



FACULTAD DE CIENCIAS ECONÓMICAS
“LIC. JOSÉ BENJAMÍN CAÑAS”
LICENCIATURA EN ADMINISTRACIÓN DE EMPRESAS CON
ESPECIALIDAD EN COMPUTACIÓN



TEMA:
DISEÑO DE UN MANUAL DE SEGURIDAD DE LA INFORMACIÓN
COMPUTARIZADA PARA LAS INSTITUCIONES OFICIALES
AUTÓNOMAS

TRABAJO DE GRADUACIÓN PRESENTADO POR:

BLANCA MARGARITA CASCO DE RIVAS
ROSIMAR VIRGINIA ORELLANA MEZQUITA
SILVIA DORELI HERNÁNDEZ FLORES

PARA OPTAR AL GRADO ACADÉMICO DE:
LICENCIADO EN ADMINISTRACIÓN DE EMPRESAS CON
ESPECIALIDAD EN COMPUTACIÓN

NOVIEMBRE, 2001

SAN SALVADOR

EL SALVADOR

CENTROAMERICA

UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR

**LIC. JOSÉ MAURICIO LOUCEL
RECTOR**

**ING. NELSON ZÁRATE SÁNCHEZ
VICE RECTOR ACADÉMICO**

**LICDA. ANA MARTA CONCEPCIÓN MORENO DE ARAUJO
DECANO FACULTAD DE CIENCIAS ECONÓMICAS
“LIC. BENJAMÍN CAÑAS”**

**LIC. SAMUEL ERNESTO LINARES
ASESOR**

JURADOS

ING. GUILLERMO ANTONIO VALENCIA	PRESIDENTE
ING. SIGIFREDO PORTILLO	PRIMER VOCAL
LIC. SAMUEL ERNESTO LINARES	SEGUNDO VOCAL

NOVIEMBRE, 2001

SAN SALVADOR

EL SALVADOR

CENTROAMERICA

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”



ACTA DE EXAMEN PROFESIONAL

HABIENDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR: LOS INGENIEROS GUILLERMO ANTONIO VALENCIA GUZMAN, SIGIFREDO EDUARDO PORTILLO CHACON Y EL LICENCIADO SAMUEL ERNESTO LINARES POLANCO.

A LAS DIECINUEVE HORAS DEL DIA VEINTISIETE DE JULIO DEL AÑO DOS MIL UNO.

A LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

BLANCA MARGARITA CASCO DE RIVAS.

ROSIMAR VIRGINIA ORELLANA MEZQUITA.

SILVIA DORELI HERNANDEZ FLORES.

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"DISEÑO DE UN MANUAL DE SEGURIDAD DE LA INFORMACION COMPUTARIZADA PARA LAS INSTRUCCIONES OFICIALES AUTONOMAS".

PARA OPTAR AL GRADO DE: LICENCIATURA EN ADMON. DE EMP. CON ESP. EN COMPUTACION.
Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO: APROBADO
YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

SAN SALVADOR, VEINTISIETE DE JULIO DEL AÑO DOS MIL UNO.


PRIMER VOCAL
DR. SIGIFREDO EDUARDO PORTILLO CHACON.


SEGUNDO VOCAL
LIC. SAMUEL ERNESTO LINARES POLANCO.


PRESIDENTE DEL JURADO
DR. GUILLERMO ANTONIO VALENCIA GUZMAN.

DEDICATORIA

Al trino Dios (Mi Padre Celestial, a Jesús mi Salvador y al Espíritu Santo de Dios, mi ayudador y guiador) dedico este triunfo, pues a el sea la gloria, honra, alabanza y el poder, quien me impulso siempre a seguir, me dio las fuerzas y energías para no desmayar, quien me dio la inteligencia y sabiduría para alcanzar la victoria.

“Porque el Dios de todo Saber es Jehová”

1 Samuel 2:3

AGRADECIMIENTOS

A mi querido esposo: José Armando, a mis amadas y preciosas hijas: Margarita, Karen y Roxana, les expreso mi gratitud por su amor, comprensión y apoyo incondicional en todo, y hacer más ligera mi carga

Agradecimientos a mis amados hermanos en la fe, quienes con sus oraciones, me fortalecieron y me levantaron los brazos.

A mis compañeros de trabajo del Ministerio de Hacienda, les expreso mis agradecimientos por todo el apoyo que me brindaron durante el desarrollo de mi carrera y trabajo de grado, que Dios les bendiga.

A mis maestros, a nuestro asesor Licenciado Samuel Ernesto Linares por sus aportes en este logro y a mis compañeras de trabajo de grado Rosimar y Silvia con especial cariño.

Blanca Margarita Casco de Rivas

DEDICATORIA

Todo lo que poseemos nos es dado por Dios, que hay en esta tierra que podamos ofrecerle, que no tenga ya... Solo puedo ofrecerte mi vida misma, por eso a ti Jesús que fuiste mi compañero incansable, que pusiste muchas personas buenas que fueron ángeles a mi alrededor que me ayudaron, a ti que me fortaleciste hasta en el peor de los momentos, a ti que me diste motivos de lucha cuando me sentí derrotada, SIMPLEMENTE: A TI QUE ME PERMITISTE LLEGAR A ESTE PUNTO, A ti y solo a ti dedico la culminación de este esfuerzo durante estos cinco años.

AGRADECIMIENTOS

- *A mis padres por la educación que me procuraron, que fueron la base para llegar a este punto y por todas sus oraciones y apoyo que me acompañaron a lo largo de este esfuerzo.*
- *A todos mis maestros que formaron en mi el deseo por estudiar y me dieron las primeras herramientas para hacerlo .*
- *A Nicolás Arnoldo Santos, por creer en mi y darme animo.*
- *A Marta de Cordero, por darme el empujoncito necesario para iniciar esta empresa.*
- *A Nelson Armando Cansino por ser mi amigo y mi ángel durante el curso de las materias a lo largo de la carrera.*
- *A mi amado esposo Javier Morales Palma por apoyar mi decisión de estudiar, y ser un ejemplo de dedicación para los estudios.*
- *A mis hijos, mis queridos bebés Maverick Jared y Jonathan Adriel por acompañarme en el camino, que fueron los más bellos motivos que Dios me envió para perseverar.*
- *A Carmen Palma por darme apoyo y animo para la elaboración de este trabajo*
- *A Samuel Ernesto Linares, por guiarnos en lo que para nosotras era nuevo y desconocido, su asesoría fue la afinación de este trabajo.*

Rosimar Virginia Orellana Mezquita

DEDICATORIA

Dedico esta victoria a Dios Todopoderoso, a mi esposo Erasmo y a mi hijo Josué.

