso no autorizado a datos	Divulgación o robo de información.	s	Controles de acceso lógico a datos en las aplicaciones.	e
	Borrado, modificación o revelación desautorizada o inadvertida de información	Inconsistencia de datos o datos faltantes.	s	Controles lógicos a datos.	e
	Condiciones de trabajo adversas	Predisposición a distracción, bajo rendimiento de usuarios.	s	Ambiente de trabajo cómodo.	e
	Destrucción de un componente de hardware	Pérdida de tiempo por necesidad de reemplazo.	s	Redundancia de los componentes.	e
	Destrucción negligente de datos	Pérdida de información.	s	Controles lógicos a datos en las aplicaciones.	e
	Documentación deficiente	Mayor probabilidad de errores por falta de instrucciones.	n		d
	Entrada sin autorización a habitaciones	Robo de equipos o insumos, divulgación de datos.	s	Control de acceso físico a instalaciones del centro de cómputos.	m
	Entrenamiento de usuarios inadecuado	Predisposición a errores y bajo rendimiento de usuarios.	s	Capacitación grupal de usuarios en el uso del sistema.	m
	Falta de auditorías	Predisposición a un rendimiento mediocre y falta de concienciación sobre responsabilidades y seguridad.	n		d
	Falta de cuidado en el manejo de la información (Ej. Password)	Divulgación de datos.	s	Insistencia con respecto al uso discreto de datos críticos.	m
	Ingeniería social - Ingeniería social inversa	Robo o modificación de información.	n		m
	Mal uso de derechos de administrador (sesiones abiertas)	Divulgación o robo de información, sabotaje interno.	n		d
	No-cumplimiento con las medidas de seguridad del sistema	Medidas correctivas tomadas por la gerencia, según la gravedad del incidente.	s	Permanente concienciación de los usuarios.	m
	Pérdida de confidencialidad o integridad de datos como resultado de un error humano.	Error en la información.	s	Controles lógicos de acceso a datos y de integridad de datos de entrada al sistema.	e
	Desvinculación del personal	Robo o modificación de información, sabotaje interno.	n		m
	Uso descontrolado de recursos (DoS)	Retraso en las actividades o falta de sistema.	n		d

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	Acceso no autorizado a datos de documentación.	Divulgación, robo o modificación de información.	s	Control de acceso físico a instalaciones del centro de cómputos.	m
	Borrado, modificación o revelación desautorizada de información	Documentación incorrecta.	n		d
	Browsing de información	Divulgación de información.	s	Controles de acceso lógico al sistema.	e
	Copia no autorizada de un medio de datos	Divulgación de información.	s	Control de acceso físico a instalaciones del centro de cómputos.	m
	Descripción de archivos inadecuada	Documentación incorrecta.	n		d
	Destrucción negligente de datos	Documentación incorrecta.	n		d
	Documentación insuficiente o faltante, funciones no documentadas	Entorpecimiento de la administración y uso del sistema.	n		d
	Factores ambientales	Destrucción de datos.	s	Seguridad física y buen diseño del edificio.	m
	Mal interpretación	Entorpecimiento de la administración y uso del sistema.	n		d
	Mantenimiento inadecuado o ausente	Documentación incorrecta, redundante y compleja.	n		d
	Medios de datos no están disponibles cuando son necesarios	Entorpecimiento de la administración y uso del sistema.	n		d
	Robo	Divulgación de información.	s	Controles de acceso físico a datos.	m
	Uso sin autorización	Divulgación, robo o modificación de información.	s	Controles de acceso físico a datos.	m
	Virus, gusanos y caballos de Troya	Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad.	s	Herramientas antivirus y firewall.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	Corte de luz, UPS descargado o variaciones de voltaje.	Interrupción del funcionamiento de equipos.	s	Generador, UPS, estabilizador, tres líneas independientes.	e
	Dstrucción o mal funcionamiento de un componente	Interrupción de la tarea del usuario.	s	Insumos de respaldo y equipamiento asegurado.	e
	Factores ambientales	Dstrucción o avería de equipos.	s	Insumos de respaldo y equipamiento asegurado.	e
	Límite de vida útil	Avería de equipos.	s	Insumos de respaldo y equipamiento asegurado.	e
	Mal mantenimiento	Avería de equipos e incremento en el costo de equipamiento de respaldo.	s	Mantenimiento tercerizado por el asegurador de la red.	e
	Robo	Pérdida de equipamiento e interrupción de la tarea del usuario.	s	Controles de acceso físicos, guardias de seguridad, alarmas.	e
Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	Factores ambientales	Dstrucción de insumos.	s	Insumos de respaldo.	e
	Límite de vida útil	Dstrucción o avería de insumos.	s	Insumos de respaldo.	e
	Recursos escasos.	Interrupción en el funcionamiento normal de la empresa.	s	Insumos de respaldo.	e
	Uso descontrolado de recursos.	Incremento no justificado del gasto de insumos.	s	Administración estricta de insumos.	e
	Robo	Pérdida de insumos e incremento en el gasto.	s	Controles de acceso físicos, guardias de seguridad, alarmas.	e
	Transporte inseguro de medios de datos	Pérdida de datos, de insumos, e incremento en el gasto.	s	Personal asignado a dicha tarea con normas internas a cumplir.	m

Nombre del Activo	Factor de riesgo	Consecuencias?	Se protege?	Cómo?	Es efectiva?
Datos de usuarios.	Falta de espacio de almacenamiento	Retraso de las actividades.	s	Capacidad de almacenamiento sobredimensionada.	e
	Mala configuración del schedule de backups	Pérdida de datos del usuario.	n		m
	Medios de datos no están disponibles cuando son necesarios	Retraso en las actividades.	s	Permanente disponibilidad de estos medios por personal del centro de cómputos.	e
	Pérdida de backups	Pérdida de datos del usuario y retraso de la tarea.	s	Controles de acceso físico y lógico al equipo usado para tal copias de respaldo.	m
	Perdida de confidencialidad en datos privados y de sistema	Divulgación de información.	s	Controles de acceso físico y lógico a las PC's de los usuarios.	m
	Portapapeles, impresoras o directorios compartidos	Divulgación de información.	s	Carpetas de usuarios no compartidas en la red.	e
	Robo	Divulgación de información.	s	Controles de acceso físico y lógico a los equipos.	e
	Sabotaje	Pérdida, modificación o divulgación de datos.	s	Controles de acceso físico y lógico a los equipos y copias de respaldo de los datos	e
	Spoofing y sniffing	Divulgación, modificación y robo de información.	n		d
	Virus	Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad.	s	Herramientas antivirus y firewall.	m

4- CÁLCULO DE NIVELES DE VULNERABILIDAD

En este cuadro se calculan los niveles de vulnerabilidad (o niveles de riesgo) en los que incurre cada activo arriba mencionado. Para esto se tiene en cuenta el nivel de importancia asignado a cada uno y la probabilidad de ocurrencia de estos riesgos. Para realizar dicho cálculo se desarrollaron las siguientes operaciones:

PROBABILIDAD DE OCURRENCIA: representan la probabilidad de que ocurran los factores de riesgo mencionados, en una escala del 1 al 3. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en la organización.

PORCENTAJE DE LA PROBABILIDAD DEL RIESGO: se calcula el porcentaje de probabilidad de que ocurra un determinado factor de riesgo, con respecto a la cantidad de factores de riesgo intervinientes para dicho activo. Esto es debido a que cada activo está afectado por un número diferente de riesgos posibles, de manera que este cálculo sirve para obtener un porcentaje de probabilidades equilibrado por igual para cualquier activo, independientemente de la cantidad de factores de riesgo que lo afectan.

NIVEL DE VULNERABILIDAD: en este momento interviene el nivel de importancia, multiplicando al porcentaje de probabilidad del riesgo. De esta forma se obtiene el nivel de vulnerabilidad de cada activo con respecto a un factor de riesgo. La suma de estos valores es el nivel de vulnerabilidad total que corresponde a cada activo.

Rango		1 a 10		B - M - A		
Nº Activo	Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
1	Servidores y switch central.	10	Acceso no autorizado	2	20,00	200,00
			Corte de luz	1	10,00	100,00
			Destrucción de un componente	1	10,00	100,00
			Error de configuración	1	10,00	100,00
			Factores ambientales	1	10,00	100,00
			Límite de vida útil - Máquinas obsoletas	1	10,00	100,00
			Mal mantenimiento	1	10,00	100,00
			Modificación no autorizada de datos	1	10,00	100,00
			Robo	1	10,00	100,00
			Virus	3	30,00	300,00
	Cantidad de factores de riesgo = 10					1300,00

ANEXO I – ANÁLISIS DE RIESGOS

Nº Activo	Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
2	Bases de datos.	10	Base de datos compleja	2	10,53	105,26
			Copia no autorizada de un medio de datos	2	10,53	105,26
			Errores de software	1	5,26	52,63
			Falla de base de datos	1	5,26	52,63
			Falla en medios externos	1	5,26	52,63
			Falta de espacio de almacenamiento	1	5,26	52,63
			Mala configuración del schedule de backups	1	5,26	52,63
			Mala integridad de los datos	1	5,26	52,63
			Medios de datos no están disponibles cuando son necesarios	1	5,26	52,63
			Pérdida de backups	2	10,53	105,26
			Perdida de confidencialidad en datos privados y de sistema	1	5,26	52,63
			Perdida de datos en tránsito	1	5,26	52,63
			Portapapeles, impresoras o directorios compartidos	1	5,26	52,63
			Robo	1	5,26	52,63
			Robo por uso de laptops	1	5,26	52,63
			Sabotaje	1	5,26	52,63
			Spoofing y sniffing	1	5,26	52,63
			Transferencia de datos incorrectos	1	5,26	52,63
			Virus	3	15,79	157,89
				Cantidad de factores de riesgo = 19		

ANEXO I – ANÁLISIS DE RIESGOS

Nº Activo	Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
3	Software de aplicación, programas fuente y sistemas operativos.	9	Acceso no autorizado a datos (borrado, modificación, etc.)	2	14,29	128,57
			Aplicaciones sin licencia	2	14,29	128,57
			Conocimiento insuficiente de los documentos de requerimientos en el desarrollo	2	14,29	128,57
			Error de configuración	1	7,14	64,29
			Errores en las funciones de encriptación	1	7,14	64,29
			Falla del sistema	1	7,14	64,29
			Falta de compatibilidad	1	7,14	64,29
			Falta de confidencialidad	1	7,14	64,29
			Mala administración de control de acceso (salteo del login, etc.)	1	7,14	64,29
			Pérdida de datos	1	7,14	64,29
			Poca adaptación a cambios del sistema	1	7,14	64,29
			Prueba de software deficiente	1	7,14	64,29
			Software desactualizado	1	7,14	64,29
			Virus	3	21,43	192,86
Cantidad de factores de riesgo = 14						1221,43
4	Backup.	9	Copia no autorizada a un medio de datos	2	15,38	138,46
			Errores de software	1	7,69	69,23
			Falla en medios externos	1	7,69	69,23
			Falta de espacio de almacenamiento	1	7,69	69,23
			Mala configuración del schedule de backups	1	7,69	69,23
			Mala integridad de los datos resguardados	1	7,69	69,23
			Medios de datos no están disponibles cuando son necesarios	1	7,69	69,23
			Pérdida de backups	2	15,38	138,46
			Robo	1	7,69	69,23
			Rótulos inadecuado en los medios de datos	1	7,69	69,23
			Sabotaje	1	7,69	69,23
			Spoofing y sniffing	1	7,69	69,23
			Virus	3	23,08	207,69
			Cantidad de factores de riesgo = 13			

ANEXO I – ANÁLISIS DE RIESGOS

Nº Activo	Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad	
5	Datos en tránsito, datos de configuración y datos en medios externos.	8	Copia no autorizada de un medio de datos	2	16,67	133,33	
			Errores en las funciones de encriptación	1	8,33	66,67	
			Falla en medios externos	1	8,33	66,67	
			Mala integridad de los datos	1	8,33	66,67	
			Medios de datos no están disponibles cuando son necesarios	1	8,33	66,67	
			Perdida de confidencialidad en datos privados y de sistema	1	8,33	66,67	
			Perdida de datos en tránsito	1	8,33	66,67	
			Portapapeles, impresoras o directorios compartidos	1	8,33	66,67	
			Robo por uso de laptops	1	8,33	66,67	
			Sabotaje	1	8,33	66,67	
			Spoofing y sniffing	1	8,33	66,67	
			Virus	3	25,00	200,00	
			Cantidad de factores de riesgo = 12				1000,00
6	Administrador de sistemas (Departamento de Sistemas).	7	Administración impropia del sistema de IT (roles y responsabilidades)	1	14,29	100,00	
			Almacenamiento de passwords negligente	2	28,57	200,00	
			Configuración impropia del SendMail	1	14,29	100,00	
			Errores de configuración y operación	1	14,29	100,00	
			Falta de auditorías en sistema operativo	3	42,86	300,00	
			Mal uso de derechos de administrador	3	42,86	300,00	
			Mala evaluación de datos de auditoría	3	42,86	300,00	
			Cantidad de factores de riesgo = 7				1400,00

ANEXO I – ANÁLISIS DE RIESGOS

Nº Activo	Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
7	Cableado, antenas, switch, hubs, módem.	6	Ancho de banda insuficiente	1	10,00	60,00
			Conexión de cables inadmisibles	1	10,00	60,00
			Daño de cables inadvertido	1	10,00	60,00
			Factores ambientales	1	10,00	60,00
			Interferencias	1	10,00	60,00
			Límite de vida útil	1	10,00	60,00
			Longitud de los cables de red excedida	1	10,00	60,00
			Mal mantenimiento	1	10,00	60,00
			Reducción de velocidad de transmisión	1	10,00	60,00
			Riesgo por el personal de limpieza o personal externo	1	10,00	60,00
	Cantidad de factores de riesgo = 10					600,00
8	Red.	6	Abuso de puertos para el mantenimiento remoto	1	7,69	46,15
			Ausencia o falta de segmentación	1	7,69	46,15
			Complejidad en el diseño de las redes de sistemas de IT	1	7,69	46,15
			Conexiones todavía activas	3	23,08	138,46
			Configuración inadecuada de componentes de red	2	15,38	92,31
			Denial of service	1	7,69	46,15
			Errores de configuración y operación	1	7,69	46,15
			Falla en la MAN	1	7,69	46,15
			Falta de autenticación	1	7,69	46,15
			Mal uso de servicios de mail	2	15,38	92,31
			Sincronización de tiempo inadecuada	1	7,69	46,15
			Spoofing y sniffing	1	7,69	46,15
			Transporte inseguro de archivos	1	7,69	46,15
				Cantidad de factores de riesgo = 13		

ANEXO I – ANÁLISIS DE RIESGOS

Nº Activo	Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
9	Usuarios.	5	Acceso no autorizado a datos	2	12,50	62,50
			Borrado, modificación o revelación desautorizada o inadvertida de información	1	6,25	31,25
			Condiciones de trabajo adversas	1	6,25	31,25
			Destrucción de un componente de hardware	1	6,25	31,25
			Destrucción negligente de datos	1	6,25	31,25
			Documentación deficiente	3	18,75	93,75
			Entrada sin autorización a habitaciones	2	12,50	62,50
			Entrenamiento de usuarios inadecuado	2	12,50	62,50
			Falta de auditorías	3	18,75	93,75
			Falta de cuidado en el manejo de la información (Ej. Password)	2	12,50	62,50
			Ingeniería social - Ingeniería social inversa	1	6,25	31,25
			Mal uso de derechos de administrador (sesiones abiertas)	3	18,75	93,75
			No-cumplimiento con las medidas de seguridad del sistema	2	12,50	62,50
			Pérdida de confidencialidad o integridad de datos como resultado de un error humano en el sistema	1	6,25	31,25
			Desvinculación del personal	1	6,25	31,25
			Uso descontrolado de recursos (DoS)	1	6,25	31,25
	Cantidad de factores de riesgo = 16					843,75

ANEXO I – ANÁLISIS DE RIESGOS

Nº Activo	Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
10	Documentación de programas, de hardware, de sistemas, procedimientos administrativos locales, manuales, etc.	4	Acceso no autorizado a datos	2	14,29	57,14
			Borrado, modificación o revelación desautorizada de datos	1	7,14	28,57
			Browsing de información	1	7,14	28,57
			Copia no autorizada de un medio de datos	2	14,29	57,14
			Descripción de archivos inadecuada	1	7,14	28,57
			Destrucción negligente de equipos o datos	1	7,14	28,57
			Documentación insuficiente o faltante, Funciones no documentadas	3	21,43	85,71
			Factores ambientales	1	7,14	28,57
			Mal interpretación	2	14,29	57,14
			Mantenimiento inadecuado o ausente	2	14,29	57,14
			Medios de datos no están disponibles cuando son necesarios	1	7,14	28,57
			Robo	1	7,14	28,57
			Uso sin autorización	1	7,14	28,57
			Virus, gusanos y caballos de Troya	3	21,43	85,71
			Cantidad de factores de riesgo = 14			
11	Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	3	Corte de luz o UPS descargado	1	16,67	50,00
			Destrucción o mal funcionamiento de un componente	1	16,67	50,00
			Factores ambientales	1	16,67	50,00
			Límite de vida útil	1	16,67	50,00
			Mal mantenimiento	1	16,67	50,00
			Robo	1	16,67	50,00
Cantidad de factores de riesgo = 6						300,00
12	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	2	Factores ambientales	1	16,67	33,33
			Límite de vida útil	1	16,67	33,33
			Recursos escasos	1	16,67	33,33
			Uso descontrolado de recursos	1	16,67	33,33
			Robo	1	16,67	33,33
			Transporte inseguro de medios de datos	1	16,67	33,33
Cantidad de factores de riesgo = 6						200,00

ANEXO I – ANÁLISIS DE RIESGOS

Nº Activo	Nombre del Activo	Nivel de Importancia	Factor de Riesgo	Probabilidad de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
13	Datos de usuarios.	1	Falta de espacio de almacenamiento	1	10,00	10,00
			Mala configuración del schedule de backups	1	10,00	10,00
			Medios de datos no están disponibles cuando son necesarios	1	10,00	10,00
			Pérdida de backups	2	20,00	20,00
			Perdida de confidencialidad en datos privados y de sistema	1	10,00	10,00
			Portapapeles, impresoras o directorios compartidos	1	10,00	10,00
			Robo	1	10,00	10,00
			Sabotaje	1	10,00	10,00
			Spoofing y sniffing	1	10,00	10,00
			Virus	3	30,00	30,00
	Cantidad de factores de riesgo = 10					130,00

5- CONCLUSIONES

5.1 NIVELES DE VULNERABILIDAD

En el cuadro se listan los niveles de vulnerabilidad y los porcentajes de riesgo para cada activo, considerando distintos rangos de valores para la importancia, de 1 a 10, de 1 a 3 y sin tener en cuenta la importancia (es decir con un valor de 1). A la derecha los valores que observamos representan el número de los activos, ordenados en forma descendiente de acuerdo al riesgo que corren dicho activos.