AGRADECIMIENTOS

A DIOS TODOPODEROSO

Le doy gracias por haberme guiado hasta aquí y renovar mis fuerzas cuando yo desfallecía, por el Título que es un regalo que de Él proviene, por sus misericordias que son nuevas cada mañana.

A MI AMADO ESPOSO

Por sus oraciones, su apoyo, su confianza y la motivación que día con día él me transmitía para seguir adelante, por aguantarme en los momentos difíciles y nunca protestar.

A MI HIJO

Por darme el tiempo que a él le correspondía, por sus oraciones y a pesar de su edad comprender, que tenía que reunirme y acceder.

A MI PASTOR

Porque siempre estuvo apoyándome con sus oraciones, intercediendo ante el Padre por mí, por esas palabras de aliento en el momento justo.

A MI HERMANA

Por su ayuda, por su aliento y por sus oraciones.

A MI SUEGRA ALBA DE CHÁVEZ

Por sus oraciones y por incentivarme a seguir adelante.

A MI CUÑADA ZULMA DE BATARSÉ

Por su apoyo en todo momento, por sus oraciones, por su ayuda incondicional de una u otra manera.

A LIC. SAMUEL ERNESTO LINARES

Por el tiempo, la paciencia y por la disposición de compartir sus conocimientos.

A MIS COMPAÑEROS DE TRABAJO Y A LA CONGREGACIÓN

Que colaboraron de una u otra manera, son muchas personas que estuvieron orando, dándome palabras de aliento y de valentía, que me ayudaron llevando o trayendo documentos, que Dios los Bendiga y les multiplique grandemente, por el apoyo brindado en este documento.

El fin de todo el discurso oído es este: Teme a Dios y guarda sus mandamientos; porque esto es el todo del hombre. Eclesiastés 12:13

Silvia Doreli Hernández Flores

INDICE

	Página
INTRODUCCIÓN	i
CAPÍTULO I - SITUACIÓN PROBLEMÁTICA	
1.1 PLATEAMIENTO Y DELIMITACIÓN DEL PROBLEMA	
1.1.1 Instituciones Oficiales Autónomas	1
1.1.2 Situación Problemática	2
1.1.3 Descripción del Problema.	3
1.1.4 Formulación del Problema	5
1.1.5 Justificación	5
1.1.6 Delimitación	7
1.1.7 Alcance	8
1.1.8 Limitaciones	10
1.1.9 Objetivos de la Investigación	10
CAPÍTULO II - MARCO TEÓRICO REFERENCIAL	
2.1 MARCO REFERENCIAL DE LA INVESTIGACIÓN	
2.1.1 Marco Histórico de la Información Computarizada	12
2.1.2 Marco Normativo	15
2.1.3 Marco Teórico	18
2.1.3.1 Sistemas de Información	18

2.1.3.2	Seguridad	22
2.1.3.3	Manuales	73
2.2	TEORIA ADOPTADA	83
2.2.1	Instituciones Oficiales Autónomas	83
2.2.2	Información Computarizada	84
2.2.3	Áreas que se consideran esenciales en la protección de la Información Computarizada	84
2.2.4	Tipo de manual que se ofrecerá	86

CAPITULO III - INVESTIGACIÓN DE CAMPO REALIZADA EN LAS INSTITUCIONES OFICIALES AUTÓNOMAS SUBVENCIONADAS

3.1	OBJETIVOS DE LA INVESTIGACIÓN	88
3.1.1	Objetivo General	88
3.1.2	Objetivos Específicos	88
3.2	METODOLOGÍA DE LA INVESTIGACIÓN	89
3.2.1	Método	89
3.2.2	Fuente de Investigación	89
3.2.3	Determinación del Universo	89
3.2.4	Determinación de la Muestra	90
3.2.4.1	Procedimiento de Selección de la Muestra	90
3.2.5	Técnicas de Recolección de los Datos	92

3.3	RECOLECCIÓN DE LOS DATOS	93
3.4	TABULACIÓN Y ANÁLISIS DE LOS DATOS	94
3.4.1	Tabulación de los Datos	94
3.4.2	Análisis de los Datos	145

PROPUESTA:

“DISEÑO DE UN MANUAL DE SEGURIDAD
DE LA INFORMACIÓN COMPUTARIZADA PARA
LAS INSTITUCIONES OFICIALES AUTÓNOMAS”

3.5	CONCLUSIONES Y RECOMENDACIONES	154
3.5.1	Conclusiones	154
3.5.2	Recomendaciones	155

BIBLIOGRAFÍA

ANEXOS

No. 1: Lista de Instituciones Oficiales Autónomas .

No. 2: Cuestionario Investigación Preliminar

No. 3: Cuestionario Investigación de Campo

INTRODUCCIÓN

Una de las principales preocupaciones de los administradores de sistemas y de los responsables de seguridad informática es que el usuario desconoce cuan necesario es observar medidas para proteger la información computarizada.

Por lo que la seguridad conlleva y requiere poner en práctica una serie de medidas que han sido plasmadas en un documento para la seguridad informática denominado “Manual De Seguridad Para La Información Computarizada En Las Instituciones

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Oficiales Autónomas” , el cual ayudará a la gestión de la seguridad en el área de informática en tales instituciones.

El contenido del presente trabajo de graduación es el siguiente:

Capitulo I, denominado Situación Problemática, el cual describe lo que son las instituciones autónomas y los problemas a los que está expuesta la información computarizada actualmente, en dichas instituciones, incluyendo el enunciado del problema, justificación, delimitación, alcance y limitaciones de la investigación.

Capitulo II, expone el resultado de la investigación bibliografica, como marco referencial, por lo que comprende el marco histórico de la información computarizada, el marco normativo, y el marco teórico que describe principalmente los temas: sistemas de información, seguridad y manuales. Y como punto final este capitulo comprende la teoría adoptada como resultado de la recopilación y análisis de la información teórica.

Capitulo III contiene la investigación de campo realizada en las instituciones oficiales autónomas subvencionadas, abarcando desde el establecimiento de objetivos, la descripción de la metodología utilizada, la tabulación y presentación de los datos, hasta lo que es el análisis de la información recopilada, confrontando la realidad con la teoría, para poder elaborar una propuesta que de solución a las necesidades encontradas.

La propuesta denominada “Diseño de un manual de seguridad de la información computarizada, para las instituciones oficiales autónomas”, es la fase del trabajo que presenta el producto de la investigación tanto teórica como práctica, y constituye un documento completo en sí mismo, por lo que tiene su propia numeración y contiene una serie de apartados que surgen, como respuesta a las necesidades detectadas y pretenden darles solución.

Finalmente se presentan una serie de conclusiones y recomendaciones que surgieron de toda la experiencia a lo largo de la elaboración de este trabajo.

TEMA: “DISEÑO DE UN MANUAL DE SEGURIDAD DE LA INFORMACIÓN COMPUTARIZADA PARA LAS INSTITUCIONES OFICIALES AUTÓNOMAS”

CAPÍTULO I

SITUACIÓN PROBLEMÁTICA

1.1 PLANTEAMIENTO Y DELIMITACIÓN DEL PROBLEMA

1.1.1 INSTITUCIONES OFICIALES AUTONOMAS

En el Salvador dentro del campo de la administración pública, funcionan las instituciones Oficiales Autónomas, que fueron creadas por Decreto, Mandato u Ordenanza Legal de conformidad a los artículos 121 y 122 de la Constitución Política de la República de El Salvador, de 1950; dicho decreto continuó en vigencia en el artículo 225 de la Constitución Política de 1983.

Los presupuestos especiales y sistemas de salario de las entidades autónomas tienen que someterse a la aprobación del Órgano Legislativo según Artículo 227 de la Constitución Política de 1983, antes citada.

Además de los fondos presupuestados, los organismos autónomos reciben amplio apoyo financiero del Estado en forma directa a través de transferencias corrientes y de capital, préstamos de tesorería y préstamos externos obtenidos mediante convenios subsidiarios.

Algunas de estas instituciones únicamente reciben subvención o subsidio del Estado al iniciar sus operaciones, luego generan u obtienen sus propios recursos, llegando a ser autofinanciables, por lo que se identifican como instituciones financieramente autónomas respecto del Gobierno Central. Otras en cambio, periódicamente o continuamente reciben aportes del Estado, bajo diferentes formas, y a veces de ellos

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

depende su continuidad, de modo que son financieramente dependientes, pero relativamente autónomas en lo administrativo.

Las Instituciones Oficiales Autónomas cuentan con estructura administrativa propia, similar a las de la empresa privada, pero diferente en cuanto a: normatividad de las funciones, selección de personal, sistema operativo, fuentes de financiamiento, rendición de cuentas, mercado forzado de usuarios, grado de politización y elementos socializantes.

La máxima autoridad administrativa de estas instituciones generalmente es la Junta Directiva y el Presidente de la misma, recayendo en este funcionario o Director Ejecutivo la dirección y la representación legal de la entidad.

1.1.2 SITUACIÓN PROBLEMÁTICA

Antes de la automatización computarizada, los datos sobre las personas o instituciones se mantenían y se aseguraban como registros en papel, dispersos en negocios o unidades organizacionales por separado. Los sistemas de información computarizados concentran los datos en archivos de computadora que pueden ser accedidos más fácilmente por mucha gente y grupos fuera de la institución. En consecuencia los datos automatizados pueden ser más susceptibles de destrucción, fraude, error y mal uso.

En nuestro país el incremento de tecnología de información ha obligado a que tanto empresas privadas como públicas se modernicen.

Las instituciones autónomas no son la excepción, en cuanto al uso de tecnología informática, cada una ha ido automatizando sus operaciones para el procesamiento de la

información, contando en la actualidad todas ellas con redes de información (existe una red cliente servidor instalada por el gobierno central con el objetivo de estandarizar los procesos financieros y de recursos humanos), algunas de estas instituciones además de esta red, cuentan con redes propias, en las que se destacan puntos comunes en cuanto a tipo de arquitectura, protocolos de comunicación, topología de red, sistema operativo, lenguajes de programación y bases de datos entre otros.

Toda organización posee un recurso muy valioso como lo es la información computarizada, relacionada con el que hacer y operatividad de cada organización. Pero cuando grandes cantidades de datos están almacenados electrónicamente, son más vulnerables que cuando se tienen en forma manual.

Los sistemas de tiempo compartido y de acceso remoto convirtieron la vulnerabilidad de la comunicación de datos en una cuestión decisiva de seguridad, hoy día dicha vulnerabilidad se agrava cada vez más con la proliferación de redes de computadoras.

1.1.3 DESCRIPCIÓN DEL PROBLEMA

A medida que la tecnología ha ido evolucionando y con ella la importancia de los sistemas de información de las instituciones públicas y privadas, la seguridad del entorno informático (hardware, software, comunicaciones, entre otros) se ha convertido en una de las grandes preocupaciones de los profesionales de esta actividad, ante esta situación los directivos de cada empresa deben entender claramente, que es necesario considerar las inversiones en medidas para proteger la información computarizada, que contribuyan a mantener la operatividad y rentabilidad de las empresas.

Pero la alta administración no está conciente de la importancia indiscutible de este factor, es por ello que la seguridad de la información computarizada es un aspecto que aún no se aborda con el adecuado rigor en algunas de estas empresas.

Por lo anterior, se consideró investigar la situación actual sobre la seguridad de la información computarizada en las instituciones denominadas Oficiales Autónomas (Subvencionadas) del municipio de San Salvador, a fin de diseñar un manual de seguridad de la información computarizada para tales instituciones, que les permita contrarrestar riesgos tanto fuera como dentro de las instituciones.

Dentro de los riesgos o peligros a que están expuestas las instituciones se mencionan los siguiente:

- Destrucción de las instalaciones donde se encuentra el área de informática (infraestructura inadecuada, incendio, inundación)
- Acceso de personas no autorizadas a las instalaciones (falta de vigilancia y/o controles de ingreso a las instalaciones)
- Pérdida total o parcial de la información (virus, política inadecuada de los backup)
- Daño a los archivos y/o información (por falta de equipo que permita proporcionar energía eléctrica en caso de ocurrir una falla en el suministro de la misma).
- Robo de información
- Operación inadecuada de los sistemas (por no contar con personal idóneo, para la operación de los mismos).

- Falta de mantenimiento preventivo en el hardware (provoca daños en los equipos)
- Falta de documentación y estandarización para el desarrollo de las aplicaciones con que cuentan.
- Ausencia de un plan de contingencias (provocar no seguir operando, en caso de desastres)
- Ausencia de personas responsables de la seguridad de la información computarizada
- Falta de un documento que norme la gestión de la seguridad en las Instituciones Oficiales Autónomas entre otros.

1.1.4 FORMULACIÓN DEL PROBLEMA

¿De que manera la información computarizada es afectada por la ausencia de un Manual de Seguridad en las Instituciones Oficiales Autónomas del municipio de San Salvador?.

1.1.5 JUSTIFICACIÓN

Las empresas se desarrollan en un medio globalizante que exige evolución permanente. Los avances en materia de tecnología y sus efectos socioeconómicos, agudizan la necesidad de estar creando cada día nuevas modalidades administrativas, de manera que se haga un uso racional de todos los recursos disponibles para la consecución de los objetivos de toda organización.