<i>Activos</i>	Niveles de vulnerabilidad						Activos ord. Desc.		
	Imp. (1 a 10)	R %	Imp. (1 a 3)	R %	Imp. (1)	R %	1a10	1a3	S/ imp (1)
1 Datos de usuarios.	130	1,2	130	3,4	130	7,5	1	2	4
2 Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	200	1,8	100	2,6	100	5,8	2	3	2
3 Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	300	2,8	100	2,6	100	5,8	3	1	3
4 Cableado, antenas, routers, switch, bridge.	600	5,5	200	5,3	100	5,8	4	4	7
5 Usuarios.	844	7,8	338	8,9	169	9,7	8	6	10
6 Red.	785	7,2	262	6,9	131	7,5	6	8	1
7 Datos en tránsito, datos de configuración, datos en medios externos.	1000	9,2	375	9,9	125	7,2	5	5	12
8 Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	629	5,8	314	8,3	157	9,1	7	7	6
9 Backup.	1177	10,8	392	10,4	131	7,5	9	10	9
10 Bases de datos.	1263	11,6	379	10,0	126	7,3	11	12	11
11 Software de aplicación, programas fuente, sistemas operativos.	1221	11,3	407	10,8	136	7,8	10	9	8
12 Servidores y switch central.	1300	12,0	390	10,3	130	7,5	12	13	5
13 Administrador de sistemas (Departamento de sistemas).	1400	12,9	400	10,6	200	11,5	13	11	13
	10848,45	100	3786,72	100	1734,46	100			

5.2 ANÁLISIS DE IMPORTANCIAS

Aquí vemos un análisis donde se tiene en cuenta el nivel de vulnerabilidad obtenido con una ponderación de la importancia de 1 a 10. Se calculó el porcentaje de los riesgos y el porcentaje de la importancia. Al calcular la diferencia entre estos porcentajes (Dif. de %) se obtiene el porcentaje que muestra cuán sobrevaluados o menospreciados están los activos de acuerdo a sus riesgos. A continuación se calcula el número que representan los porcentajes anteriormente mencionados, de la siguiente manera:

- Para aplicar la diferencia de porcentajes a la importancia actual, se multiplican.

Imp. x Dif. de %

- Este resultado no está en escala de 1 a 10, por lo que con una regla de tres simple, se centran los valores:

100 % ----- 10 puntos de importancia

Imp. x Dif. de % ----- ? (= Diferencia de importancia)

A este resultado se le suma (o resta de acuerdo al signo) a la importancia actual, obteniendo la importancia que debería tener cada activo (importancia ideal), de acuerdo al nivel de riesgos encontrado.

Importancia ideal = Importancia actual + Diferencia de importancia

Orden de Activos		<i>Activos</i>	Σ Riesgo (nivel de vulnerab.)		Importancia (actual)		<i>Dif.</i> <i>de</i> %	<i>Dif. de</i> <i>Imp.</i>	Importancia (ideal)
según (Imp. Actual)	según (Imp. Ideal)			%		%			
1	1	1 Datos de usuarios.	130	1,20	1	1,25	-0,05	-0,01	0,99
2	2	2 Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	200	1,84	2	2,50	-0,66	-0,13	1,87
3	3	3 Hardware (teclado, monitor, unidades de discos, medios removibles)	300	2,77	3	3,75	-0,98	-0,30	2,70
8	5	4 Cableado, antenas, routers, switch, bridge.	629	5,79	6	7,50	-1,71	-1,02	4,98
5	4	5 Usuarios.	600	5,53	5	6,25	-0,72	-0,36	4,64
4	8	6 Red.	785	7,23	6	7,50	-0,27	-0,16	5,84
6	6	7 Datos en tránsito, datos de configuración, datos en medios externos.	1400	12,91	8	10,00	2,91	2,32	10,32
13	9	8 Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	844	7,78	4	5,00	2,78	1,11	5,11
7	11	9 Backup.	1000	9,22	9	11,25	-2,03	-1,83	7,17
9	10	10 Bases de datos.	1221	11,26	10	12,50	-1,24	-1,24	8,76
11	12	11 Software de aplicación, programas fuente, sistemas operativos.	1177	10,85	9	11,25	-0,40	-0,36	8,64
10	13	12 Servidores y switch central.	1263	11,64	10	12,50	-0,86	-0,86	9,14
12	7	13 Administrador de sistemas (Departamento de sistemas).	1300	11,98	7	8,75	3,23	2,26	9,26
			10848,45	100	80	100	0	-1	79

5.3 VALORES MÁXIMOS, MÍNIMOS Y REALES

Se muestran los valores máximos y mínimos de vulnerabilidad que pueden obtener los activos cuando las probabilidades son llevadas a puntos extremos. Este cálculo es necesario para compararlos con los valores relevados que figuran en la tercera columna. Estos cálculos se realizan sin tener en cuenta la influencia de la importancia, es decir se representan exclusivamente las debilidades de cada activo, con las medidas de seguridad que actualmente existen en la empresa.

Activos - Riesgos totales (Sin ponderar la importancia)	(333)	%	(111)	%	(123)	%
1 Datos de usuarios.	300	7,7	100	7,7	100	5,8
2 Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	300	7,7	100	7,7	100	5,8
3 Hardware (teclado, monitor, unidades de discos, medios removibles, etc.)	300	7,7	100	7,7	100	5,8
4 Cableado, antenas, routers, switch, bridge.	300	7,7	100	7,7	125	7,2
5 Usuarios.	300	7,7	100	7,7	126	7,3
6 Red.	300	7,7	100	7,7	130	7,5
7 Datos en transito, datos de configuración, datos en medios externos.	300	7,7	100	7,7	130	7,5
8 Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	300	7,7	100	7,7	131	7,5
9 Backup.	300	7,7	100	7,7	131	7,5
10 Bases de datos.	300	7,7	100	7,7	136	7,8
11 Software de aplicación, programas fuente, sistemas operativos.	300	7,7	100	7,7	157	9,1
12 Servidores y switch central.	300	7,7	100	7,7	169	9,7
13 Administrador de sistemas (Departamento de sistemas).	300	7,7	100	7,7	200	11,5
	3900,00	100	1300,00	100	1734,00	100
	100 - max	%	33 - min	%	actual	%

5.4 PORCENTAJES DE RIESGOS CUBIERTOS

Como consecuencia del cuadro anterior, se puede calcular que el porcentaje de riesgos descubiertos en la empresa es del 44,5% (1734 puntos), considerando el nivel máximo de riesgos como el 100% (3900 puntos), y sabiendo que el porcentaje mínimo es de 33,3% (1300 puntos). Por esto podemos concluir que la empresa debería reducir en 11,2% el porcentaje de riesgos descubiertos, para así conseguir el nivel mínimo de riesgos posible.

<i>Porcentaje de riesgos descubiertos:</i>	<i>44,5 %</i>
<i>Porcentaje de riesgos mínimo:</i>	<i>33,3 %</i>
<i>Desviación:</i>	<i>11,2 %</i>

ANEXO II – CUESTIONARIOS

1- RELEVAMIENTO INICIAL

Para el desarrollo de la presente auditoría fue necesario entrevistar a distintos usuarios del sistema y demás personas que interactúan con él. En el presente anexo se adjuntan los cuestionarios utilizados para la realización de éstas entrevistas.

1.1 HARDWARE

- Topología y protocolos de red
 - Protocolos
 - Conexión al exterior con sucursales y fábrica
- Características del servidor:
 - tipo o marca de servidor,
 - capacidad de procesamiento,
 - cantidad de memoria,
 - capacidad de disco,
 - placas de red,
 - dispositivos varios (CD's, cintas, scanner, switch, hub, etc.),
 - UPS o sistemas de alimentación alternativa del servidor,
 - servidor alternativo, espejo o de contingencia,
 - servidor de datos o de impresión,
- Impresoras y Gestión de impresión
- PC's
 - Cantidad
 - Características particulares
 - Terminales o PC's
 - Clones o de marcas
 - Características generales
- Web
 - Tipo de conexión
 - Permisos o acceso de las PC's
 - Firewall y virus wall
 - Página dinámica o estática
 - Servidor propio o web hosting.
- Back up
 - Disco espejo
 - Tercerización
 - Dispositivos de back up (CD's, cintas magnéticas, HD, disquete, etc.)

1.2 SOFTWARE

- Software del servidor
 - OS
 - Aplicaciones
 - Motor de bases de datos
- OS y software de las PC's
- Aplicaciones bases en cada sector de la empresa (administración, ventas, cómputos, etc.)
- Gestión de virus.

- Detalle de aplicaciones propias, enlatadas
- Gestión de red física y lógica
- Licencias.

1.3 USUARIOS

- Organigrama.
- Responsabilidades en área de informática
 - Responsables de Redes
 - Responsables de Bases de datos
 - Responsables de Aplicaciones
 - Responsables de Servicio técnico
- Tipo de perfiles de usuarios según sectores
 - Clasificación del perfil
 - Accesos del perfil a aplicaciones o datos.

2- SEGURIDAD LÓGICA

2.1 IDENTIFICACIÓN – ID’S

2.1.1 *Altas*

- ¿Qué datos hay en el perfil del usuario cuando se hace un alta? ¿Se guardan los siguientes datos?
 - ID de usuario,
 - Nombre y apellido completo,
 - Puesto de trabajo y departamento de la empresa,
 - Jefe inmediato,
 - Descripción de tareas,
 - Consentimiento a que auditen sus actividades en el sistema, y de que conoce las normas de “buen uso” del sistema,
 - Explicaciones breves y claras de cómo elegir su password,
 - Tipo de cuenta o grupo al que pertenece (empleado, gerente, etc.),
 - Fecha de expiración de la cuenta,
 - Datos de los permisos de acceso y excepciones,
 - Restricciones horarias para el uso de recursos,
- ¿Que otros datos del usuario son necesarios en el ID? ¿Que datos guardan en la planilla de personal?
- ¿El ID de usuario puede repetirse? ¿Y si una cuenta fue borrada o eliminada, puede utilizarse un ID ya usado y eliminado para un usuario nuevo?

2.1.2 *Bajas*

- ¿Cómo se relacionan con los de RRHH? ¿El departamento de RRHH se encarga de comunicar las modificaciones en el personal? ¿Qué se hace al respecto? ¿Cómo se actualiza la lista?
- ¿Cómo se administran los despidos (o desvinculación del personal)? ¿Se tiene en cuenta una política de despidos para evitar actos de vandalismo por posibles disgustos de los empleados desvinculados de la empresa?
- ¿Hay algún histórico de las cuentas que se dan de baja?
- ¿Se guardan los archivos y datos de las cuentas eliminadas? ¿Por cuánto tiempo? ¿Qué datos se guardan? ¿Con qué motivo?

2.1.3 *Mantenimiento*

- ¿Hay procedimientos para asignar los usuarios a un grupo de acuerdo a ciertas características?
- ¿Hay procedimientos para dar de alta, baja, modificar, suspender, etc. una cuenta de usuario?
- ¿Se hacen revisiones de las cuentas de usuarios? ¿Se revisan sus permisos?
- ¿Hay procedimientos para determinar los nuevos requerimientos relacionados con cambios en funciones del empleado? ¿Cómo se mantienen actualizadas las cuentas cuando esto pasa?
- ¿Se documentan las modificaciones que se hacen en las cuentas? ¿Se lleva un histórico de los cambios?

2.1.4 Permisos

- ¿Tienen una clasificación de los recursos (datos) en base a la sensibilidad?
¿O en base a los tipos (base de datos, archivos de configuración, datos personales, según el departamento de la organización.)? ¿Cómo se define la sensibilidad de los objetos?
- ¿Tienen distinción de los tipos de accesos que tiene cada usuario a cada recurso? (lectura, escritura, etc.)
- ¿Quién les asigna los permisos a los usuarios?

2.1.5 ID inactivas

- ¿Después de qué período de inactividad en que el usuario no realiza acciones en el sistema, se limpia la pantalla asociada al usuario, se desconecta el usuario inactivo o pide la password de nuevo?
- Antes de terminar con la sesión, ¿se avisa al usuario que se lo desconectará? Si en un determinado tiempo el usuario no responde, ¿entonces se termina la sesión?
- ¿Después de qué período de inactividad (de cuantos días) se pone una cuenta de usuario como inactiva, porque el usuario no se ha logeado? ¿Este proceso es automático (del sistema operativo) o lo realiza el administrador?

2.1.6 Acciones correlativas a usuarios

- ¿Los usuarios se identifican en forma única o existen usuarios genéricos que todas las personas usan? ¿Todos los usuarios tienen un perfil o pertenecen a algún grupo?
- ¿El sistema genera históricos o logs de las actividades de los usuarios en el sistema, para poder seguirles el rastro?
- ¿Tienen forma de asignar responsabilidades individualmente a cada usuario, identificándolo a través de su ID?

2.1.7 Grupos - Roles

- ¿Existen grupos de usuarios? ¿Cómo se forman los grupos? ¿Según el departamento de la empresa donde trabajen, según el rol que desempeñen? ¿Por qué esa clasificación?
- ¿El acceso puede controlarse con el tipo de trabajo o la función (rol) del que pide acceso?
- ¿Los ID hacen referencia a una persona, o son anónimos? ¿Hacen referencia a un grupo?
- ¿Se eliminan los que vienen por default en el sistema operativo? (Cuentas Guest, por ejemplo)

2.1.8 Súper usuario

- ¿Qué tipos de perfil de administrador hay?
- ¿Cuántas personas y quiénes son administradores?
- ¿Desde qué terminal puede logearse un administrador?
- Además de la cuenta de administrador, ¿tienen otra cuenta para las funciones comunes?

2.1.9 Display

- ¿Qué datos se muestran cuando alguien intenta logearse? ¿Se muestran los siguientes datos?
 - Nombre de usuario
 - Password
 - Grupo o entorno de red
 - Estación de trabajo
 - Fecha y hora
- ¿Qué datos se muestran cuando alguien logra logearse? ¿Se muestran los siguientes datos?
 - Fecha y hora de la última conexión.
 - Localización de la última conexión (Ej. número de terminal)
 - Intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.

2.1.10 Varios

- ¿Utilizan el ID de usuario como un control de acceso a los recursos, o solo para ingreso al sistema?
- ¿Un usuario puede tener solo una sesión abierta, de alguna aplicación, de acuerdo a sus tareas o puede tener varias? ¿Depende de la cantidad de grupos a los que pertenezca?

2.2 AUTENTICACIÓN

2.2.1 Datos de autenticación

- ¿Cómo se protegen los datos de autenticación cuando están siendo ingresados por el usuario? ¿Qué se muestra en pantalla cuando se tipea el password? ¿Espacios, asteriscos, no se mueve el cursor?
- ¿Cómo se guardan los datos de autenticación en disco? ¿Encriptados? ¿Bajo password? ¿De que forma se los asegura?
- ¿Cómo se restringe el acceso a estos datos? ¿Hay un control de acceso más severo con estos datos? ¿Se los clasifica como confidenciales?
- ¿Quién tiene acceso a estos datos?
- ¿Cómo se transfieren los datos de autenticación desde la terminal que se logea hasta el servidor encargado de autenticar? ¿Encriptados, o solo en texto plano?

2.2.2 Alcance de la autenticación

- ¿Que alcances tienen las autenticaciones? ¿Es una autenticación para una aplicación en particular, para toda la red, o solo para la LAN, y otra para la WAN?

2.2.3 Límites de los intentos de logeo

- ¿Se lockea el usuario después de varios intentos fallidos de autenticación o se inhabilita la cuenta o la terminal?
- ¿Después de cuantos intentos?