Por otra parte, desde 1991 El Salvador ingresó a un proceso continuo de modernización del sector público, tendiente a establecer las mejores relaciones entre Estado y sociedad,

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

en el marco de una economía de mercado y de un sistema democrático. Entre una de las normativas emanadas de la Secretaría Técnica de la Presidencia de la República, se encuentra el numeral 33; que menciona:

“La informática, como medio tecnológico para la administración, debe constituirse en herramienta efectiva para la toma de decisiones en todos los niveles.

Adicionalmente debe proveer nuevas alternativas de comunicar información a la ciudadanía, cliente final del Estado”¹

Toda empresa o institución sea ésta pública o privada se ve en la necesidad de procesar grandes volúmenes de datos, que se convierten posteriormente en información, en cuyo proceso interviene la tecnología informática, esta información es de suma importancia para cada institución y el no tenerla en el momento preciso puede provocar no dar el servicio oportuno o hasta pérdida parcial o total de la misma, causada por la vulnerabilidad a los desastres naturales, las fallas en el hardware y en el software, los errores de los empleados y el uso por personas no autorizadas, pueden evitar que los sistemas de información operen adecuadamente, es por ello la importancia de poner en práctica medidas de seguridad encaminadas a la protección de la información computarizada, siendo que ésta es un patrimonio valioso, que le permitirá contrarrestar riesgos y asegurar la continuidad del procesamiento de información necesaria, para el adecuado desempeño de las funciones institucionales.

Por lo anterior surgió la necesidad de realizar esta investigación para determinar la manera en que la información computarizada es afectada por la ausencia de elementos

¹ Normativa General Para la Modernización del Órgano Ejecutivo, Jul 23-1999

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

de seguridad en las Instituciones Oficiales Autónomas del municipio de San Salvador, a fin de analizar la posibilidad de elaborar un manual de seguridad de la información computarizada, el cual coadyuvará a la gestión de la seguridad para contrarrestar riesgos actuales y futuros que impida a dichas instituciones prestar sus servicios eficientemente, así como contribuir con la modernización de los servicios informáticos.

1.1.6 DELIMITACIÓN

1. Delimitación Espacial

Área de informática de las Instituciones Oficiales Autónomas subvencionadas del Órgano Ejecutivo.

2. Delimitación Temporal

En el período comprendido de Agosto del 2000 a Mayo del 2001.

3. Delimitación Social

Instituciones Oficiales Autónomas subvencionadas del Órgano Ejecutivo

4. Delimitación Geográfica

Se llevó a cabo en el Municipio de San Salvador en las Instituciones Oficiales Autónomas (subvencionadas) del Órgano Ejecutivo.

1.1.7 ALCANCE

La investigación se llevará a cabo estrictamente en el área de informática de las instituciones según muestra seleccionada, dicha investigación comprenderá el tema de la seguridad de la información computarizada, para ello se evaluará la seguridad física (la evaluación de la seguridad física no incluye la operatividad y funcionamiento de los programas), seguridad lógica, seguridad en el personal, además se evaluarán procedimientos de backup y respaldo, políticas de seguridad, y plan de contingencia. Todo esto a fin de hacer un diagnóstico de los riesgos, daños o peligros a los que está expuesta la información de dichas instituciones y poder así diseñar un manual que contenga un conjunto de normas, políticas, procedimientos, disposiciones y acciones, para la seguridad de la información computarizada en cada una de las instituciones en las que se enmarca la investigación.

Debido a que el ámbito de aplicación de la seguridad de la información computarizada es bien amplio, se hace necesario establecer parámetros para delimitar el problema, por lo que la investigación se enmarcará dentro de los límites sugeridos por José Antonio Echenique en su libro “Auditoria en Informática”² quien propone que la seguridad informática debe comprender los siguientes elementos: Seguridad física, Seguridad lógica y confidencialidad, Seguridad en el personal, Elementos Técnicos y Procedimientos, Elementos Administrativos, Participación de la Auditoria y Plan de Contingencia.

² José Antonio Echenique, Auditoria Informática, Mc Graw Hill L.R. 90

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Seguridad física

La seguridad física comprende los siguientes campos: vigilancia, protección de instalaciones, controles de seguridad, edificios y equipos de cómputo, entre otros.

Seguridad lógica y confidencialidad

Se relaciona con la protección de la información de cualquier transformación o pérdida, a través de un conjunto de normas y medidas.

Seguridad en el personal

Esta implica la protección de la confidencialidad y la confiabilidad del personal, y consiste en las medidas que se tomen para garantizar la integridad, estabilidad y lealtad del mismo.

Elementos técnicos y procedimientos

Se refiere a la definición por escrito de la información necesaria para garantizar la operación y utilización segura de los equipos.

Elementos administrativos

Están relacionados con el papel administrativo dentro de la seguridad, estableciendo sus responsabilidades y participación dentro de la misma.

Participación de la auditoria

Se relaciona, con el papel que los auditores deben tomar en cuanto a seguridad para la información computarizada.

Plan de contingencia

Se relaciona con el planeamiento de todas las acciones específicas, que se tomarán cuando surja un evento que no esté considerado en el proceso de planeación formal, comprendiendo un conjunto de procedimientos de recuperación para casos de desastres.

1.1.8 LIMITACIONES

Para realizar la investigación es necesario hacer uso de fuentes de información, pero éstas no siempre están disponibles, por lo que a continuación se mencionan algunas limitantes:

- 1) Falta de información bibliográfica sobre el tema
- 2) El acceso a la información primaria no es un 100%
- 3) No se tuvo el acceso a una institución que sirviera como caso práctico.

1.1.9 OBJETIVOS DE LA INVESTIGACIÓN

• General

Diseñar un manual de seguridad de la información computarizada para las Instituciones Oficiales Autónomas.

• Específicos

- a) Sintetizar la información bibliográfica sobre elementos de seguridad y las Instituciones Oficiales Autónomas Subvencionadas.
- b) Determinar elementos de seguridad, que poseen las Instituciones Oficiales Autónomas. Subvencionadas.

- c) Establecer si los elementos encontrados cumplen con los requerimientos de seguridad, para el manejo de la información computarizada.
- d) Diseñar un Manual de Seguridad de la Información Computarizada para las Instituciones Oficiales Autónomas Subvencionadas.

CAPÍTULO II:

MARCO TEÓRICO REFERENCIAL

2.1 MARCO REFERENCIAL DE LA INVESTIGACIÓN

2.1.1 MARCO HISTÓRICO DE LA INFORMACIÓN COMPUTARIZADA

La computación es el conjunto de conocimientos y técnicas en que se basan los procesos de tratamiento automático de la información, mediante computadoras u ordenadores electrónicos; y surge en la década de los años 40 de este siglo y a lo largo de su evolución ha experimentado cambios drásticos a medida que la tecnología avanza.

En sus inicios se caracterizó por la utilización de tubos al vacío, que más adelante fueron sustituidos por transistores. De igual forma el uso de tarjetas perforadas se reemplazó por micro chips y las bandas magnéticas que permitieron introducir y extraer información de la computadora con mayor rapidez y a la vez albergan una mayor condensación de la información en un espacio muy reducido.

La idea de utilizar la computación como herramienta para el tratamiento de grandes cantidades de datos, surgió durante un censo realizado en los Estados Unidos de forma manual que duró 3 años, entonces al acercarse el nuevo censo y enfrentarse a que aún no se había completado el procesamiento de los datos del primero, dio pie a la utilización de la computación para el tratamiento de información, por ello el término informática es usado en sustitución de computación.

Una computadora interactúa con el mundo a través de una o más aplicaciones que realizan tareas específicas y manejan entradas y salidas. Si ésta computadora es parte de una red, algunas de estas aplicaciones deberán ser capaces de comunicarse con aplicaciones que se encuentren en otra red de computadoras. Una ***suite de protocolos de red*** es un sistema de reglas comunes de que ayudan a definir el complejo proceso de la transferencia de datos. Los datos viajan de una aplicación que está en una computadora hacia el hardware de red de la misma, y luego por el medio de transmisión hasta el hardware de red de la computadora de destino, que a su vez los envía a la aplicación receptora.

La información son los datos procesados para la toma de decisiones, en un sistema integrado usuario máquina que suministra información, ésta apoya las operaciones de administración, análisis y funciones de toma de decisiones, ésta información debe ser previamente clasificada.

Además el surgimiento y mejora de los sistemas de tratamiento de base de datos, y el sistema de información entre otros, han contribuido a concretar como fin primordial de la computación ofrecer soporte a la información.

Hasta la década de los años ochenta la información en sí no se consideraba como un activo de importancia para la empresa, pero en la actualidad los cambios mundiales como el surgimiento de la economía global y la transformación de economías industriales en economías de servicio, han alterado el entorno de las empresas y le han dado una perspectiva diferente a la importancia del conocimiento y la información.

Son éstas necesidades crecientes de información y los avances tecnológicos los que dan origen a los sistemas de información.

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de ésta.

La preocupación sobre la seguridad informática es un fenómeno relativamente reciente. En el entorno de grandes sistemas, se ha abordado desde sus inicios en gran parte porque el desarrollo inicial de los sistemas informáticos fueron llevados a cabo por las agencias de inteligencia, pero siempre se han dejado de lado de forma involuntaria, elementos vitales para garantizar la protección de la información.

Uno de los factores que ha tenido que considerarse dentro de la seguridad es la protección contra virus, el cual aunque tiene diferentes intenciones cuando surgieron se encontraban principalmente para paquetes que eran copiados sin autorización y borraban toda la información que se tenía en un disco.

Históricamente los virus informáticos fueron descubiertos por la prensa el 12 de octubre de 1985, con una publicación del New York Times que hablaba de un virus que se difundió y aparentemente era para optimizar los sistemas IBM basados en tarjeta gráfica EGA, pero al ejecutarlo salía la presentación y al mismo tiempo borraba todos los archivos del disco duro, con un mensaje al finalizar que decía “caíste”.

Pero las primeras referencias de virus con fines intencionales surgieron el 1º. De abril de 1983 cuando Digital Equipment Corporation (DEC) empleó una subrutina para proteger su famoso procesador de textos Decmate II, que en caso de copia ilegal borraba todos

los archivos de su unidad de disco. Actualmente los virus tienen infinidad de motivos y formas de propagación.

En los años de 1990, empieza la preocupación principal por la seguridad en nuestro país, lógicamente mientras más son los usuarios de los sistemas más es el riesgo que se corre. Uno de los peligros más grandes se encuentra en las redes de comunicación, pues contienen vacíos de seguridad y en muchas ocasiones se consideran como normales.

2.1.2. MARCO NORMATIVO²

Debido a la importancia que tiene para las empresas la información y el auge que está teniendo el procesamiento de información en forma computarizada, ha sido necesario incluir en las legislaciones algunas disposiciones con el objetivo de protegerla.

En nuestro país la legislación en el Código Penal, actualizado en enero de 2000, cubre las áreas siguientes:

1. Daños a instalaciones físicas:

Cuando el propósito de ocasionar perjuicio, destruyere, inutilizare, hiciere desaparecer o deteriorare una cosa total o parcialmente ajena, mediante manipulación informática, se impondrá prisión de 2 a 7 años (Art. 221 y numeral 2 del Art. 222).

2. Estafas o fraudes:

El delito de estafa será sancionado con prisión de cinco a ocho años cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos. (Numeral 5 del Art. 216).

² Según Código Procesal Penal de El Salvador, en lo referido a daños

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

3. Derechos de autor:

Las leyes de derecho de autor y las disposiciones del Código Penal en el capítulo VII de los delitos relativos a la Propiedad Intelectual así como los tratados internacionales sobre derechos de autor, protegen al software de la copia ilegal. Dichas leyes y tratados protegen los derechos del autor del software y le otorgan una variedad de derechos exclusivos, que incluyen el derecho a producir o “copiar” el software. La copia del software sin la autorización del autor constituye una violación a los derechos de autor y la ley condena a los infractores.

Es necesario estar al tanto de que las siguientes conductas violan el contrato de licencia y pueden ser contrarias a la ley:

- a) Copiar o distribuir software, programas, aplicaciones, códigos y manuales sin permiso ni licencia del titular de los derechos de autor.
- b) Ejecutar un programa en dos o más computadoras simultáneamente, salvo que esté permitido expresamente en el contrato de licencia.
- c) Estimular, permitir, obligar o presionar a empleados de empresas a reproducir, o usar copias no autorizadas.
- d) Infringir las leyes que prohíben la copia ilegal de software porque alguien lo pide o lo exige.
- e) Prestar programas para que sean copiados o copiar programas que han sido pedidos en préstamos
- f) El que produjere, plagiar, distribuyere o comunicare públicamente, en todo o en parte, una obra literaria, artística, científica o técnica o su

transformación o una interpretación o ejecución artística plagiada en cualquier tipo de soporte o fuere comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios, será sancionado con prisión de uno a tres años.(Artículo 226 pág.57)

- g) La instalación en la memoria temporaria de una computadora cuando se ejecuta el programa desde un disco, desde el disco duro, desde un CD-ROM, u otro medio de almacenamiento.
- h) La copia del software en otro medio, como un disquete o el disco duro de una computadora;
- i) La ejecución del programa en una computadora desde un servidor de red en el que reside o se ha guardado el software.