- ¿Que se hace después de la inhabilitación: se espera un tiempo y muestra nuevamente la pantalla de logeo o el administrador debe aprobar la operación de re-logeo?

2.2.4 Firmas digitales

- ¿Se usan firmas digitales para autenticar a los usuarios dentro de la organización, cuando mandan mensajes internos? ¿Y para mensajes externos?
- ¿Serían necesarias para algún documento?

2.2.5 Varias

- Interoperatividad: ¿De qué forma se “ponen de acuerdo” Windows y LINUX para la autenticación? ¿Es necesaria esa interoperatividad para algo? ¿Es necesaria alguna herramienta para esta comunicación?
- Separación de tareas: ¿Se manejan los controles de acceso de manera que una sola persona no tenga acceso a todo, en relación a una sola transacción? ¿Existe separación de tareas a través del control de acceso?
- Rotación de tareas: si existe rotación de tareas, ¿cómo es el mecanismo en el control de acceso para posibilitar esto? ¿Se modifican los permisos? ¿O tienen todos los permisos necesarios permanentemente?
- Vacaciones: ¿son obligatorias las vacaciones en la empresa? Si es así, ¿cómo se manejan con las passwords durante los períodos de vacaciones? ¿Que ocurre con la cuenta del administrador en el período de vacaciones? ¿Puede ser modificada? ¿Cómo controlan que no sea modificada durante su ausencia?

2.3 PASSWORDS

2.3.1 Generación

- ¿Las passwords son generadas con procesos automáticos (programas de generación de passwords) o son creadas por los usuarios? ¿Se usan estos programas en alguna máquina, por ejemplo en los servidores?
- ¿Qué características deben tener estas passwords?
 - ¿Cuál es el conjunto de caracteres permitidos (alfa, numéricos y caracteres especiales)?
 - ¿Cuál es el largo mínimo y máximo del password (seis a ocho, preferentemente nueve)?
 - ¿La password se inicializa como expirada para obligar al cambio?
 - ¿De qué forma se hace cumplir este requerimiento? ¿Se pone una fecha de expiración? ¿No se permite al usuario logearse ya que su password ha expirado?
- ¿Se chequean contra un diccionario on line para verificar que no sean palabras que existan?
- ¿Se permite que contengan el nombre de la empresa, o el nombre del usuario?
- ¿Dos cuentas pueden tener las mismas passwords?
- Si existe más de una cuenta de administrador, ¿algunas de estas (o todas) tienen las mismas passwords?

- ¿El password puede ser igual al ID del usuario?

2.3.2 *Cambios*

- ¿Qué procedimiento existe para el cambio de las passwords de los usuarios?
¿Se puede cambiar en cualquier momento?
- ¿Quién puede hacer los cambios? ¿El administrador? ¿Los usuarios a través de una opción en el menú? ¿Le tienen que avisar a alguien cuando cambian la contraseña? ¿Tiene que pedir autorización?
- ¿Qué procedimiento existe para comprobar que las passwords asignadas por default (por el administrador o por el sistema operativo) han sido cambiadas por el usuario?
- ¿Cuál es el procedimiento para manejo de password perdidas o reveladas?
¿Cómo se cambian? ¿Solo se cambia la password o se cambia también la cuenta y el nombre del usuario?
- ¿Con qué frecuencia es necesario cambiar la password antes que se vuelva obsoleta?
- Al modificar la password de una cuenta, ¿se puede repetir la misma password?
- ¿Se guarda una base de datos con las últimas password de los usuarios?
¿Cuántas passwords de cada usuario se guardan?

2.3.3 *Entrenamiento a usuarios*

- ¿Se entrena a los usuarios en la administración del password? ¿Se les enseña a:
 - no usar passwords fáciles de descifrar?
 - no divulgarlas?
 - no guardarlas en lugares donde se puedan encontrar?
 - entender que la administración de passwords es el principal método de seguridad del sistema?

2.4 CONTROL DE ACCESO LÓGICO

- Modelos de control de acceso: ¿Siguen algún tipo de modelo o mecanismo estándar de control de acceso? ¿Sería factible y económico implementar uno?
- Aplicación: ¿para el control de acceso usan una aplicación? ¿Cómo se administra? ¿Qué características tiene? ¿Esta aplicación es:
 - Propia del sistema operativo?
 - De aplicación y programas propios o comprados?
 - Con paquetes de seguridad agregados al sistema operativo?

2.4.1 *Criterios de acceso*

- ¿Qué criterio usan para el control de acceso? ¿Alguno de los siguientes?:
 - Identidad (ID de usuario)
 - Roles
 - Localización: ¿existen controles de acuerdo a la localización de la información?
 - Recursos: ¿se pide un password cada vez que alguien quiera entrar a una carpeta compartida del servidor de Linux? ¿El password que los usuarios ingresan para la aplicación de la empresa sirve para explorar el sistema y así

poder ver las carpetas de los servidores? ¿Es necesario poner otro password además del login?

- Tiempo: ¿se limita el momento del día (o del año) en el que un usuario puede entrar al sistema? ¿Cómo? ¿Que días, horas? ¿Con qué aplicación?
- Limitaciones a los servicios: ¿Existen restricciones de servicio? ¿Cómo?
- Modos de acceso:
 - ¿Si el acceso es desde módem existen distintos permisos que desde terminal?
 - ¿Se toma en cuenta el número de teléfono al comunicarse vía módem?
 - ¿Usan un sistema call-back?
- Transacción: ¿se permite hacer ciertas transacciones a unos usuarios que otros no pueden hacer? ¿Dependiendo de qué? ¿Del tipo de usuario y del grupo?
- Aplicación: ¿se restringe el acceso a ciertos programas a ciertos usuarios? ¿Cómo?

2.4.2 *Mecanismos de control de acceso interno*

¿Cuáles de estos mecanismos de control de acceso se usan?

- Passwords
- Listas de control de acceso (ACL)
 - ¿Existe una ACL o matriz, o algo similar donde se especifiquen los usuarios y los accesos que tienen?
 - ¿Qué sería más conveniente, una lista o una matriz? ¿Por qué?
 - ¿Con qué aplicaciones se manejan? ¿Con alguna del sistema operativo, o con otro software?
 - ¿Cómo se actualiza? ¿En forma manual o, si se modifica la lista de usuarios del sistema, se actualiza automáticamente la ACL? ¿Con qué frecuencia se revisa y actualiza?
 - ¿Se usa encriptación para almacenarla? ¿Se protege de alguna manera? ¿Qué sería lo mejor y por qué para protegerla?
- Interfaces de usuarios restringidas
 - ¿Se restringen las interfaces que ven los usuarios, (como el escritorio de Windows) de manera que los usuarios solo vean lo que les está permitido?
 - ¿Cómo se hacen las restricciones? ¿Con la vista de menús?
 - ¿Los usuarios solo ven una determinada vista o ciertas tablas de las bases de datos?
- Encriptación: ¿se encriptan algunos datos? ¿Cuales?
 - ¿Las ACL?
 - ¿Los mensajes?
 - ¿Las passwords y datos de las cuentas de usuarios?
 - ¿Los datos de configuración?
 - ¿Los datos críticos de la empresa?
 - ¿Los datos que están siendo transmitidos (internamente en la Lan o externamente a través de Internet o el módem)?
- Protección de puertos: ¿usan dispositivos externos físicos para proteger el puerto de los intrusos (llaves de hardware, por ejemplo)?

2.4.3 Control de acceso externo

- Mecanismos de control de acceso externo:
 - Gateways (puertas de seguridad) o firewalls seguros
 - Acceso de personal contratado, consultores o mantenimiento
 - Autenticación basada en host: ¿existe una autenticación que da acceso al sistema basándose en la identidad del host que pide el acceso, y no en la identidad del usuario que quiere entrar?
- ¿Existe acceso externo a los datos, desde Internet o desde el módem? ¿Quién tiene ese acceso?
- ¿Qué procedimientos se tienen en cuenta para mantener la integridad y la confiabilidad de los datos? ¿Se tienen en cuenta los siguientes?
 - ¿Alguna forma de identificación o autenticación?
 - ¿Control de acceso para limitar lo que se lee, ve, borra, modifica, etc.?
 - ¿Firmas digitales?
 - ¿Ponen las copias de seguridad de la información pública, en otro lado, no en la misma máquina?
 - ¿Prohíben el acceso público a bases de datos “vivas” (live data base o bases de datos)?
 - ¿Verifican que los programas y la información pública no tenga virus?
 - ¿Passwords one-time?
 - ¿Están separados los datos que se publican en Internet de los datos del interior de la empresa?
 - ¿Son los mismos datos o están en PC's diferentes?
 - ¿Usan alguna forma de acceso remoto para cambiar las configuraciones de un sistema?

2.5 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

- ¿Ha habido intentos de intrusión? ¿Vale la pena implementar un sistema como estos?
- ¿Se usa algún software de IDS? ¿Son tolerantes al fallo? ¿Usan muchos recursos? (Ejemplos: OmniGuard, RealSecure, Cisco Secure IDS)
- ¿Se usan herramientas de monitorización de red para encontrar intrusos?
- ¿Se releen los logs de auditoria buscando pistas de IDS? ¿Se buscan algunas de las siguientes?
 - Muchos intentos fallidos de autenticación,
 - Tráfico excesivo de red,
 - Muchas violaciones a permisos.
- Si hubiera una entrada de un intruso, ¿se documenta? ¿Que medidas se tomarían (o tomaron) para que no ocurra más?

2.6 DENIAL OF SERVICE

- ¿Se llevan a cabo algunas de las siguientes actividades?
 - ¿Instalan ACL en los routers?
 - ¿Quitan los servicios de red no necesarios o no utilizados, por ejemplo: ECHO, etc.?
 - ¿Separan los datos críticos de los que no lo son, a través de lo que haya disponible, como por ejemplo: sistemas de cuotas (disk QUOTAS, o particiones, o volúmenes)?

- ¿Establecen valores base para la actividad normal, en cuanto a memoria, utilización de disco, de la CPU o tráfico de red?
- ¿Usan herramientas para detectar cambios en la configuración o en los archivos?
- ¿Usan configuraciones redundantes de red y tolerantes a fallos?

3- SEGURIDAD EN LAS COMUNICACIONES

3.1 CONFIGURACIÓN DE RED

3.1.1 *Activos de la red*

- ¿Cómo es la topología de la red? ¿Existe un inventario o gráfico topológico? Debería incluir lo siguiente:
 - switch,
 - routers,
 - hub's,
 - modem,
 - PC's,
 - conexiones de radio,
 - fibra óptica,
 - etc.
- ¿Cuántos dispositivos de esta lista hay y en que forma están ubicados y utilizados?
- ¿Qué filtros tiene cada uno de estos dispositivos?
- ¿Existe encriptación a nivel de hardware?
- ¿Por qué pusieron un switch en lugar de un router? ¿Por el costo? ¿Por el tamaño de la red?
- ¿Por qué implementaron un sistema radial? ¿Es demasiado inseguro? ¿No es muy caro?

3.1.2 *Servidor de Hosting*

- ¿Qué se tuvo en cuenta para elegir ese servidor de hosting?
 - precio,
 - medidas de seguridad,
 - respaldo en caso de emergencia, de caída del servidor y de pérdida de info.
- ¿Qué características tienen los servidores? (de mail, de Internet, de datos o aplicaciones).
- ¿Causa alguna dificultad que el servidor esté físicamente lejos de las sucursales?

3.1.3 *Comunicaciones*

- Con respecto al MODEM con el que se comunican con la fabrica:
 - ¿Pasa por el firewall?
 - ¿Los datos van encriptados?
- ¿Se realizan los controles de acceso adecuados a los servidores que se encuentran conectados a Internet?

3.1.4 *Recursos compartidos*

- ¿Se comparten los discos de las PC's en la red? ¿Por que?
 - ¿Que carpetas comparten?
 - ¿Se pueden ver las carpetas de los mails de mis compañeros?

- ¿Tienen contraseñas estas carpetas? ¿Quién pone las contraseñas: el dueño de la información o el administrador?

3.1.5 Configuración de puertos

- ¿Se deshabilitaron los puertos que no son necesarios? ¿Cuáles? ¿De qué protocolos o servicios? ¿Quién lo hizo?
- ¿Se prueban los puertos de la red? ¿Y el firewall? ¿Con qué herramientas?
- ¿Se ha hecho una prueba de auto hackeo?
- ¿Con qué herramientas se prueban o pueden probar los puertos? ¿Solo con el SQuid? ¿Por qué no usaron otro programa?

3.1.6 Testeo mensual de la red

- ¿Se hace algún chequeo periódico de la red y sus permisos?
- ¿Qué se controla?
- ¿Se documentan la ejecución y los resultados de estas pruebas?

3.1.7 Acceso remoto

- ¿Cómo se mantienen las máquinas con Linux? ¿Vía acceso remoto? ¿Quién las mantiene?
- ¿Qué herramientas se usan? ¿Cómo funciona la herramienta?
- ¿Se debe cambiar la configuración del firewall para hacer este acceso remoto?
- ¿Qué servicios son necesarios para el mantenimiento (HTML, FTP, IP, DNS, TELNET)? ¿El firewall no tiene restricción en ese servicio, se le saca la restricción del servicio al firewall o solo habilito una dirección específica, la de la máquina desde donde se hace el mantenimiento?
- ¿Qué es lo que se mantiene con este sistema?
- ¿Cómo se aseguran que no entren llamadas, sino que solo salgan los pedidos?

3.1.8 Medidas de fiabilidad

- ¿Existen medios alternativos de transmisión de datos en caso de que exista alguna contingencia con la red? ¿Que se haría si se cae un nodo? ¿Está prevista esa situación?
- ¿Existe una redundancia de acceso a Internet? (si no funciona ADSL tener un dial up configurado)

3.2 MAIL – CHAT

3.2.1 Herramientas

- ¿Con qué herramienta administran el correo en el servidor y cómo se hace?
- ¿Es una herramienta del sistema operativo? ¿Es comprada? ¿Por qué eligieron esa?
- ¿Es configurable?
- ¿Quién es el encargado de su configuración?
- ¿Se chequea periódicamente que la configuración sea eficiente? ¿Con qué frecuencia? ¿Se encuentran errores?

- ¿Se actualiza a las versiones más nuevas de esta herramienta? ¿Cómo se enteran de las nuevas versiones?
- ¿El servidor de mail es el mismo que el servidor de Internet o el de aplicaciones?
- ¿Con qué herramienta los usuarios leen sus mail? ¿Lo hacen desde sus PC's?
- ¿Qué configuraciones tienen estas herramientas?
 - Habilitada la vista previa
 - Confirmación de lectura
 - Block sender
 - Chequeo de virus en correo entrante y saliente
 - Controles ACTiveX y Scripts
- ¿Quién las configura? ¿Los usuarios o el administrador? ¿Todas las PC's tienen la misma configuración?
- ¿Cómo configuran el IncrediMail?
- ¿Se le deshabilitan las mismas características que nombré arriba?

3.2.2 *Proceso de recepción y envío de mails*

- ¿Cómo es el proceso de recepción de mail? ¿El servidor baja los mails de toda la empresa a sus discos, y luego los reparte a sus destinos?
- ¿Los mails se borran del servidor cuando son descargados a la máquina del usuario? ¿O no se borran nunca del servidor? ¿Cómo es esta política?
- ¿Los mensajes están comprimidos dentro del servidor?
- ¿Automáticamente se envían los mail a cada cuenta de usuario cuando llegan al servidor o se guardan en disco del servidor y se envían en un determinado momento (por ejemplo, varias veces al día, o cuando el usuario lo solicita)?
- Al recibir cualquier tipo de mail, ¿existen mecanismos de filtrado que nos permiten buscar ciertas frases o palabras dentro del encabezado o cuerpo del mensaje? ¿Podemos determinar si hay algún mail con un determinado asunto, de manera de evitar los virus o los correos no deseados?

3.2.3 *Espacio en disco*

- ¿Cómo se administra la capacidad de disco asignada a los mails?
 - ¿Se asigna un espacio de disco a la totalidad del correo?
 - ¿Se asigna un espacio de disco a cada usuario del mail?
 - ¿Se asigna un espacio de disco a cada cuenta de mail?
 - ¿Se asigna un espacio de disco a cada departamento?
 - ¿Existen distintas cantidades asignadas a los usuarios de acuerdo a su perfil o grupo, o todos los usuarios tienen la misma cantidad de espacio en disco?
- ¿Que pasa si se llega al límite de espacio en disco asignado? ¿Ha pasado alguna vez? ¿Se le avisa al usuario correspondiente que limite el uso de su cuenta de mail? ¿Se puede suspender solo su servicio de mail sin afectar el resto de la empresa?
- ¿Cuándo se suspende la recepción de mails? ¿Cuando se ha llenado el servidor o antes, para poder hacer algo para vaciarlo?
- ¿Existe un límite para los mensajes de salida o de entrada?

3.2.4 *Mail Interno y Externo*

- ¿Existen direcciones de mail para todos los empleados? ¿Solo algunos empleados tienen? ¿De qué depende este servicio?
- ¿Ese mail es interno o también existe una casilla para mail externo para cada empleado?
- ¿Cómo funciona el mail interno, va al hosting y después al servidor de correo o va directamente al servidor de correo?
- ¿Existe algún tipo de control para asegurarse que los usuarios no usan el mail de la empresa para fines personales sino para su trabajo?
- ¿Se controla que no se suscriban a listas de correo o cadenas de mails con esta dirección de mail?
- ¿Controlan los SPAMS en estas direcciones? ¿Cómo lo hacen?
- Al enviar mails hacia todos los empleados, ¿la lista se oculta con el CCO o copia oculta, o se los lista en el campo de TO?
- ¿Permiten el conocimiento público de las direcciones externas de mails de los empleados?
- ¿Están publicadas en Internet o solo las administran sus propietarios?
- ¿Existen direcciones de mails destinadas a la comunicación con el cliente, como el libro de quejas, consultas, etc.(Ej. ventas@laempresa.com)? ¿En donde se encuentran? ¿Quién las administra? ¿El departamento correspondiente o el administrador de web?

3.2.5 *Correo basura*

- ¿Cómo se identifica al correo basura?
- ¿Cómo se administra el correo basura?
- ¿Con qué herramienta lo hacen? ¿Cómo se configura?
- ¿Cómo se define qué es correo basura y qué no?
- ¿Qué pasa si a una cuenta llega gran cantidad de correo basura?
- ¿El correo basura se elimina directamente o es posible generar logs para su posterior análisis?
- ¿Qué conclusión se ha sacado de esos análisis?
- ¿El correo basura se baja hasta el servidor de mails y desde ahí se elimina, o directamente se elimina antes de ser bajado, en el ISP? ¿Cómo lo administra el ISP?

3.2.6 *Chat*

- ¿Se permiten los servicios de chat?
- ¿Cuáles se usan? MSN, ICQ, Yahoo! ¿Chat? ¿Otros?
- ¿Se permite bajar archivos a través de estos programas?
- ¿Se usan programas de file sharing (Morfeus, Kazaa, Napster, Audio Galaxy, iMesh, eDonkey2000, etc.)?

3.2.7 *Copia de seguridad*

- ¿Se genera una copia de seguridad de los mensajes enviados y recibidos? ¿De todos? ¿Se guardan en el disco? ¿Se comprimen?
- ¿Se hacen back up de las carpetas del SendMail (como las dbx del Outlook Express)?
- ¿Se imprimen para su control o para que conste en algún archivo en papel?

- ¿Poseen un sistema propio de mail record definido o alguna herramienta automática de gestión de mails record?

3.2.8 *Privacidad – Firma digital – Encriptación de mails*

- ¿Prohíben el envío de archivos de la empresa u otros documentos confidenciales vía mail?
- ¿Se toman medidas de seguridad especiales cuando el mensaje de salida tiene datos confidenciales? ¿Se exige que vaya firmado, o encriptado? ¿Se exige que la dirección de destino sea conocida o confiable?
- ¿Se utiliza la firma digital en algún tipo de mensajes? ¿Qué tipo de firma se usa?
- ¿Se usa para mensajes externos e internos?
- ¿La clave privada de la firma digital es realmente privada, o la utilizan las secretarías (por ejemplo) para mandar mensajes en nombre de sus jefes? ¿Cómo se controla esto?
- ¿Utilizan la priorización de mail para la encriptación de los mismos?
- ¿Que sería importante proteger, en el caso de mensajes internos y externos?:
 - ¿Integridad?
 - ¿Confidencialidad?
 - ¿No repudio?
 - ¿Autenticación del remitente?
- ¿Se pide generalmente una confirmación de lectura en los mails salientes? ¿En todos, solo en los que tienen datos confidenciales, o cuando el usuario los configura?
- ¿Se encriptan los datos confidenciales que se guardan en disco (ejemplo: EFS – Encrypted File System - de Microsoft)?
 - ¿Archivo con contraseñas?
 - ¿Archivos de configuración?
 - ¿Archivos top secret?
 - ¿Qué otros datos se encriptan?

3.3 **VIRUS – ANTIVIRUS**

3.3.1 *Herramientas*

- ¿Cuáles de éstas medidas o herramientas poseen para evitar los virus?
 - Paquetes de software antivirus
 - Firewalls
 - Sistemas de detección de intrusos
 - Monitorización para evaluar el tráfico de red y detectar anomalías, como la acción de troyanos.
 - Creación de un disco de rescate o de emergencia
 - Procedimientos para cuando ocurra una infección con virus.
 - Hardware de seguridad de red dedicado
 - Back up de datos
- ¿Está habilitada alguna herramienta antivirus mientras se envían y reciben mails? ¿Cuál? ¿Por qué se usa esa?
- ¿Están seguros que detecta los virus y los elimina correctamente?
- ¿Han probado con otra herramienta?
- ¿Qué precio tiene el antivirus que compran? ¿Y las actualizaciones?

- ¿Hay un antivirus instalado en cada PC (incluyendo los servidores) o hay un solo antivirus en toda la red?
- ¿Que significa que el antivirus sea corporativo? ¿Uno para los servidores y otra versión para los clientes? ¿En qué se diferencian?

3.3.2 *Mensajes infectados – Procedimientos*

- ¿Se han detectado mensajes infectados? ¿Que problemas trajo? ¿Era de Windows o de Linux? ¿Cómo lo solucionaron?
- Si se encuentra un mail con virus, ¿qué se hace para que no lleguen más de esa misma persona? ¿Se identifica la fuente del mail, para bloquearla desde el router o desde el servidor de correo? ¿Se avisa al ISP para que no deje entrar más mails de esa dirección? ¿Se observan los headers de los mails para identificar su origen verdadero?
- Si las disqueteras están activadas en las PC's de los usuarios, ¿cómo se aseguran que los usuarios analicen los disquetes antes de abrir archivos?
- ¿Se generan disco de rescate con el antivirus? ¿Para todas las máquinas o solo para los servidores? ¿Quién es el encargado de esto? ¿Alguna vez han sido necesarios?
- ¿Cómo es la protección contra el mail-bombing? ¿Que medidas se toman?
- ¿Suspenden la recepción de mail cuando el servidor está ocupado en un determinado porcentaje de su capacidad (80% por ejemplo)?
- ¿Qué procedimiento siguen en el caso de una infección con un virus?
- ¿Cada cuanto se hace un escaneo total de virus en los servidores? ¿Quién se encarga? ¿Se hace automáticamente cada vez que hay una actualización o periódicamente?
- ¿El escaneo de las maquinas se realiza por cuenta de cada usuario o lo realiza el encargado de sistemas? ¿No seria más seguro que el encargado lo haga a intervalos regulares de tiempo?
- ¿Qué prioridad tiene el SendMail?
- ¿El firewall tiene algo que ver con el análisis de los virus, o solo se encarga de los servicios de la red? ¿El antivirus y el firewall están relacionados de alguna forma, son compatibles entre sí? Ej. Firewall y antivirus de Norton se complementan para generar un nivel de seguridad superior.
- ¿Cómo se realiza el download de los mails desde el servidor hasta las PC's? ¿Cada PC se identifica según el usuario que se logea? ¿O es según el número de terminal de la PC en la red? ¿Se puede configurar una cuenta (Ej.: la de algún Gerente) en otra máquina (que no sea la del Gerente) y bajar los mails desde ahí?

3.3.3 *Actualización de antivirus*

- ¿Cómo se actualizan las definiciones de virus? ¿Quién las baja de Internet? ¿Quién ejecuta las actualizaciones en la PC's? ¿Cómo se enteran de las nuevas actualizaciones de virus?
- ¿Cuánto tiempo lleva diseminar y actualizar el antivirus en toda la organización?
- ¿Se hacen chequeos ocasionales para ver si se han actualizado los antivirus?

3.4 DOCUMENTACIÓN – NORMAS

- ¿Qué documentación existe de la red?
 - ¿Diagramas topológicos?
 - ¿Procedimientos?
 - ¿Manuales?
 - ¿Certificados (Ej.: de calidad, etc.)?
 - ¿Licencias de software?
 - ¿Planes de contingencia, de seguridad, etc.?
 - ¿Contratos (Ej.: responsabilidades y mecanismos de transmisión al establecer una comunicación con las fábricas)
 - ¿Cambios realizados en la configuración de la red?
 - ¿Qué mas?
- ¿Poseen cada uno de estos elementos de documentación de la empresa?:
 - Manual de uso del software y de hardware usado (del software desarrollado y del comprado).
 - Diagramas de red y documentación de la configuración de routers, switches y dispositivos de red.
 - Procedimientos de emergencia (plan de contingencia)
 - Plan de seguridad
 - Manual de procesos estándares del Sistema Operativo (en especial de Linux)
 - Métodos para compartir datos entre sistemas (por ejemplo con las fábricas, entre las sucursales o entre las PC's de la red)
- ¿Se han instalado correctamente todos los parches de seguridad disponibles del sistema operativo y de los programas usados? ¿Cómo se conoce de los parches? ¿Están suscriptos a un mailing list?
- ¿Hay alguna documentación donde se anote la configuración de las PC's en la red? ¿Sus números IP, sus placas de red, etc.?

3.5 ATAQUES DE RED

- ¿Han tenido algún ataque en la red?
- ¿Que se ha hecho para arreglarlo?
- De los siguientes métodos contra los ataques más comunes, ¿qué está implementado?
 - Denial of service:
 - ¿Hay herramientas Anti DoS?
 - ¿Limitan el tráfico de red?
 - ¿Generan una “baseline” o líneas de base con la actividad normal del sistema?
 - ¿Se hizo alguna simulación ocupando una gran cantidad de recursos de algún tipo?
 - ¿Instalan los parches de seguridad del sistema operativo?
 - ¿Implementan un sistema de cuotas (Disk Quotas)?
 - ¿Utilizan alguna herramienta para detectar cambios en la información de configuración u otros archivos (como Tripwire)?
 - Sniffing:
 - ¿Las líneas de comunicación se segmentan tanto como sea práctico?

- ¿Los datos de logeo y otros datos sensibles son transmitidos encriptados?
- ¿Las cuentas privilegiadas (como root) se logean usando passwords one time o shadow passwords, y autenticación fuerte?
- Spoofing:
 - ¿Tienen alguna herramienta anti-spoofing?
 - ¿Los routers son configurados para que rechacen los ataques de spoofing?
 - ¿Solo los hosts apropiados son definidos como confiables en el Linux (como el /etc/hosts.equiv)? ¿Y este archivo tiene los permisos restringidos?
 - Por más que el acceso externo esté prohibido, ¿se configura el control de acceso para denegar cualquier tráfico de la red externa que tiene una dirección fuente que debería estar en el interior de la red interna?
- Ataque a las passwords:
 - ¿Donde se guardan las password del sistema operativo? ¿En el archivo /etc/passwd y /etc/group?
 - ¿Se chequean regularmente las passwords para comprobar su consistencia los archivos que nombré arriba?

3.6 FIREWALL

- ¿Qué firewall usan?
- ¿En que máquina (servidor) se encuentra el Firewall? ¿En una máquina dedicada? ¿En el servidor de Internet?

3.6.1 Tipos de firewall

- ¿Qué tipo de firewall hay?
 - ¿Gateway de filtrado de paquetes (Packet Filtering Gateways)?
 - ¿Gateway de aplicación?
 - ¿Gateways híbridos o complejos?
 - ¿Otro?

3.6.2 Política de configuración

- ¿En base a que criterios definieron las configuraciones del firewall?
- ¿Tienen una política definida en cuanto a la configuración del firewall?
- ¿Usan una política de acceso a servicios?
- ¿Usan una política de dial-in y dial-out?
- ¿Usan una política de diseño y configuración del firewall? ¿Alguna de estas dos?:
 - Postura de negación preestablecida: se especifica sólo lo que está permitido y se prohíbe todo lo demás:
 - ¿Se examinan los servicios que los usuarios necesitan?
 - ¿Se considera como afectarían la seguridad tales servicios y como se los puede proporcionar a los usuarios de manera segura?
 - ¿Se permiten sólo los servicios que se comprenden o se tiene experiencia, que se pueden proporcionar con seguridad y para los cuales existe una necesidad legítima?

- Postura de permiso preestablecido: se especifica sólo lo que está prohibido y se permite todo lo demás.

3.6.3 Características del firewall

- ¿Qué controles de acceso tiene el firewall? ¿Que servicios tiene habilitados y cuáles deshabilitados?
- ¿Soporta autenticación? ¿Con qué técnica? ¿Incluye las direcciones NAT (Network address translation) en la autenticación? ¿Y passwords?
- ¿Que habilidades tiene para monitorizar la red? Incluye:
 - ¿Intentos no autorizados de ingreso?
 - ¿Genera logs?
 - ¿Provee reportes? ¿O mails?
 - ¿Tiene alarmas?
- ¿Es lo suficientemente rápido para que no demore a los usuarios en sus intentos por acceder a la red (cómo es su performance)?
- ¿Qué tan configurables son sus opciones?
- ¿Puede adaptarse a distintas configuraciones de red o de sistemas (es escalable)?
- ¿Es fácil de configurar?
- ¿Es fácil de usar?
- ¿Es fácil de mantener?
- ¿Tiene un buen servicio postventa?
- Si se cae el firewall, ¿que pasa? ¿Es una “falla segura”?
- ¿Se hizo alguna prueba de la configuración del firewall? ¿Trató de hacerse un intento de entrada sin autorización, por ejemplo?

3.7 CONFIGURACIÓN DE SERVICIOS Y PROTOCOLOS DE RED

- De todos estos servicios:
 - ¿Cuáles se usan en la red?
 - ¿Cómo están configurados?
 - ¿Están habilitados o prohibidos?
 - ¿Existen excepciones?
 - ¿Poseen acceso de entrada y/o salida?
 - ¿Que pasa con los otros puertos que quedan libres?
- ¿Se desactivan completamente los siguientes servicios o protocolos?
 - SUID (set user ID), RLOGIN, RSH, REXEC (Comandos “r” Remote), SU (SuperUser), NetStar, GOPHER, TFTP (Trivial File Transfer Protocol), Telnet, SYSTAT, FINGER, TALK, EXPN, VFRY.
- ¿Cómo se configuran los siguientes servicios o protocolos?
 - POP (Post Office Protocol), MIME, HTTP, SMTP, FTP, Applets, Pruebas Cgi, Scripts Query, SHELL, NIS.

3.8 HERRAMIENTAS PARA ADMINISTRACIÓN DE RED Y PROTOCOLOS

- ¿Usan alguna de estas herramientas o protocolos para la seguridad de la red?
 - Tcp-wrappers, Netlogv, Satan, AntiSniff, Cops, SafeSuite, Gabriel, Courtney, Tcplist, SSL (secure socket layer), SHTTP, SMIME, NOCOL (Network Operations Center On-Line).
- ¿Las herramientas que se usan tienen las siguientes funciones?

- ¿Pueden monitorear y filtrar peticiones entrantes a distintos servicios?
¿Cómo lo hacen? ¿Con qué aplicación?
- ¿Indican la hora, la máquina origen (el número de IP) y el puerto de esa conexión?
- ¿Pueden seguir una traza de todos los intentos de conexión tanto admitidos como rechazados?
- ¿Se monitorea la red buscando ciertos protocolos con actividad inusual? Se controlan los siguientes:
 - Conexiones tftp,
 - Accesos vía rsh (remote shell),
 - Comandos en el puerto de sendmail como vrfy, expn, etc.
 - Algunos comandos de rpc (remote procedure call) como el rpcinfo,
 - Peticiones al servidor de NIS,
 - Peticiones al demonio de mountd.
- ¿Se llevan estadísticas de uso de los protocolos?
- ¿Se puede utilizar para detectar cambios en los patrones de uso de la red, y todo aquello que nos puedan hacer sospechar que algo raro está pasando en la misma?
- ¿Se audita el tráfico IP?
- En la captura de paquetes IP, ¿se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc.?
- ¿Tienen la posibilidad de filtrar paquetes Por hardware o por software?
- ¿Van creando una base de datos de todas las máquinas chequeadas y las va relacionando entre ellas (Satan es una herramienta que hace esto)?
- ¿Qué otra funcionalidad no nombramos que si tiene la herramienta usada?
¿Que función sería muy útil al trabajar en la red?
- ¿Se mantiene actualizado el software? ¿Se investiga para mantener actualizadas las herramientas? ¿Alguien está a cargo de esta actividad?
- ¿Se buscan herramientas nuevas que faciliten la tarea? ¿Consultan a algún Organismo (como el CERT)?

4- SEGURIDAD DE LAS APLICACIONES

4.1 ELECCIÓN DEL SISTEMA A USAR

¿Se hicieron los siguientes cuestionarios al elegir los sistemas operativos y programas usados en la empresa? ¿Qué respuestas tenían?

- Para todo tipo de sistemas se debe tener en cuenta los siguientes requisitos:
 - Requerimientos funcionales: ¿qué funciones debe cumplir el sistema?
 - Entorno necesario: ¿Windows, Unix o Linux?
 - Requerimientos de compatibilidad: ¿se ajusta a estándares o a regulaciones internacionales, o a programas existentes en la empresa?
 - Requerimientos de performance: respuestas por segundo, errores, etc.
 - Requerimientos de interoperatividad: ¿cómo se relaciona con los demás sistemas?
 - Fiabilidad: errores tolerables del sistema
 - Amigable: fácil de usar.
 - Precio y precio adicional de mantenimiento
 - Documentación y manuales propios del software
- Además hay que tener en cuenta los siguientes requisitos de seguridad
 - Identificación y autenticación,
 - Control de acceso,
 - Login,
 - Evaluación de protocolos,
 - Incorruptibilidad,
 - Fiabilidad,
 - Seguridad en la transmisión,
 - Back up de datos,
 - Encriptación,
 - Funciones para preservar la integridad de datos,
 - Requerimientos sobre privacidad de datos.