Los propietarios de los derechos de autor de la mayoría del software comercial otorgan de manera directa o indirecta una licencia para que el cliente use el software de acuerdo a lo establecido en un tipo de contrato denominado “contrato de licencia de usuarios final” (conocido también como CLUF).

El CLUF se puede encontrar en uno o en varios lugares diferentes, dependiendo del producto. Los tres lugares más comunes donde puede encontrar el contrato de licencia son:

- Impreso en una hoja de papel separada que acompaña el producto adquirido;

- Impreso en el manual del usuario, generalmente en el interior de la cubierta superior o en la primera página del manual; en forma electrónica y en pantalla, dentro del producto del software.

4. Violación de la confidencialidad:

El que se apodera de documentos, soporte informático u otros objetos, para descubrir o revelar un secreto evaluable económicamente, perteneciente a una empresa y que implique ventajas económicas será castigado con prisión de seis meses a dos años.

2.1.3. MARCO TEÓRICO

2.1.3.1 SISTEMAS DE INFORMACIÓN (SI)

a) Concepto de Sistema de Información

Es un conjunto de componentes relacionados entre sí que permiten capturar, procesar, almacenar y distribuir la información para apoyar la toma de decisiones y el control de una institución. Para apoyar lo anterior, los sistemas de información pueden ayudar a los administradores y al personal a analizar problemas y crear nuevos productos.

Un SI produce la información que la institución requiere para la toma de decisiones, control de las operaciones, análisis de problemas y creación de nuevos productos por medio de tres actividades

Alimentación o insumo: La captura o recolección de datos primarios dentro de la institución o de su entorno para procesarlos en un sistema de información.

Procesamiento: La conversión de insumo en forma que sea más comprensible para los seres humanos.

Producto o salida: La distribución de información procesada a las personas o en las actividades en donde será usada.

Aparte de estas actividades los SI requieren de retroalimentación que se define como "el producto regresado a personas indicadas dentro de la institución para ayudarles a corregir la etapa de alimentación.

Cabe destacar, que los sistemas de información, se pueden clasificar en:

Sistemas de información basados en computadoras:

Sistemas Informales: operan bajo reglas no establecidas de comportamiento.

Sistemas Formales: son estructurados, operan bajo reglas predeterminadas fijas.

- Manuales. (tecnología papel y lápiz)
- Basados en computadoras (SIBC, tecnología de HW, SW de la computadora).

b) ¿Porque Sistemas de Información?

Hasta la década de los ochenta los administradores no necesitaban saber como la información se obtenía, procesaba y distribuía en sus instituciones, requiriendo un mínimo de tecnología. La información en sí no se consideraba como un activo de importancia para la empresa.

En la actualidad pocos administradores pueden darse el lujo de ignorar como se maneja la información al interior de las instituciones y dado que es un apoyo a la tecnología de decisiones.

c) Importancia de la información

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Cuando se habla de la función informática generalmente se tiende a hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información más consistente, entre otros.

Sin embargo se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la información.

Es muy importante conocer su significado dentro la función informática, de forma esencial cuando su manejo está basado en tecnología moderna, para esto se debe conocer que la información:

- Está almacenada y procesada en computadoras;
- Puede ser confidencial para algunas personas o a escala institucional;
- Puede ser mal utilizada o divulgada;
- Puede estar sujeta a robos, sabotaje o fraudes

Los primeros puntos nos muestran que la información esta centralizada y que puede tener un alto valor y los últimos puntos nos muestran que se puede provocar la destrucción total o parcial de la información, que incurre directamente en su disponibilidad que puede causar retrasos de alto costo. Pensemos por un momento que hoy se sufre un accidente en el centro de cómputo o el lugar donde se almacena la información. Ahora preguntémonos: ¿Cuánto tiempo pasaría para que la organización este nuevamente en operación? Es necesario tener presente que el lugar donde se centraliza la información con frecuencia es el centro de cómputo, puede ser el activo más valioso y al mismo tiempo el más vulnerable.

d) Tipos de Sistemas de Información

Los diferentes tipos de sistemas de información están destinados a procesar datos: capturan los detalles de las transacciones, permiten que se tomen decisiones o comunicar la información entre personas y localidades.

Los tipos de sistemas de información que existen son:

1. Sistema de procesamiento de transacciones
2. Sistema de información gerencial
3. Sistema de apoyo para la toma de decisión
4. Sistema de información para oficinas

Sistema de procesamiento de transacciones

Procesa datos referente a las transacciones. Las razones del procesamiento son: registro, clasificación, orden, cálculo, sintetización, almacenamiento, visualización de los resultados.

Sistema de información gerencial

Proporciona información para el apoyo en la toma de decisiones donde los requisitos de información pueden identificarse de antemano. Las decisiones respaldadas por este sistema frecuentemente se repiten.

Sistema de apoyo para la decisión

Ayuda a los gerentes en la toma de decisiones únicas y no reiteradas que relativamente no están estructuradas.

Parte del proceso de la decisión consiste en determinar los factores a considerar cuál es la información innecesaria.

Sistemas de información para oficinas

Combina actividades de procesamiento de datos, transferencia de datos y procesamiento de palabras destinadas a automatizar el manejo de la información para la oficina. Frecuentemente extrae datos almacenados como resultado de un procesamiento de datos. Incluye el manejo de la correspondencia, reportes y documentos.

Los sistemas de información son la base de muchas de las actividades que ocurren en las organizaciones y en la sociedad. Las organizaciones con éxito generalmente han aprendido cómo utilizar la información como un instrumento eficaz para la administración. Y han desarrollado sistemas de información que responden a las necesidades de las personas.

Los sistemas de información en los que intervienen las computadoras se llaman sistemas de información computarizados.

Estos sistemas de información computarizados son accesibles a una gran variedad de usuarios. Con una computadora personal se puede manejar información contable y administrativa para probar el impacto de estrategias alternas así como evaluar el motivo de los resultados actuales de la empresa; resumir grandes volúmenes de datos en una visualización o presentación gráfica.

2.1.3.2 SEGURIDAD

La seguridad es una cualidad o estado de seguro, garantía o conjunto de garantía que se da a alguien sobre el cumplimiento de algo.

Ejemplo: Seguridad Social que es un conjunto de organismos, medios, medidas, entre otros, de la administración estatal para prevenir o remediar los posibles riesgos,

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

problemas y necesidades de los trabajadores, como enfermedad, accidentes laborales, incapacidad, maternidad o jubilación; se financia con aportaciones del estado, trabajadores y empresarios.

Se dice también de todos aquellos objetos, dispositivos, medidas, entre otros, que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa. La seguridad se resume entonces como la protección de los recursos con que cuenta una organización.