4.2 CONTROL DE DATOS DE APLICACIONES

- ¿Existe un control de cambios para los archivos del sistema o para las bases de datos de la empresa, como por ejemplo una base de datos, que se modifique cada vez que alguien haga una modificación sobre un archivo?
- ¿Existen restricciones de datos de salida, por ejemplo al portapapeles o a la impresora, y otros?
- ¿Cómo es el acceso a las librerías de programa (o a la carpeta “Archivos de programa”)?
- ¿Cómo se asegura la confidencialidad de los datos en una laptop? ¿Qué datos hay en las laptops de la empresa, o de los usuarios?
- ¿Se generan logs en cada transacción de manera de poder hacer un “undo”? ¿Estos registran los cambios en los datos críticos del sistema?
- ¿Se generan históricos de auditoria indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios – gestión de configuración)?
- ¿Los archivos de programa y los de trabajo se almacenen en directorios separados?

4.3 CONTROL DE DATOS EN EL DESARROLLO

- ¿Se asegura la integridad, exactitud y validez de los datos de entrada y salida de las aplicaciones?
- ¿Las variables, parámetros y / o fórmulas de cálculo se incluyen en tablas o archivos separados de los programas, para facilitar su modificación?
- ¿Existe un proceso de control de cambios para el desarrollo? ¿Cómo se documentan estos cambios?
- ¿Controlan el contenido de los archivos de entrada? ¿Controlan que existan los archivos antes de ejecutar el programa?
- ¿Se hacen controles sobre la validez de los datos ingresados manualmente? (Controles de integridad de datos)
- ¿Se controla la consistencia de los datos de salida de las aplicaciones?
- ¿Las aplicaciones se operan a través de menús obligatorios o es a través de comandos del sistema? ¿Los operadores de estas aplicaciones pueden editar los datos reales del mismo (o sea las bases de datos)?

4.4 SEGURIDAD DE BASES DE DATOS

- ¿Los archivos de la base de datos tienen control de acceso? ¿O solo se hacen controles en las aplicaciones?
- ¿Se controlan las siguientes ocurrencias?
 - tiempo y duración de los usuarios en el sistema,
 - número de conexiones a bases de datos,
 - número de intentos fallidos de conexiones a bases de datos,
 - ocurrencias de deadlock con la base de datos,
 - estadísticas de entrada-salida para cada usuario,
 - generación de nuevos objetos de bases de datos,
 - modificación de datos.
- ¿Se hace algún chequeo regular de la seguridad de la base de datos? ¿Se documentan los chequeos incluyendo lo siguiente?
 - ¿Se hacen y son efectivos los backups y los mecanismos de seguridad?
 - ¿Hay algún usuario de la base de datos que no tenga asignado un password?
 - ¿Hay algún usuario que no ha usado la base de datos por un período largo de tiempo?
 - Además del administrador de datos, ¿quién tiene acceso a los archivos del software de base de datos, a los del sistema operativo y a las tablas del sistema (FAT)?
 - ¿Quién puede ejecutar un editor SQL?
 - ¿Quién tiene acceso de lectura – escritura a los archivos de programa?
 - ¿Qué usuarios tienen los mismos permisos que el administrador?
 - ¿La base de datos tiene suficientes recursos libres para trabajar?
- ¿Se borran físicamente los registros de las bases de datos cuando un usuario los elimina, o se marcan como “borrados”?

4.5 CONTROL DE APLICACIONES

- ¿Todas las máquinas de la empresa tienen los mismos programas con las mismas versiones? ¿Existe un estándar de configuración de PC's a seguir?

- ¿Usan alguna herramienta como el Norton Ghost para copiar la configuración de las PC's?
- ¿Existe un procedimiento para instalar las aplicaciones en las máquinas de los usuarios?
- ¿Quién los instala y administra?
- ¿Existen controles para realizar la instalación o la actualización de parches de las aplicaciones?
- ¿Cómo se documenta la instalación o actualización del software que se instala en las máquinas?
- ¿Existe algún procedimiento para encontrar programas que no deberían estar en las máquinas de los usuarios, ya sea por problemas de licencias o virus? ¿Existe un método a seguir? ¿Se usa algún producto para detectar estos programas? ¿Se hacen auditorías periódicas para verificar?
- ¿Cómo se controla a los usuarios y las aplicaciones que bajan de la web? ¿Cómo controlan que éstas tengan las licencias correspondientes (esto puede terminar en un problema para la empresa)? ¿Se borran las versiones de prueba (trial version) o demos cuando expiran?
- ¿Se permiten los registros on line de las aplicaciones?
- ¿Existen métodos para autorizar y registrar software?
- ¿Cómo manejan las actualizaciones del software?
- ¿Existe alguna forma de configurar las PC's de manera que no se pueda instalar software nuevo sin autorización del administrador?
- ¿Puede pasar que un usuario no este autorizado para modificar las carpetas c:\Windows o c:\Archivos de programa, pero otro (el administrador de sistemas) sí? ¿Cómo se configura esto en el sistema de control de acceso de la empresa? ¿Se usa?

4.6 MANTENIMIENTO DE APLICACIONES

- ¿Cómo se etiquetan y almacenan los instaladores de los programas o los drivers? ¿Se almacenan en disco duro, en disquete, en CD, en cinta?
- ¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte?
- ¿Se controla el funcionamiento correcto de las aplicaciones? ¿Se hacen chequeos periódicos sobre el funcionamiento, la configuración, etc.? ¿Se generan alertas?
- ¿Cómo se administran las emergencias?
- ¿Si se hacen cambios de emergencia, cómo se documenta?
- ¿Se borran los archivos de las carpetas temporales, para que no se llenen los discos de basuras y provoquen la caída del sistema?
- ¿Se revisan periódicamente los sistemas para eliminar los programas o servicios innecesarios (como algunos servicios web, FTP, http)? ¿Se buscan vulnerabilidades nuevas durante estas revisiones?
- ¿Es automático el método de actualización de los Antivirus para que los mensajes internos en el interior y el exterior de la organización no propaguen virus? ¿Se programan los escaneos automáticos de virus una vez por semana? ¿Por qué no la actualiza la aplicación automáticamente con un schedule?
- ¿Existe alguna aplicación de gestión para tomar decisiones de alto nivel gerencial? ¿Esta obtiene datos automáticamente de las bases de datos?

- ¿Existe un undelete como la Papelera de Reciclaje de Norton? ¿En el servidor o en las PC's?
- ¿Está habilitado el undelete de DOS?
- ¿Se hace un back up de la configuración de los sistemas antes de hacer algún cambio de manera de poder hacer un undo?
- ¿Los cambios complejos en los archivos de configuración se hacen primero (a modo de prueba) en una copia de los archivos o se hacen directamente en la configuración original?
- ¿Se registran o documentan los cambios hechos a una configuración?

4.7 CICLO DE VIDA

- ¿Qué aplicaciones se desarrollaron en la empresa? ¿Una para cada área de la empresa?
- ¿Qué metodología estándar usan para el desarrollo de sistemas? ¿De qué fases consta? ¿Qué mecanismos de seguridad manejan durante estas fases?

4.7.1 Iniciación

- ¿Cómo se expresan las necesidades del sistema?

4.7.2 Desarrollo

- ¿Se hace un análisis de riesgos antes de empezar con el desarrollo?
- ¿En caso de que haya participación de terceros en el desarrollo (como en la web, o en LINUX) el código fuente queda en la empresa? ¿Dejan documentación? ¿Tienen alguna reglamentación para trabajar con terceros?
- ¿Usan métricas durante el desarrollo? ¿Les sirven? ¿Qué miden? ¿En qué las utilizan?
- ¿Se mantienen registros históricos de las modificaciones llevadas a cabo en los sistemas durante el desarrollo y el mantenimiento? ¿Qué se guarda?
 - sistema que afecta,
 - fecha de la modificación,
 - persona que realizó el cambio,
 - descripción global de la modificación,
 - ¿Qué mas?
- ¿En qué momento se definen los requisitos de seguridad de un sistema? ¿Es durante el desarrollo?

4.7.3 Implementación

- ¿En qué lenguajes se implementan los sistemas? ¿Reusan software?
- ¿Qué medidas de seguridad toman durante la implementación?

4.7.4 Prueba

- ¿Cómo se hace la prueba de los sistemas?
- ¿Se generan planes de prueba?
- ¿Qué tipos de prueba se llevan a cabo? ¿De unidad? ¿De integración? ¿Por módulos? ¿Por sistema?
- ¿Se generan escenarios de prueba para el testeo?
- ¿Se documentan las pruebas y sus resultados? ¿Qué datos se guardan?

- ¿Cómo se realiza el control de cambios del sistema?

4.7.5 Instalación y mantenimiento

- ¿Qué metodología usan para el mantenimiento?

4.7.6 Documentación

- ¿Qué documentación generan de los desarrollos que hacen? ¿Se incluyen las siguientes cosas?
 - Generalidades del sistema, incluyendo fecha de implementación y analista / programador responsable.
 - Documentación del sistema, incluyendo sus objetivos, diagramas general y de funciones y diseños de registros.
 - Documentación de los programas, incluyendo objetivos, diagrama de flujo y archivos de entrada y salida que utiliza.
 - Manual de operación, que contenga el diagrama de flujo general de procesamiento donde se identifiquen los procesos que deben haber finalizado y las interfaces de entrada que se deben haber cubierto como paso previo a la ejecución de cada proceso, los procedimientos de supervisión, seguridad y control sobre los procesos y los pasos a seguir ante la ocurrencia de errores.
 - Manual de usuario.
 - Manual de características de seguridad.
 - Descripción del hardware y software, políticas, estándares, procedimientos, backup, plan de contingencia, descripción del usuario y del operador del sistema.

4.7.7 Compra

- ¿Qué medidas se toman antes de comprar un sistema?
- ¿Cómo es el análisis que se hace?
- ¿Existe documentación de los sistemas comprados, así como los vendedores y del soporte postventa?

5- SEGURIDAD FÍSICA

5.1 CONTROL DE ACCESO AL CENTRO DE CÓMPUTOS

- ¿Se hizo un análisis costo beneficio a la hora de implementar los controles?
¿Cómo se asesoraron?
- ¿Se restringe el acceso al centro de cómputos a la gente que no pertenece a esa área?
- ¿Existen algunos de los siguientes métodos? ¿Dónde?
 - tarjetas de entradas,
 - guardias de Seguridad,
 - llaves Cifradas (Looked Door),
 - circuito cerrado de televisión.
- ¿Cuál es la función de la doble puerta en la entrada?
- ¿Qué tipos de autenticación se utilizan en la empresa? Hay cuatro formas:
 - con algo que el individuo sabe (password, PIN, etc.),
 - algo que el individuo procesa (un token, una smart card, etc.),
 - algo que el individuo es (controles biométricos),
 - algo que sabe hacer (como los patrones de escritura).
- ¿Por qué no usan las otras? ¿Por el costo? ¿No vale la pena?
- ¿Solo dejan entrar a aquellos que lo necesiten? ¿Les hacen algún control de seguridad?

5.2 CONTROL DE ACCESO A EQUIPOS

¿Cómo se controlan los siguientes accesos?

- ¿La BIOS tiene habilitada una contraseña?
- ¿Las PC's tienen habilitados los dispositivos externos, como la disquetera o la lectora de CD? ¿Cómo se controlan estos dispositivos?
- ¿Cómo se controlan los virus en las disqueteras o CD's? ¿Qué otros peligros pueden tener?
- ¿Son dispositivos booteables (se permite desde el setup de la máquina el booteo con estos dispositivos)?
- ¿Ha habido robo de datos usando estos dispositivos?
- ¿Existen copadoras de CD's en la empresa? ¿Quién tiene acceso a ellas? ¿En qué máquinas están?
- ¿Usan llave de bloqueo en las CPU's?
- ¿Las CPU's y dispositivos externos extraíbles están guardados con llave?
- ¿Existe algún control sobre los terceros que realizan el mantenimiento?
- ¿Existen entradas no autorizadas en las PC's, como puertos no usados y no deshabilitados?
- ¿Puede alguien enchufar e instalar una impresora u otro dispositivo (un zip o un disco removible) en alguna máquina?
- ¿Cómo se realiza el control sobre los dispositivos que se instalan en las PC's?
¿Se hace una revisión periódica de los mismos? ¿Quién las hace? ¿Cada cuanto? ¿Qué buscan?
- ¿Se apagan los servidores en algún momento? ¿Es necesario que queden prendidos las 24 hs.?

5.3 UTILIDADES DE SOPORTE

¿Existen, se mantienen y revisan todos estos aparatos periódicamente en busca de fallas?

- Aire acondicionado (18° C a 20° C)
- Calefacción
- Humidificador en la biblioteca de cintas y centro de cómputos
- Luz de emergencia en el centro de cómputos
- Detectores de humo, agua y calor
- Instalación de alarmas:
 - contra fuego,
 - humo,
 - calor,
 - intrusos,
 - agua,
 - ¿Qué otras hay?
- Servidor de repuesto o redundante
- UPS (Uninterruptible power supply) ¿para mantener los servidores de red funcionando por cuántas horas? ¿Cuántos UPS? ¿En qué máquinas?
- Estabilizador de tensión: ¿cuántos? ¿En qué máquinas?
- Extinguidores de incendio:
 - ¿Son los adecuados?
 - ¿Son manuales o automáticos (rociadores)?
 - ¿Se corta la energía eléctrica cuando se activan estos rociadores?
 - ¿Están en el lugar correcto? ¿En qué lugares? ¿Cómo eligieron el lugar?
 - ¿Se revisan las posibles fallas eléctricas o posibles causas de incendio?
 - ¿Qué pasa con las máquinas cuando cae la lluvia artificial? ¿Existen cubiertas plásticas para protección de agua?
 - ¿Qué pasa con los extinguidores de incendio en el centro de cómputos?
- ¿Hay una sola red eléctrica?
- ¿Hay un dispositivo que evite la sobrecarga de la red eléctrica?
- ¿Hay hardware especial de aislamiento y protección de dispositivos magnéticos?

5.4 ESTRUCTURA DEL EDIFICIO

- ¿Se tuvo en cuenta la seguridad de los datos y equipos en el momento de hacer la estructura de los edificios? ¿O se hizo primero la red y luego el edificio?
- Centro de cómputos:
 - ¿Está ubicado en pisos elevados (para prevenir inundaciones)?
 - ¿Existe un piso o techo falso para pasar el cableado por debajo de él? ¿El área debajo del piso o del techo falso es fácilmente accesible?
 - ¿Es lo suficientemente grande, anticipándose al crecimiento de la red y predispuesto a reinstalaciones?
 - ¿La localización del centro de cómputos, tiene paredes externas o ventanas?
 - ¿Está cerca del (backbone) caño central de la red?
 - ¿Esta permitido comer, fumar y beber dentro del centro de cómputos?

- ¿En el resto de los escritorios se puede?
- Cableado:
 - ¿Usan cableado estructurado? ¿Quién lo instaló? ¿Terceizaron la instalación?
 - ¿Usaron alguna norma para hacer el cableado?
 - ¿Se tuvo en cuenta el lugar de los canales de red, de manera que no sean afectados por desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos?
 - ¿Que tipo de cable usan para que no haya interferencias?
 - ¿Qué medidas toman para las interferencias?
 - ¿Cómo previenen los daños o cortes en los cables?
 - ¿Cómo calcularon el ancho de banda de la red? ¿Es suficiente?
 - ¿Bocas de red: son suficientes? ¿Hay de más? ¿Cómo protegen a las que sobran? ¿Están habilitadas o no? ¿Cómo las deshabilitan?
- ¿Se conoce por donde van las cañerías de manera que no interfieran con la red?
- ¿El local se sitúa encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas?
- ¿Esto causa molestias o interferencias?
- ¿Existe un interruptor de energía de emergencia en la puerta de salida?
- ¿Los muebles son de madera? ¿Son inflamables?

5.5 INTERCEPTACIÓN FÍSICA, VISUAL Y ELECTROMAGNÉTICA

- ¿Puede haber emisiones electromagnéticas desde los monitores o desde los cables UTP, que se pueden interceptar o provocar ruidos?
- Emisiones visuales: ¿se evita que los monitores puedan verse a través de las ventanas?
- Emisiones de sonido (ruido): ¿se toma alguna medida para que no afecten el funcionamiento normal? ¿Hay ruidos que puedan causar problemas? ¿La ubicación de las antenas de radio interfiere con los datos de alguna manera? ¿No son necesarias las cortinas de aluminio para aislar de ruido a las señales? ¿Usan algún otro tipo de aislamiento en algún lado?

5.6 SISTEMAS MÓVILES

- ¿Si se usan laptops o PC's portátiles, se tienen en cuenta los diferentes riesgos a los que se someten los datos de la empresa?
- ¿Los dueños de las laptops son conscientes de la inseguridad que generan al tener datos sensibles en ellas? ¿Tienen en cuenta estos puntos?
 - ¿Se encriptan los datos en un sistema móvil?
 - ¿Se almacenan en lugares seguros los equipos móviles?
 - ¿Las laptop tienen password de acceso?
 - ¿Cómo se maneja el trabajo desde la casa?
 - ¿Se hacen backups de los datos de los sistemas móviles? ¿Cómo y en qué medio?

5.7 EMERGENCIAS

¿Cómo se procede en caso de una emergencia?

- Error físico de disco de un servidor,
- Error de memoria RAM,
- Error de tarjetas controladoras de disco,
- Incendio total o factores catastróficos,
- Durante y después de la situación de emergencia, ¿se controla el acceso al centro de cómputos?

5.8 CLASIFICACIÓN DE DATOS Y HARDWARE

- ¿Existen procesos para rotular, manipular y dar de baja la computadora, sus periféricos y medios de almacenamiento removibles y no removibles? ¿Cómo son estos procesos? ¿Con qué se rotulan los dispositivos?
- ¿Tienen un inventario de recursos de hardware y software? ¿Existe documentación sobre los dispositivos instalados en cada máquina, su configuración, modificación, forma de mantenimiento, versión, etc.?
 - ¿Cómo se guarda? ¿Es una planilla?
 - ¿Dónde se almacena?
 - ¿Quién lo actualiza?
 - ¿Cada cuanto?

5.9 BACKUP

- ¿Con qué frecuencia hacen los backups?
- ¿Qué datos se almacenan? (datos y programas de aplicación y de sistemas, equipamiento, requerimientos de comunicaciones, documentación)
 - Software de base y su configuración:
 - ¿Se hacen discos de inicio de Windows?
 - ¿Hay imágenes Ghost de las máquinas?
 - ¿Se hacen backups de la configuración de red?
 - Software aplicativo,
 - Parámetros de sistema,
 - Logs e informes de auditorías,
 - Datos,
 - ¿Qué más?
 - Backups del Hardware.
 - Modalidad externa: ¿contratan un tercero que proporcione los insumos necesarios en caso de emergencia?
 - Modalidad interna: si tienen más de un local, en ambos locales deben tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local. ¿Se realizan estas actividades en la empresa?
 - Radio: ¿si se cae un nodo de la radio, que pasa? ¿Hay algún servicio técnico o de respaldo para esto?
- ¿Hay backup especiales (con datos distintos, o particulares)? ¿Cada qué período de tiempo se hacen? ¿Que datos guardan?
- ¿Qué tipo de back up hacen? (backups normales, backups incrementales, backups diferenciales) ¿En qué áreas o datos usan incrementales, en cuáles usan normales, etc.?
- ¿En qué medio se almacena? ¿Con qué dispositivo se hace?
- ¿Cómo es la rotación de los medios de backup? ¿En una semana, un mes?

- ¿Con qué aplicación se hacen? ¿Con algún tipo especial de aplicación de manejo de backup? ¿Es una del sistema operativo, del administrador de archivos u otra? ¿Utilizan archivos de tipo específicos o archivos .zip, por ejemplo?
- ¿Hay herramientas de back up automáticas, o sea que a través de una agenda hacen las copias?
- ¿Quién es el encargado o el responsable? ¿Los hace el administrador de sistemas?
- ¿Tienen formalizados los procedimientos de back up? ¿Existe un procedimiento escrito? ¿Si falta el responsable del backup, quién los hace?
- ¿Existen procedimientos escritos para recuperar archivos backupeados, o un Plan de backup?
- ¿Hacen pruebas periódicas de recuperación de backups?
- ¿Quién puede levantar los archivos de los usuarios, los backups de Mis Documentos, cualquier otro usuario?
- ¿Qué PC's o máquina es la que tiene mayor prioridad? ¿Cómo son las prioridades? ¿Según qué se determinó la prioridad de las máquinas: según un análisis de impacto, según la confidencialidad de la información?
- ¿Los backups se almacenan dentro y fuera del edificio? ¿Estos lugares son seguros?
- ¿Cómo se rotulan e identifican?
- ¿Hay documentación escrita sobre los backups hechos, sus modificaciones, fechas, etc.?
- ¿Se necesita algún dispositivo (llaves, tarjeta) para entrar al almacén de cintas?
- ¿Se crean discos de inicio de Windows?
- ¿Hay información afuera de la red interna de la empresa que sea valiosa? ¿El web host tiene datos importantes de usuarios? ¿Se hacen backups de estos datos? ¿Dentro de la empresa o por el web host?
- ¿Hay backups de las páginas web y de sus actualizaciones?
- ¿Existen procedimientos automáticos para que, en caso que un usuario cometa un error en la base de datos, ésta pueda volverse a su estado anterior? ¿Cómo se hace?

6- ADMINISTRACIÓN DEL CENTRO DE CÓMPUTOS

6.1 COUNTERMEASURES DEL CPD

- ¿Se realizan los siguientes chequeos en el sistema?
 - Diariamente:
 - ¿Extraen un logístico sobre el volumen de correo transportado?
 - ¿Extraen un logístico sobre las conexiones de red levantadas?
 - Semanalmente
 - ¿Extraen un logístico sobre los intentos de ingresos desde el exterior a la red interna?
 - ¿Extraen un logístico con las conexiones externas realizadas desde nuestra red?
 - ¿Obtienen un logístico sobre los downloads de archivos realizados y quién los realizó?
 - ¿Obtienen gráficos sobre tráfico en la red?
 - ¿Obtienen logísticos sobre conexiones realizadas en horarios no normales (desde dónde, a qué hora y con qué destino)?
 - Mensualmente
 - ¿Realizan un seguimiento de todos los archivos logísticos a fin de detectar cambios en las estadísticas obtenidas (realizados en comparación con los archivos del mes anterior, por ejemplo)?
 - ¿Existe un programa que haga estas comparaciones? ¿Se usa? ¿Da buenos resultados?
- ¿Existen procedimientos para dar publicidad a las nuevas normas de seguridad?
 - ¿Cómo harían el aviso de las políticas de seguridad?
 - ¿A través del mailing?
 - ¿Con charlas o reuniones?
 - ¿Exposición en transparencias?
 - ¿Por una notificación expresa a cada empleado?
- ¿Cómo funciona el boletín mensual que les entregan a los usuarios? ¿Qué temas trata?
- ¿Se entrena a los usuarios y administradores? ¿Quién es el encargado? ¿Por qué?
- ¿Se tienen en cuenta los delitos no tecnológicos? (Ej: discutir temas privados de la organización en lugares no aptos, ingeniería social, etc.)
- ¿Existe algún tipo de mesa de reportes donde los usuarios con incidentes de seguridad pueden recibir ayuda o realizar un reporte? ¿Existe un tipo de feedback o buzón de sugerencia de cambios de los usuarios?
- ¿Existe un Plan de Sistemas formal? (plan a corto plazo de actividades del CC)
 - ¿Quién los hace?
 - ¿En base a qué estudios definen las cosas por hacer?
- ¿Existe un Plan Estratégico de Sistemas? (plan a largo plazo de proyectos)
- ¿Existen políticas, normas, estándares y procedimientos que sirvan como base para la planificación, el control y la evaluación de las actividades del área de sistemas de información?

- ¿Existe una planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información? Deberá incluir como mínimo el detalle de:
 - los procesos a realizar,
 - los controles que se efectúan,
 - los mecanismos de registros de problemas y hechos,
 - los procedimientos sobre cancelaciones y re-procesos en cada una de las actividades,
 - las relaciones con otras áreas,
 - los mecanismos de distribución de la información.
- ¿Existe documentación detallada sobre el equipamiento informático?
¿Incluye los siguientes datos?
 - distribución física de las instalaciones (identificación de PC's y equipos, y puesto de trabajo),
 - inventario de "hardware" y "software" de base,
 - número de serie de hardware,
 - número de licencia de software,
 - inventario de insumos,
 - diagramas topológicos de las redes,
 - tipos de vínculos,
 - ubicación de nodos,
 - trabajos de mantenimiento y entrada del personal externo.
- ¿Se tienen en cuenta tanto al centro de procesamiento de datos principal como de los secundarios, redes departamentales, sucursales y al centro alternativo para contingencias?
- ¿Se actualiza la lista de activos?
- ¿Existe algún manual de seguridad, para el personal de seguridad o para los usuarios? Existe alguno de los siguientes documentos:
 - Plan de contingencia,
 - Plan de continuidad,
 - Plan de seguridad,
 - Manual de procedimientos del CPD,
 - Trusted Facility Manual: detalla las funciones y privilegios de la seguridad. Contiene: configuración, administración y operación del sistema, guías para el buen uso de las características de protección del sistema, etc.
 - Security Features User's guide: asiste a los usuarios del sistema, describe como usar las protecciones, las responsabilidades de la seguridad del sistema.
- ¿Es automático el método de actualización de los antivirus para que los mensajes internos en el interior y el exterior de la organización no propaguen virus? ¿Se programan los escaneos automáticos de virus? ¿Cada cuanto tiempo? ¿Porque no se actualiza la aplicación automáticamente con un schedule?
- ¿Cómo se etiquetan y almacenan los instaladores de los programas o los drivers? ¿Se almacenan en disco duro, en disquete, en CD, en cinta?
- ¿Se borran los archivos de las carpetas temporales, para que no se llenen los discos de basuras y provoquen la caída del sistema?
- Todas estas tareas ¿Son realmente útiles? ¿Se dan en la práctica?

6.2 RESPONSABILIDAD DEL EQUIPO DE SEGURIDAD

- ¿Cómo se administran las emergencias? ¿Si se hacen cambios de emergencia, cómo se documenta?
- ¿Quién es el encargado de la seguridad? ¿Y de una política de seguridad y su administración?
- ¿Quién se encarga de administrar la estructura de seguridad una vez implementada?
- ¿Existe un solo responsable del centro de cómputos?
- ¿Qué privilegios (o accesos) se le dan a las personas recién contratadas en el centro de cómputos?
- ¿Cuál es la diferencia de permisos entre los desarrolladores y los administradores?
- ¿Quién asigna los permisos a los distintos roles o grupos?
- ¿Quién es el encargado de informar a los ejecutivos de la empresa sobre la administración de seguridad, actividad de seguridad de la información, y riesgos? ¿Se realizan informes periódicos? ¿Son a pedido de alguien o a modo de auto evaluación?
- ¿Quién es el encargado de recomendar la separación de tareas y responsabilidades para las funciones de IT?
- ¿Quién es responsable de asegurar que los sistemas de seguridad física están en su lugar?
- ¿Existe en los empleados y altos ejecutivos una conciencia sobre su importancia de la seguridad?
- Todas estas tareas ¿Son realmente útiles? ¿Se dan en la práctica?

7- AUDITORÍAS Y REVISIONES

7.1 AUDITORÍAS GENERALES

- ¿Se hacen auditorías en la empresa?
- ¿Qué objetos se auditan? Para cada clase de objetos, ¿qué accesos se auditarán?
 - Archivos y directorios
 - Claves del registro
 - Servicios
 - Objetos del kernel
 - Impresoras
- ¿Qué actividades se monitorizan?
 - Monitorización del sistema general
 - Monitorización de reinicio de los sistemas
 - Monitorización de colapsos (crashes) del sistema
 - Monitorización de fallas de hardware
 - Monitorización de procesos
 - Monitorización de aplicaciones
- Gestión de red: ¿Para el monitoreo de la red se utilizan aplicaciones propias de Linux, como:
 - monitores de tráfico de red?
 - monitores de rendimiento?
 - monitores de control de cantidad de archivos abiertos?
 - monitores de usuarios conectados al servidor?
 - aplicación de monitoreo gráfico de la red?
- ¿Qué otra clase de eventos se auditarán?
- ¿Con qué tipo de herramientas se hace la monitorización?
 - Escáner de puertos y vulnerabilidades
 - Chequeadores del sistema de archivos
 - Analizadores de logs de eventos
 - Analizadores de registro
 - Analizadores de listas de control de acceso (ACL)
 - Sniffers de paquetes
 - Herramientas para craquear passwords
 - Escáner de seguridad integral (Overall security scanners)
- ¿Se hacen chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad? ¿Sería útil?
- ¿Cuánto se monitoriza? (Monitorizar tiene un impacto directo en la performance del sistema) ¿Cómo hacen para que los recursos alcancen? ¿Cómo hacen con cada uno de los cuellos de botella?
 - Carga de CPU
 - Memoria disponible
 - Performance del sistema de disco
 - Ancho de banda de la red
- ¿Cuándo se eliminan los logs para evitar llenar el disco? ¿Tienen un tamaño máximo?
- ¿Qué pasa con la información que se obtiene de las auditorías? ¿Pasa algo de lo siguiente?

- Se solicita la información y se ve que:
 - No tiene y se necesita.
 - No se tiene y no se necesita.
- Se tiene la información pero:
 - No se usa.
 - Es incompleta.
 - No esta actualizada.
 - No es la adecuada.
 - Se usa, está actualizada, es la adecuada y está completa.
- ¿Las auditorías permiten rastrear las acciones de cada usuario?
 - ¿Que se audita?
 - ¿Se audita según las acciones, las maquinas o los usuarios?
 - ¿Cada uno de estos activos en particular o depende de los sectores y/o máquinas y/o sensibilidad de la información?
- ¿Las auditorías soportan investigaciones luego de los hechos, con datos sobre cómo, cuando y por qué cesaron las operaciones normales?
- ¿Se reúne información de las auditorías para formar perfiles de los usuarios del sistema? ¿Observan, por ejemplo, patrones en los usuarios, como las terminales que utilizan, horas de acceso, y permisos que solicitan, para determinar qué acciones son inusuales y deben ser investigadas?
- ¿Se usan herramientas automáticas para revisar los registros de auditorías en tiempo real?
- ¿Debido a que no hay herramientas que generen warnings ni alarmas, se revisan los logs de auditorías periódicamente? ¿Qué se revisa?
- ¿La aplicación es en tiempo real?
- ¿La aplicación es del sistema operativo, es un programa desarrollado por ustedes o es un programa comprado?
- Se deberían utilizar chequeos aleatorios, con frecuencias más bajas, para hacer auditorias manuales y/o mensuales de este tipo.
- ¿Se generan históricos de auditoria indicando qué procesos se corrigieron, quién los corrigió y qué cambios hizo (control de cambios – gestión de configuración)?
- ¿Se investiga la actividad sospechosa? ¿Se toman acciones?
- ¿Se documentan la ejecución y los resultados de estas pruebas?

7.2 LOGS:

- ¿Está controlado el acceso a los logs on line de auditoria?
- ¿Cómo se identifica qué tipo de logs son generados? ¿Se almacenan en diferentes carpetas los que son generados por diferentes programas?
- ¿Los logs se almacenan externamente a la empresa? ¿Los almacenamientos externos de logs de auditorías se retienen por un período de tiempo? ¿Está controlado el acceso a estos logs, también?
- ¿Hay demasiada información guardada? ¿Los archivos largos de logs hacen más difícil encontrar irregularidades?
- Los logs de los eventos deberían contener los siguientes campos:
 - Fecha y hora
 - Tipo (severidad del evento)
 - Fuente (el componente que disparó o logeo el evento)
 - Categoría (subgrupo de eventos de seguridad)

- ID del evento (número único que identifica el evento)
- Usuario (nombre del usuario relacionado con el evento, si hay)
- Computadora (máquina donde se logeo el evento)
- Descripción (datos como mensajes de error, asociados con el evento)
- Datos (datos binarios asociados con el evento)
- Análisis de los logs de auditoría:
 - ¿Qué datos son los más importantes o los más leídos?
 - ¿Cuánto tiempo lleva hacer los análisis?
 - ¿Es necesario mejorar los análisis? ¿De que forma, cuál es la falla?
- ¿Porque no se analizan los logs, aunque sea los que posean alguna conducta irregular?
 - ¿Es totalmente necesario un sistema automático de monitorización y análisis de logs que emita alarmas ante determinados eventos?
 - ¿Porque esto no se da en la realidad?
 - ¿Es mucho trabajo?
 - ¿No vale la pena?
 - ¿No hay gente que se dedique a esto?

7.3 LÍNEA DE BASE

- ¿Se hace una línea de base de la performance de los servidores y de la red?
¿Qué medidas se toman?
- ¿Qué datos se recogen para hacer la línea?
- ¿A qué intervalo de tiempo se toman estos datos? ¿Con qué frecuencia se tomarán las líneas base?
- ¿Se hacen nuevamente las líneas de base si se modifica alguna configuración en el sistema?
- ¿Cuándo se actualizan las líneas de base?
- ¿Cómo se guardan? ¿Dónde? ¿En qué formato?

7.4 RESPONSABILIDADES DE LOS ENCARGADOS DE SEGURIDAD

- ¿Quién administra, desarrolla e implementa los procedimientos de auditoría y revisión? ¿Quién conduce la auditoría?
- ¿Quién selecciona los eventos de seguridad a ser auditados?
- ¿Quién administra la documentación sobre los resultados?
- ¿Quién se encarga de monitorizar y reaccionar a los avisos (warnings) y reportes?
- ¿Quién hace chequeos aleatorios para verificar el cumplimiento de los requerimientos y procedimientos de seguridad?
- ¿Quién se encarga de reunir datos de las auditorías para formar perfiles de los usuarios del sistema?
- ¿Quién revisa los reportes de auditorías buscando anomalías?
- ¿Hay separación de tareas entre los que administran el control de acceso y los que hacen las auditorías, o son las mismas personas?
- ¿Quién se encarga de buscar nuevas herramientas que faciliten la auditoría?