SEGURIDAD INFORMÁTICA

Es un conjunto de disciplinas entrelazadas que tienen como finalidad la protección contra accidentes o daños a todos los recursos con los que cuenta la unidad de informática, afín de identificar sus causas y eliminarlas o disminuirlas.

Objetivo de la seguridad informática

El objetivo de la seguridad es garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas o de la información contenida en ellos, así como tratando de proteger las redes privadas y sus recursos mientras que se mantienen los beneficios de la conexión, ya sea una red local o una red publica como lo es Internet.

Los recursos informáticos se pueden agrupar en tres tipos principales:

Recursos Humanos los cuales están constituidos por el personal de informática, los usuarios y staff.

Instalaciones y equipo este se refiere al Hardware (CPU, consola de operación), los dispositivos de almacenamiento (discos, cintas), los dispositivos de entrada/salida (impresoras, terminales), equipo especial (controladores, servidores), Equipo de respaldo

(archivos documentados), edificio (pisos instalaciones eléctricas, cristales), equipo de comunicación (módem multiplexores, cables).

Datos e información compuesto por el software (sistema operativo, utilerías, paquetes, aplicaciones desarrolladas), Administrativos (documentos, procedimientos), Registros y estadísticas (de personal, financieros y de ventas).

ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN

Entre los aspectos más importantes para la seguridad de la información se encuentran los siguientes:

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.

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.

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.

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), vídeo (secuencia o tramas), etc.

Base de datos: Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

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.

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.

Ataque pasivo: Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intersección de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

Amenaza. Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ej. Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

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.

Golpe (breach). Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, entre otros.

PRINCIPIOS FUNDAMENTALES DE LA SEGURIDAD INFORMÁTICA

En el ámbito de la seguridad informática existen una serie de principios básicos que es necesario tener en cuenta al diseñar cualquier política de seguridad, a continuación se detallan:

1. Principio de menor privilegio

Éste es quizás el principio más fundamental de la seguridad, y no solamente de la informática. Básicamente, el principio de menor privilegio afirma que cualquier objeto (usuario, administrador, programa, sistema, entre otros) debe tener tan sólo los privilegios de uso necesario para desarrollar su tarea y ninguno más. Esto quiere decir que cualquier usuario tan solo debe poder acceder a los recursos que necesite, para realizar las tareas que tenga encomendadas y sólo durante el tiempo necesario.

Al diseñar cualquier política de seguridad es necesario estudiar las funciones de cada usuario, programas, entre otros, definir los recursos a los que necesita acceder para llevarlas a cabo, identificar las acciones que necesita realizar con estos recursos, y establecer las medidas necesarias para que tan solo pueda ejecutar estas acciones.

2. La seguridad no se obtiene a través de la oscuridad

Un sistema no es más seguro porque escondamos sus posibles defectos o vulnerabilidades, sino porque los conozcamos y corriamos estableciendo las medidas de seguridad adecuadas. El hecho de mantener posibles errores o vulnerabilidades en secreto no evita que existan, y de hecho evita que se corrijan.

No es buena medida basar la seguridad en el hecho de que un posible atacante no conozca las vulnerabilidades de nuestro sistema. Los atacantes siempre disponen de los medios necesarios para descubrir las debilidades más insospechadas de nuestro sistema.

No se consigue proteger un sistema evitando el acceso de los usuarios a la información relacionada con la seguridad. Por ejemplo, evitando el acceso a determinados manuales donde se especifican las órdenes que pueden utilizarse para entrar en el sistema. Educar

a los usuarios o diseñadores sobre el funcionamiento del sistema y las medidas de seguridad incluidas, suele ser mejor método para protegerlo.

No obstante tampoco se trata de hacer público en las noticias un nuevo fallo de nuestro sistema o un método para romperlo. En primer lugar hay que intentar resolverlo, obtener un medio para eliminar la vulnerabilidad y luego publicar el método de protección.

3. Principio del eslabón más débil

En todo sistema de seguridad, el máximo grado de seguridad es aquel que tiene su eslabón más débil. Al igual que en la vida real la cadena siempre se rompe por el eslabón más débil, en un sistema de seguridad el atacante acaba encontrando y aprovechando los puntos débiles o vulnerabilidades.

Cuando se diseña una política de seguridad o establezcamos los mecanismos necesarios para ponerla en práctica, debemos contemplar todas las vulnerabilidades y amenazas. No basta con establecer mecanismos muy fuertes y complejos en algún punto en concreto, sino que hay que proteger todos los posibles puntos de ataque.

4. Defensa en profundidad

La seguridad de nuestro sistema no debe depender de un solo mecanismo por muy fuerte que éste sea, sino que es necesario establecer varios mecanismos sucesivos. De este modo cualquier atacante tendrá que superar varias barreras para acceder a nuestro sistema.

Por ejemplo en nuestro sistema podemos establecer un mecanismo de password altamente seguro como primera barrera de seguridad. Adicionalmente podemos utilizar algún método criptográfico fuerte para cifrar la información almacenada. De este modo

cualquier atacante que consiga averiguar nuestro password y atravesar la primera barrera, se encontrará con la información cifrada y podremos seguir manteniendo su confidencialidad.

5. Punto de control centralizado

Se trata de establecer un único punto de acceso a nuestro sistema, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él. No se trata de utilizar un solo mecanismo de seguridad, sino de “alinearlos” todos de modo que el usuario tenga que pasar por ellos para acceder al sistema.

Este único canal de entrada simplifica nuestro sistema de defensa, puesto que nos permite concentrarnos en un punto único. Además nos permite monitorizar todos los accesos o acciones sospechosas.

6. Seguridad en caso de fallo

Este principio afirma que en caso de que cualquier mecanismo de seguridad falle, nuestro sistema debe quedar en un estado seguro. Si nuestros mecanismos de control de acceso al sistema fallan, es mejor que como resultado no dejen pasar a ningún usuario.

Por ejemplo cuando hay un corte de fluido eléctrico los ascensores están preparados para bloquearse mediante algún sistema de agarre, mientras que las puertas automáticas están diseñadas para poder abrirse y no quedar bloqueadas.

7. Participación universal

Para que cualquier sistema de seguridad funcione es necesaria la participación universal, o al menos no la oposición activa de los usuarios del sistema. Prácticamente cualquier

mecanismo de seguridad que establezcamos puede ser vulnerable si existe la participación voluntaria de algún usuario autorizado para romperlo.

La participación voluntaria de todos los usuarios en la seguridad de un sistema es el mecanismo más fuerte conocido para hacerlo seguro. Si todos los usuarios prestan su apoyo y colaboran en establecer las medidas de seguridad y en ponerlas en práctica el sistema siempre tenderá a mejorar.