7.5 AUDITORÍAS DEL SERVIDOR

- CPU del servidor usado
 - ¿Qué trabajos usan más CPU?

- ¿Quién usa más CPU?
- ¿En qué momento se usa más el CPU?
- ¿Cuánto tiempo el CPU permanece usada en un 100%?
- Memoria del servidor usada
 - ¿Qué trabajos usan más memoria?
 - ¿Quién usa más memoria?
 - ¿En qué momento se usa más la memoria?
 - ¿Cuánto tiempo la memoria permanece usada en un 100%?
- Datos del servidor usados
 - ¿Qué datos son los que consumen más tráfico, memoria o CPU?
 - ¿Qué datos se usan más?
 - ¿Qué datos se modifican más?
 - ¿Quién entra a cada dato?
- Aplicaciones del servidor usadas
 - ¿Qué aplicaciones consumen más recursos?
 - ¿Qué aplicaciones se usan más?
 - ¿Qué aplicaciones se cuelgan más veces?

7.6 AUDITORÍAS DE CONTROL DE ACCESO

- ¿Se generan logs de auditoria del control de acceso?
- ¿Cuándo se almacenan, ante qué eventos? ¿Se almacenan cuando ocurre alguno de estos eventos?
 - Login exitoso
 - Login fallido
 - Procedimientos de cambios de passwords satisfactorio
 - Procedimientos de cambios de passwords fallido
 - Lockeo de un usuario
 - Modificación en bases de datos
 - Utilización de herramientas del sistema
 - Modificación de ciertos datos (como datos de configuración, datos críticos, datos de otros usuarios)
 - Acceso a Internet
 - Alertas de virus
- ¿Dónde se almacenan?
- ¿Quién tiene acceso a los logs?
- ¿Por cuanto tiempo permanecen guardados?
- ¿Se borran cuando expira ese tiempo o se genera una estadística comprimida de los mismos y de guarda un análisis de ellos solamente?
- ¿Qué datos se almacenan en los logs? ¿Se almacenan los siguientes datos?
 - Para todos los eventos:
 - Fecha y hora del evento
 - Tipo de evento (Ej. Login, modificación de datos, etc.)
 - ID de usuario
 - Origen del evento (Ej. Terminal N° 9)
 - Acceso a Internet:
 - Páginas visitadas
 - Cookies guardadas
 - Archivos descargados
 - Servicios utilizados

- Aplicaciones utilizadas
- Modificación de ciertos datos
 - Datos modificados
 - Valor anterior
 - ~ ¿por cuanto tiempo se guarda el valor anterior de los datos?
 - ~ ¿Se hace alguna comprobación antes de efectuar el cambio definitivo?
 - ~ ¿Que se hace si se modifica algún valor de la configuración del sistema?
- Login fallido
 - Motivo del fallo
- Procedimientos de cambios de passwords
 - Password anterior
 - Password nueva fallida
 - Aplicación usada
 - Motivo del fallo
- Lockeo de un usuario
 - Motivo del lockeo del usuario
 - Aplicación que realiza el lockeo.
- Modificación en bases de datos
 - Datos modificados
 - Valor anterior
 - Aplicación usada
- Utilización de herramientas del sistema
 - Herramienta usada
 - Rastreo de acciones del usuario con esa herramienta
 - Modificaciones realizadas.
- ¿Las estadísticas que genera son buenas? ¿Faltan datos por analizar que son importantes para la administración del control de acceso?
- Prestar especial atención con los logs que fueron generados con el ID de Administrador, ¿hay irregularidades en estos logs? ¿Se han controlado alguna vez?

7.7 AUDITORÍAS DE REDES

7.7.1 Correo:

- ¿La herramienta de administración de correo genera logs de auditoria?
- ¿Qué contienen?
- ¿Quién los administra?
- ¿Cada cuanto se leen?
- ¿Se generan avisos cuando:
 - Se está por llenar el espacio asignado para el correo?
 - Hay muchos mensajes de la misma dirección fuente?
 - Hay muchos mensajes para la misma dirección destino?
 - Hay muchos mensajes con el mismo encabezado, o cuerpo, o archivo adjunto?
 - Hay posibles virus?
 - Hay SPAM?
 - Se baja la performance del correo?

- Hay algún problema para enviar o recibir los mensajes?
- Hay muchos mensajes entrantes o salientes, más de lo normal?
- Cuándo más?

7.7.2 *Mantenimiento – Monitoreo – Auditorias*

- ¿Usan herramientas de monitorización de red?
- ¿Se hace algún chequeo periódico de la red y sus permisos?
- ¿Qué datos se pueden ver?
 - Datos
 - ¿Programas que se ejecutan en las PC's y servidores?
 - ¿Qué prioridades tienen los trabajos?
 - ¿Qué prioridades tienen los usuarios?
 - ¿Con qué reglas de trabajos se están corriendo?
 - ¿El estado de cada trabajo (en cola, ejecutándose, esperando una respuesta del operador, etc.)?
 - ¿Desde dónde se ejecuta el programa (usuario, ID, terminal)?
 - ¿Porcentaje de CPU y memoria (recursos) usado por programa? ¿Y por terminal? ¿Y por usuario?
 - ¿Colas de impresión de cada usuario? ¿De cada impresora? ¿De cada terminal?
 - ¿Trabajos programados por cada usuario? ¿Por cada terminal?
 - ¿Dispositivos conectados a la red? ¿El estado de los dispositivos?
 - ¿Dispositivos con problemas?
 - ¿Qué usuario está asignado (o usando) cada dispositivo? ¿Qué trabajo lo está ocupando?
 - ¿Se monitorean los puertos de la red? ¿Se puede ver si hay intentos de intrusión?
 - Alertas de virus
 - ~ Tipo y nombre del virus
 - ~ Archivo infectado (nombre, ubicación etc.)
 - ~ Antivirus usado
 - ~ Acciones llevadas a cabo
 - ~ Resultado de las acciones (satisfactorio o no)
 - Estadísticas de red:
 - ¿En qué parte de la línea el tráfico es más intenso?
 - ¿Quién de las terminales usa más tráfico de red?
 - ¿Gráfico del uso de la red por terminal?
 - ¿Se discrimina el tráfico ocupado por mail, datos, aplicaciones, mensajes, Internet, etc.?
 - ¿Cuántos intentos de intrusos hubo?
 - ¿Cuántos intentos de otros ataques?
 - Etc.
 - Internet
 - ~ ¿Páginas más visitadas por usuario?
 - ~ ¿Tiempo promedio de estadía en Internet?
 - ~ ¿Recursos usados por Internet?
 - Mail
 - ~ ¿Cantidad de datos que se mueven diariamente vía mail?
 - ~ ¿Mensualmente?
 - ~ ¿Anualmente?

- ~ ¿Cantidad de mail enviados y recibidos por usuario?
- ~ ¿Por departamento?
- ~ ¿En toda la empresa?
- ~ ¿Controles para saber si un usuario en particular excede el promedio de mail diarios?
- ~ ¿Mensajes infectados, salientes y entrantes?
- ~ ¿Se usan estadísticas para controlar el mail bombing?
- Virus
 - ~ ¿Cantidad de mails infectados en un determinado tiempo?
 - ~ ¿Direcciones fuentes qué más mails infectados envía?
 - ~ ¿Cantidad de archivos infectados por extensión? (Ej. Los archivos de Word se infectan más que los de Excel).
- Alarmas – Avisos
 - ~ ¿Se generan avisos ante virus?
 - ~ ¿Se generan avisos ante intrusos?
 - ~ ¿Se generan avisos ante poco espacio en disco de servidores o de PC's?
 - ~ ¿Se generan avisos ante poca disponibilidad de CPU o de memoria en los servidores?
 - ~ ¿Cuándo más?
- ¿Quién se encarga de procesar y/o monitorear los datos generados por la herramienta?
- ¿Cómo se actúa en consecuencia? ¿Existe algún procedimiento específico?
- ¿Qué datos parecen faltar al monitor de red que serían útiles para la administración de la red?

8- PLAN DE CONTINGENCIAS

8.1 PLAN DE CONTINGENCIAS

- ¿Existe un plan de contingencias? ¿Cómo es? ¿Es formal? ¿Quién lo desarrolló?
- ¿Ha habido alguna contingencia que justifique el desarrollo del plan?
- ¿Se desarrolló un previo análisis de riesgo antes de realizar el plan de contingencias?
- ¿El plan de contingencias se desarrolló solo en base al área de cómputos, o se tuvieron en cuenta otras áreas de la empresa? ¿Cuáles? ¿Por qué esas áreas?
- ¿El plan de contingencias incluye un Plan de recuperación de desastres?
- ¿El plan de contingencias incluye un Plan de reducción de riesgos?
- ¿Se definen las responsabilidades y funciones de las personas en el plan de contingencias?
- ¿Existe entrenamiento para los responsables del plan de contingencias? ¿Y para los usuarios?
- ¿Poseen las acciones defensivas en caso de violación interna o externa? (Ej. desconectar los servidores, cerrar los accesos, rastrear al intruso, etc.).
- ¿Hay algún tipo de mecanismo de reportes o historial, para el manejo de incidentes?
- ¿Documentan el plan de contingencias? ¿Contiene todos estos datos?:
 - Objetivo del plan.
 - Modo de ejecución.
 - Tiempo de duración.
 - Costes estimados.
 - Recursos necesarios.
 - Evento a partir del cual se pondrá en marcha el plan.
 - Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.
- ¿Existe alguna copia del plan de contingencia fuera de la empresa? ¿Está protegida en caja de seguridad? ¿Cada cuanto se actualiza?
- ¿Se hacen pruebas del plan? ¿Con qué frecuencia? ¿Anualmente?
- ¿Se mantiene actualizado de acuerdo a nuevos puestos y funciones, o amenazas?

8.2 CPD ALTERNATIVO

- ¿Se mantiene un centro de procesamiento alternativo? ¿Qué características tiene, en comparación con el CPD principal?
- ¿Es propio o contratan un tercero que facilite el CPD? En el segundo caso, ¿cómo es el contrato para este servicio?
- ¿Cómo se aseguran que este centro tenga las mismas condiciones de seguridad y calidad que las instalaciones del CPD principal?
- ¿Existe la posibilidad de poner el CDP alternativo en otra sucursal o en otro lado? ¿Por qué?
- ¿Si llega a haber un problema, en cuanto tiempo puede estar en óptimo funcionamiento este CPD alternativo?

8.3 PLAN DE RECUPERACIÓN DE DESASTRES

- ¿Cuánto cuesta un plan de recuperación de desastres? ¿Tiene relación con la información a recuperar? ¿O a cualquier costo se salva la información crítica?
- ¿En el caso de que haya un plan, cada miembro del equipo tiene una responsabilidad asignada? ¿O la responsabilidad es del Departamento de Sistemas?
- ¿Se dividen las acciones correctivas en equipos de trabajo? ¿Cómo forman esos equipos? ¿Dependen del desastre ocurrido?
- ¿Luego del desastre existe un equipo de evaluación para corregir y documentar los errores cometidos en tal circunstancia, para luego generar un plan de contingencia de mayor efectividad y eficiencia?

8.3.1 ANTES DEL DESASTRE

- Identificación de las funciones críticas.
 - ¿Cuáles serían los datos críticos a proteger en la organización, en el momento de un desastre? (Agregar lista de datos).
 - ¿Cuáles serían los elementos de hardware y de software críticos a proteger en la organización, en el momento de un desastre? (Agregar lista de elementos).
 - ¿Cómo se ordenarían según la importancia?
- Constitución del grupo de desarrollo del plan.
 - ¿Quién sería le responsable del plan de emergencias, de su implementación y puesta en práctica? ¿El Jefe de Sistemas?
 - En cada área que cubrirá el plan debe haber un líder del plan de contingencia. ¿Quién sugiere, el Jefe de cada área? ¿Alguien de más bajo rango? ¿Por qué?
- Sistemas de información:
 - ¿Existe un responsable de la información, en cada área de la empresa? ¿Conocen sus responsabilidades? ¿Los responsables que figuran en la documentación, son los que ejercen realmente el papel de responsables de la información? ¿Qué funciones tiene que cumplir?
 - ¿Están identificados todos los sistemas de información y sus características (como si fuera un inventario de los sistemas)?
 - ¿Qué datos se almacenan de los sistemas? Se sugiere almacenar:
 - Nombre
 - Lenguaje
 - Departamento de la empresa que genera la información (dueño del sistema)
 - Departamentos de la empresa que usan la información
 - Volumen de archivos con los que trabaja
 - Volumen de transacciones diarias, semanales y mensuales que maneja el sistema
 - Equipamiento necesario para un manejo óptimo del Sistema
 - La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
 - El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la

- Institución puede funcionar adecuadamente, sin disponer de la información del Sistema).
 - Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
 - Actividades a realizar para volver a contar con el Sistema de Información (actividades de restauración).
- ¿Se puede dar un orden de importancia a los sistemas de la lista de arriba?
- Equipos de cómputos:
 - ¿Se mantiene un inventario de los equipos de cómputos? Se debería incluir:
 - Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.
 - Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
 - Datos (principales archivos que contienen los equipos): durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, dueño designado de la información.
 - Configuración de los equipos (y sus archivos de configuración).
 - Ubicación de los equipos y de los datos.
 - Nivel de uso Institucional de los equipos.
 - Etc.
 - ¿Existen pólizas de seguros para los equipos en el caso de siniestros? ¿Cómo son estos seguros?
 - ¿Las PC's o equipos se categorizan según su importancia (señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.)?
 - ¿Existe una relación de las PC's requeridas como mínimo para cada Sistema permanente de la Institución? ¿Está actualizada siempre?
- Backup:
 - ¿Existen procedimientos para realizar back up?
 - ¿Están incluidos en el plan de contingencia?
- Definición de los niveles mínimos de servicio.
 - ¿Cuáles son las contingencias o problemas que pueden ocurrir? (agregar lista de las posibles contingencias)
 - ¿Cuáles serían los peores problemas a los que se puede ver sometida la empresa? ¿Cuáles serían las peores contingencias?
 - ¿Cuáles serían las más probables?
 - ¿Cuáles son las que ocurren más a menudo?
 - ¿Cuales son las que no ocurren nunca?
 - ¿Se pueden nombrar algunas funciones o servicios que funcionen como los niveles críticos de servicio para cada una de las contingencias nombradas arriba? ¿Qué opinión tiene el jefe de cada área en cuanto a los niveles críticos de su área? Un ejemplo puede ser: el que no se caiga el servidor de aplicaciones, o el router, o la conexión de radio.
 - ¿Qué recursos se necesitan para que funcione este servicio?

- ¿Cuales son las prioridades de procesamiento que tendrán estas funciones o servicios críticos en caso de una emergencia?
- Evaluación de la relación coste / beneficio de cada alternativa.
 - ¿Qué costo tendría cada uno de los niveles críticos de servicio que se determinaron arriba? Contar los costos de implementación, de mantenimiento, de entrenamiento de usuarios, y de restauración en caso de una emergencia.
- Entrenamiento:
 - ¿Entrenan al personal de alguna manera ante un siniestro?
 - ¿Simulan siniestros para entrenar al personal?

8.3.2 *DURANTE EL DESASTRE*

- ¿Poseen un plan de emergencia (consiste de las acciones a llevar a cabo durante el siniestro)?
- ¿Se tienen en cuenta los distintos escenarios posibles? Ej.: durante el día, la noche.
- ¿Se incluyen los siguientes puntos?:
 - ¿Vías de salida?
 - ¿Plan de evacuación del personal?
 - ¿Plan de puesta a buen recaudo de los activos?
 - ¿Ubicación y señalización de los elementos contra el siniestro?
- ¿Existen funciones (encargado de retirar los equipos, encargado de las cintas, etc.) y equipos con funciones claramente definidas a ejecutar durante el siniestro?

8.3.3 *DESPUÉS DEL DESASTRE*

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción

- Evaluación de Daños: ¿se realizan las siguientes actividades después de que ha ocurrido algún desastre?
 - ¿Evalúan la magnitud del daño que se ha producido?
 - ¿Que sistemas se están afectando?
 - ¿Que equipos han quedado no operativos?
 - ¿Cuales se pueden recuperar?
 - ¿En cuanto tiempo?
 - ¿Qué más se evalúa o debería evaluarse, según sus experiencias?
- Ejecución de Actividades.
 - ¿Se determina un coordinador que se encargará de las operaciones necesarias para que el sistema funcione correctamente, después de la emergencia?
 - Para cada tipo de emergencia, de las enumeradas arriba, ¿qué acciones se deben tomar para que el sistema vuelva a su funcionamiento normal?
- Evaluación de Resultados.
 - ¿Se evalúan los desempeños de las personas, y del Plan, luego de ocurrido el desastre?
 - ¿Se genera una lista de recomendaciones para minimizar los riesgos?
- Retroalimentación del Plan de Acción.
 - ¿Se evalúa el desempeño del personal durante el desastre?

- ¿Se tiene en cuenta la información que se obtiene luego de una emergencia para retroalimentar el Plan?
 - ¿Se reordena la lista de personal afectado en tareas de emergencia, con esta experiencia obtenida?
 - ¿Se modifican las prioridades? ¿Qué elemento tenía demasiada prioridad?
 - ¿Qué actividades faltaron incluir en el plan de emergencia?
 - ¿Qué se mejoraría?
 - ¿Cuál hubiera sido el costo de no haber tenido el plan de contingencias? ¿Qué se hubiera perdido?

ACCESO: es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal, desde donde pueden ser vistos, modificados o eliminados.

ACTIVE X: es un lenguaje de programación apoyado en controles OLE, Visual Basic y librerías del entorno Windows (OCX) de Microsoft. Active X permite que interactúen aplicaciones Windows con el World Wide Web (Internet).

ADSL: (Asymmetric Digital Suscribe Line - Línea de Usuario Digital Asimétrica). Usa la infraestructura telefónica actual para proveer servicios de transmisión de datos en alta velocidad.

AMENAZA: cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal o equipo informático, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

ANTIVIRUS: son todos aquellos programas que permiten analizar memoria, archivos y unidades de disco en busca de virus. Una vez que el antivirus ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus.

ARCHIVO DE PROCESO POR LOTES (.BAT o BATCH): los ficheros de proceso por lotes o ficheros Batch se caracterizan por tener extensión BAT. Son ficheros de texto que contienen comandos, uno por cada línea escrita. Cuando se ejecuta este tipo de ficheros, cada una de las líneas en él escritas se va ejecutando de forma secuencial.

ARCHIVO, DOCUMENTO: estos términos tienen el mismo significado y hacen referencia a la información que se encuentra en un soporte de almacenamiento informático. Es el trabajo real que realiza cada usuario (textos, imágenes, bases de datos, hojas de cálculo, etc.). Cada uno de ellos se caracteriza por tener un nombre identificativo. El nombre puede estar seguido de un punto y una extensión, compuesta por tres caracteres que identifican el tipo de fichero del que se trata. Algunas extensiones comunes son: EXE y COM (ficheros ejecutables, programas), TXT y DOC (ficheros de texto), etc.

ATAQUE: término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

ATAQUE ACTIVO: acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

ATAQUE PASIVO: intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la interceptación de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

AUDITORÍA: llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

AUTENTICIDAD: capacidad de determinar si una lista de personas han establecido su reconocimiento y/o compromiso sobre el contenido del documento electrónico.

BASES DE DATOS: Es un conjunto de datos interrelacionados y un conjunto de programas para accederlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

BIOS: es la abreviatura de Basic Input / Output System e identifica al software o conjunto de programas que arrancan el ordenador (antes de encontrarse un disco de sistema) cuando se pulsa el botón de encendido. La BIOS es un programa que se no se encuentra en la memoria RAM (Random Access Memory – memoria de acceso aleatorio) pues al apagar el ordenador se borraría, sino en la memoria principal o ROM (Read Only Memory - Memoria de Sólo Lectura), cuyo almacenamiento es permanente.

CARPETA: se trata de divisiones (no físicas sino lógicas) en cualquier tipo de disco donde son almacenamos determinados ficheros. Forman parte de una manera de organizar la información del disco, guardando los documentos como si de una carpeta clasificadora se tratase.

CHAT: se trata de conversaciones escritas en Internet. Mediante una conexión a la red y un programa especial, es posible conversar (mediante texto escrito) con un conjunto ilimitado de personas, al mismo tiempo

COBOL: (Common Organization Business Oriented Language) lenguaje de programación creado en la década del 60.

CONFIDENCIALIDAD: capacidad de mantener datos inaccesibles a todos, excepto a una lista determinada de personas.

COOKIE: procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para su posterior recuperación. En la práctica la información es proporcionada desde el visualizador al servidor del Word Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

CPD: centro de procesamiento de datos, centro de cómputos.

CRIPTOGRAFÍA: (encriptación) es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.

DATOS: los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos

en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

DEPARTAMENTO DE CÓMPUTO: es la entidad encargada del buen uso de las tecnologías de la computación, organización y optimización de los recursos computacionales de la institución. Es la entidad encargada de desarrollar el plan estratégico que favorezca la prestación de servicios eficientes, eficaces y de utilidad en la transmisión de datos para apoyar efectivamente los requerimientos del usuario. Es la entidad encargada de ofrecer sistemas de información administrativa integral permitiendo en forma oportuna satisfacer necesidades de información, como apoyo en el desarrollo de las actividades propias del centro.

DOMINIO: conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado un servidor de dominios.

DOS (MS/DOS): estas siglas significan Disk Operating System (DOS). Se refieren al sistema operativo (S.O.) anterior a Windows que, en su momento, creó la empresa Microsoft.

EQUIPO DE CÓMPUTO: dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

EQUIPO DE TELECOMUNICACIONES: todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

FILTRO DE PAQUETES: programa que intercepta paquetes de datos, los lee y rechaza los que no estén en un formato predefinido.

FINGER: programa que muestra información acerca de un usuario específico, o acerca de todos los usuarios, conectados a un sistema remoto. Habitualmente se muestra el nombre y apellido, hora de la última conexión, tiempo de conexión sin actividad y terminal. Puede también mostrar archivos de planificación y de proyecto del usuario.

FIREWALL: es un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

FIRMA DIGITAL: valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

FTP: (File Transfer Protocol) protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos.

GUSANO: es programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos.

HACKER: persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

HOST: (sistema central) computador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP.

HTML: lenguaje de marcado de hipertexto, (Hyper-Text Markup Language) es el lenguaje con que se escriben los documentos en el World Wide Web (Internet).

HTTP: Protocolo de Transferencia de Hipertextos (Hyper-Text Transfer Protocol). Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

HUB: Un punto común de conexión de dispositivos en una red. Los hubs son usados comúnmente para conectar segmentos de una LAN. Un hub contiene múltiples puertos. Cuando un paquete llega al puerto, es copiado a los otros puertos, de esta manera los otros segmentos de la LAN pueden ver todos los paquetes. Un hub pasivo simplemente sirve de conductor de datos entre los diferentes puertos. Los llamados hubs inteligentes incluyen servicios adicionales como permitir a un administrador monitorear el tráfico y configurar cada puerto del hub. Estos hubs se conocen generalmente como hubs administrables (manageable hubs). Un tercer tipo de hub, llamado switching hub, lee la dirección de destino en cada paquete y lo envía al puerto correcto.

IDENTIFICACIÓN: un subtipo de autenticación, verifica que el emisor de un mensaje sea realmente quien dice ser.

INCIDENTE: cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

INFECCIÓN: es la acción que realiza un virus al introducirse, empleando cualquier método, en nuestro ordenador (o en dispositivos de almacenamiento) para poder realizar sus acciones dañinas.

INTEGRIDAD: se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

INTRANET: una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno.

IP ADDRESS: (Dirección IP) dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

ISP: (Internet Service Provider – Proveedor de servicios de Internet) Empresa que presta servicios de conexión a Internet.

LOCAL AREA NETWORK: (LAN) (Red de Área Local) red de datos para dar servicio a un área geográfica pequeña, un edificio por ejemplo, por lo cual mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

MACRO / VIRUS DE MACRO: una macro es una secuencia de operaciones o instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) realice de forma automática y secuencial. Estas son "microprogramas" que pueden ser infectados por los virus. Los documentos de texto, las bases de datos o las hojas de cálculo no son programas y por ello no deberían ser infectados por ningún virus. No obstante, en cada uno de los ficheros creados con este tipo de aplicaciones se pueden definir macros y éstas sí son susceptibles de ser infectadas. Los virus de macro son aquellos que infectan exclusivamente documentos, hojas de cálculo o bases de datos que tienen macros definidas.

MAN: Metropolitan Area Network. Red de Área Metropolitana.

MENSAJE DE DATOS: la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama o el telefax.

NAT: (Network Address Translation) las direcciones NAT son utilizadas comúnmente cuando se requiere conectividad de una LAN a Internet pero solo se tiene acceso a una sola dirección IP de Internet.

NAVEGADOR: (browser): término aplicado normalmente a programas usados para conectarse al servicio WWW.

POP: (Protocolo de Oficina de Correos - Post Office Protocol) programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita información de los mismos y utiliza al servidor como oficina despachadora de correo electrónico cuando el usuario envía una carta.

PRIVACIDAD: se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundida o transmitida a otros.

PROGRAMAS (FICHEROS .EXE y .COM): los ficheros, documentos o archivos se componen de un nombre (cuyo número de caracteres antiguamente se limitaba a 8) y una extensión que puede no existir o contener, hasta tres caracteres como máximo. Esta

extensión especifica el tipo de fichero. Si es EXE o COM, el fichero será un programa ejecutable. De esta forma si hacemos doble clic sobre él o escribimos su nombre, se realizarán determinadas acciones.

PROTOCOLO: descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.

PROXY: una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente.

REDIRECCIONAR: esta acción permite aplicar un nuevo destino. En el caso de los virus, se puede hablar de éste término cuando un virus es capaz (por ejemplo) de hacer que el sistema en lugar de acceder a una dirección en la que debería encontrar determinados componentes, es obligado por el virus a saltar o acceder a otra dirección diferente.

ROUTER: (direccionador) dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento.

SATAN: (Security Analysis Tool for Auditing Networks). Herramienta de Análisis de Seguridad para la Auditoria de Redes. Conjunto de programas para la detección de problemas relacionados con la seguridad.

SCRIPT: archivos con su extensión SCR que sirven para determinar los parámetros ("condiciones") con los que se deben ejecutar unos determinados programas. Permiten iniciar un programa con unas pautas fijadas de antemano.

SEGURIDAD: se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados. En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos. El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

SENDMAIL: aplicación de administración de correo electrónico propia del sistema operativo Linux.

SHTTP: (secure HTTP - HTTP seguro). Protocolo HTTP mejorado con funciones de seguridad con clave simétrica.

SISTEMA OPERATIVO (S.O.): existen dos términos muy utilizados en informática. Estos son los conceptos de hardware y software. El primero de ellos se refiere a todo lo que es físico y tangible en el ordenador, como unidades de disco, tarjetas gráficas, microprocesador, memoria, etc. Por otro lado está el software que se define como el conjunto de programas (o información) con la que puede trabajar el hardware (ficheros, directorios, programas ejecutables, bases de datos, controladores, etc.). El sistema operativo pertenece al software y más concretamente es el conjunto de programas (y ficheros o archivos de otro tipo) que permite que se pueda utilizar el hardware. Se puede

tener el mejor ordenador del mundo (el mejor hardware), pero si éste no tiene instalado un sistema operativo, no funcionará (ni siquiera se podrá encender). Algunos ejemplos de sistemas operativos son: MS/DOS, UNIX, OS/2, Windows 95/98/2000/NT, etc.

SMTP: (Simple Mail Transfer Protocol - Protocolo de Transferencia Simple de correo). Es el protocolo usado para transportar el correo a través de Internet.

SPAM: Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico.

SSL: (Secure Sockets Layer - Capa de Socket Segura). Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

TCP: (Transmission Control Protocol - Protocolo de control de Transmisión). Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

TELNET: Telnet es el protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto.

TEXTO PLANO: (Plain Text) se llama así al documento antes de ser encriptado.

TROJAN HORSE: (Caballo de Troya) programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

URL: (Localizador Uniforme de recursos - Uniform Resource Locator). Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web. El URL esta conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.sfp.gov.ar) más el directorio y el archivo referido.

WAN: Wide Area Network. Red de Area Extensa.

WEBMIN: es una aplicación con interface gráfica para la administración de sistemas Unix.

WWW: World Wide Web. Estrictamente la Web es la parte de Internet a la que accedemos a través del protocolo HTTP y en consecuencia gracias a browsers normalmente gráficos como Netscape o Internet Explorer.

BIBLIOGRAFÍA

1. Mario Gerardo Piattini Velthius, Emilio del Peso Navarro. 1998. **Auditoría Informática: un enfoque práctico**. Alfa-Omega - Ra-ma.
2. José Antonio Echenique. 1996. **Auditoría en Informática**. Mc Graw Hill.
3. Humberto David Rosales Herrera. **Determinación de riesgos en los centros de cómputos**. 1996. Editorial Trillas.
4. David Pitts, Hill Ball. **Red Hat Linux Unleashed. The comprehensive solution**. 1998. Sams Publishing.
5. BCRA (Banco Central de la República Argentina). “**Anexo a la Comunicación “A” 2659** - Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática”. 1998. www.bcra.gov.ar
6. BCRA (Banco Central de la República Argentina). “**Anexo a la Comunicación “C” 30275** - Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática- Fe de erratas”. 2001. www.bcra.gov.ar
7. BCRA (Banco Central de la República Argentina). “**Anexo a la Comunicación “A” 3198** - Texto ordenado actualizado de las Normas sobre Requisitos operativos mínimos del área de sistemas de información (SI) – Tecnología Informática”. 2001. www.bcra.gov.ar
8. Cobit (Control Objectives for Information Technology) “**Audit Guidelines**” 3ra. Edición. 2000.
9. Cobit (Control Objectives for Information Technology) “**Control Objectives**” 3ra. Edición. 2000.
10. ISO (International Standard Organization). “**Estándar de Seguridad ISO 17799**”
11. ISO (International Standard Organization). “The Common Criteria for Information Technology Security Evaluation” v2.1
12. DoD (Department of Defense) Rainbow Series Library. “**Trusted Network Interpretation of the TCSEC - Red Book**”. 1987.
13. DoD (Department of Defense) Rainbow Series Library. “**Password Management Guideline - Green Book**”. 1985.
14. SIGEN (Sindicatura General de la Nación). “**Normas generales control interno**”. Resolución SIGEN N° 107/98. 1998.
15. AGN (Auditoría General de la Nación). “**Normas de auditoria externa de la Auditoria General de la Nación**”. 1993.
16. ISACA (Information Systems Audit and Control Association). “**Planning the IS Audit**”. 1998.
17. ISACA (Information Systems Audit and Control Association). “**Normas generales para la auditoría de los sistemas de información**”. 1997.
18. NIST (National Institute of Standards and Technology - U.S. Department of Commerce).
19. NIST (National Institute of Standards and Technology - U.S. Department of Commerce). “**Generally Accepted Principles and Practices for Securing Information Technology Systems**”. Marianne Swanson y Barbara Guttman, 1996.
20. NIST (National Institute of Standards and Technology - U.S. Department of Commerce). “**Guide for Developing Security Plans for Information Technology Systems**” Marianne Swanson, 1998.
21. NIST (National Institute of Standards and Technology - U.S. Department of Commerce). “**Security Self-Assessment Guide for Information Technology Systems**” Marianne Swanson, 2001.
22. NIST (National Institute of Standards and Technology - U.S. Department of Commerce). “**Automated Tools for Testing Computer System Vulnerability**” W. Timothy Polk, 1992.
23. Cisco Systems. “**Cisco SAFE: A Security Blueprint for Enterprise Networks**”. Sean Convery y Bernie Trudel. 2000.
24. Cisco Systems. “**Beginner's guide to network security**”. 2001
25. CERT (Computer Emergency Response Team) “**Tutorial de seguridad**”.

26. **"IT Baseline Protection Manual - Standard security safeguards"**. Bundesanzeiger – Verlag, Alemania. 2001.
27. Hal Tipton, Micki Krause. **"Handbook of Information Security Management"**. Consulting Editors, 1998.
28. **"Internet Security Professional Reference, Second Edition"**. New Riders Publishing. 1997.
29. Gonzalo Alvarez Marañón. **"Manual onLine de Criptografía y Seguridad"**. Consejo Superior de Investigaciones Científicas (CSIC), Madrid, España. 1997.
30. Tomas Olovsson. **"A Structured Approach to Computer Security"**. Department of Computer Engineering, Chalmers University of Technology (Gothenburg – SWEDEN). Technical Report No 122, 1992.
31. Peter Vincent Herzog. **"Open-source security testing methodology manual"**, Idea Hamster, GNU, 2001.
32. **"Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network"** Macmillan Computer Publishing. 1998.
33. Steven Shaffler y Alan Simon. **"Network Security"**. AP Professional, 1994.
34. Jorge Tomás Curras. **"Transacciones comerciales en Internet"**. Columbus Internet Marketing & Consulting. Madrid. www.columbus-digital.com
35. **"SET Software Compliance Testing"**. SET Secure Electronic Transaction LLC. www.setco.org
36. **"Seguridad en Internet"**. Microsoft. www.microsoft.com
37. Ministerio de Economía de la Nación www.mecon.ar
38. Tim Dierks. **"SSL as a protocol security solution"**. Consensus Development Corp. www.consensus.com
39. **"Internet Firewalls and Security"**. 3Com. www.3com.com
40. **"Microsoft TechNotes"** - www.microsoft.com/technet
41. **"CERT"** - www.cert.org
42. Portales relativos a seguridad informática:
 - xwww.insecure.org
 - <http://securityfocus.com>
 - www.hispasec.com
 - <http://secinf.net>
 - www.securityportal.com.ar
 - www.itsec.gov.uk
 - www.privacyexchange.org