8. Simplicidad

La simplicidad es un principio de seguridad por dos razones. En primer lugar, porque mantiene las cosas lo más simple posible, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro. En segundo lugar, la complejidad permite esconder múltiples fallos. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.

LOS CONTROLES INTERNOS EN LA SEGURIDAD

Los controles se definen como las acciones tomadas para dirigir un hecho conforme a un plan previamente establecido.

Clases De Controles Internos

Atendiendo al momento en que se actúa:

1. **Controles preventivos:** establecen las condiciones necesarias para que el error no se produzca. Como ejemplos de controles preventivos tenemos la segregación de funciones, la estandarización de procedimientos, las autorizaciones, las passwords, o los formularios prenumerados.

-
2. **Controles detectivos:** identifican el error pero no lo contrarrestan, actuando solo como alarmas que permiten registrar el problema y sus causas. Sirven como verificación del funcionamiento de los procesos y de sus controles preventivos. Como ejemplo tenemos la validación de los datos de entrada, cuando se realiza con posterioridad al procesamiento de dichos datos, los totales de control, los controles cruzados o los controles de supervisión, estos últimos se componen de tres tipos de controles:
- a. Controles de aplicaciones
 - b. Controles de tecnologías de la información
 - c. Controles de usuario
3. **Controles correctivos:** permiten investigar y rectificar los errores y sus causas, están destinados a procurar que las acciones necesarias para su solventación sean tomadas. Como ejemplos de estos tenemos los listados de errores, las evidencias de auditoría o las estadísticas de causas de errores.

CONTROLES DE LA TECNOLOGÍA DE INFORMACIÓN

Son el conjunto de normas y procedimientos que deben existir en todo Centro de Proceso de datos para asegurar la confidencialidad, integridad y disponibilidad de los datos informatizados.

Aseguran que los procedimientos programados dentro de un sistema informático se diseñen, implanten, mantengan y operen de forma adecuada y que solo se introduzcan cambios autorizados en los programas y en los datos. Dentro de los controles de la

tecnología de información nos encontraremos con distintos tipo de controles entre los cuales están:

- **Controles de seguridad informática:** la dirección debe asegurar la implantación de políticas de control de: la dirección del proyecto debe garantizar que el control del diseño, desarrollo e implantación de las nuevas aplicaciones es adecuado, en caso de implantar un paquete informático adaptado hay que asegurarse que cumple acceso basadas en el nivel de riesgo que se deriva del acceso a los programas y a los datos. El acceso a funciones concretas dentro de las aplicaciones debe estar adecuadamente restringido para asegurar la segregación de funciones relevantes y evitar actividades no autorizadas además de estar restringido el acceso físico a los ordenadores. Este tipo de controles evitarán el riesgo de fraude o de que información confidencial o sensible llegue a personas no autorizadas dentro o fuera de la institución. Otro riesgo que evitaríamos con la seguridad física sería el posible daño o destrucción de las instalaciones informáticas como resultado de incendios, inundaciones o sabotajes que podrían interrumpir la ejecución de los procesos.
- **Controles de desarrollo e implantación de aplicaciones** con las exigencias del negocio, para ello debe verificarse que cada una de las etapas se realiza basándose en las políticas y procedimientos definidos por la empresa.
- **Controles de mantenimiento:** destinados a asegurar que las modificaciones de los procedimientos programados están adecuadamente diseñadas, probadas, aprobadas e implantadas.

- **Controles de seguridad de programas:** destinados a garantizar que no se puedan efectuar cambios no autorizados en los procedimientos programados
- **Controles de Seguridad de Ficheros de datos:** destinados a asegurar que no se puedan efectuar modificaciones no autorizadas en los archivos de datos.
- **Controles de la operación informática:** destinados a garantizar que los procedimientos programados autorizados se aplican de manera uniforme y se utilizan versiones correctas de los ficheros de datos. Los procedimientos de operaciones que cubren procesos diferidos por lotes que se realizan en momentos específicos deben estar documentados, programados y mantenidos de forma adecuada. Las copias de seguridad de los programas y de los datos deben estar siempre disponibles para casos de emergencia. Las instalaciones informáticas de los usuarios finales deben ser apropiadas para las necesidades de la empresa y controladas para maximizar la compatibilidad y apoyar eficazmente al usuario. Con todos estos controles podemos evitar fallos en los equipos y en el software o como mínimo tendremos capacidad para recuperarnos de ellos (ya que la continuidad del negocio puede estar en juego) o sacar poco rendimiento de los sistemas informáticos.
- **Controles de conversión de ficheros:** destinados a garantizar una completa y exacta conversión de los datos de un sistema antiguo a uno nuevo.
- **Controles de software Sistema:** destinados a asegurar que se implante un software de sistema apropiado y que se encuentre protegido contra modificaciones no autorizadas.

- **Controles de implantación:** destinados a asegurar que los procedimientos programados para los nuevos sistemas son adecuados y están efectivamente implantados, y que el sistema está diseñado para satisfacer las necesidades del usuario.

ELEMENTOS DE SEGURIDAD

Elementos de seguridad son aquellos que forman parte de un sistema de trabajo y que coordinados integralmente ayudan a proteger un ente o una cosa.

La protección no ha de basarse solo en dispositivos y medios físicos, sino en formación e información adecuada al personal, empezando con los directivos, para que en cascada, afecte a todos los niveles de la pirámide organizativa. Además, la existencia de funciones específicas cuando el entorno lo justifica, contribuye a incrementar la seguridad. Entre ellas las citadas de administración de la seguridad y auditoria de sistemas de información interna.

Existen tres niveles de protección que deben considerarse:

- **El control interno**

Basado en objetivos de control y llevado a cabo por los supervisores a distinto nivel.

- **La auditoria de sistemas de información interna:**

Esta debe ser objetiva e independiente y con una preparación adecuada, como control.

- **La auditoria de sistemas de información externa:**

Debe ser contratada cuando se considera necesaria, y como un nivel de protección más. Igualmente objetiva e independiente.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos, políticas y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren.

a) Elementos Administrativos⁴

Son aquellos que definen el papel administrativo dentro de la seguridad estableciendo sus responsabilidades y formas de participación dentro de la misma. La alta gerencia juega un papel muy importante en el establecimiento de políticas y cuantificación de riesgos.

Entre los elementos administrativos se mencionan los siguientes:

- Análisis de riesgo,
- Análisis de costo beneficio,
- Priorización de los sistemas (en función de su importancia financiera y operacional),
- Cuantificación y cualificación del impacto organizaciones por la suspensión de las actividades operativas,
- Determinación de la confidencialidad de la información.

⁴ José Antonio Echenique, Auditoría en Informática, Mc Graw Hill L.R 90

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

b) Políticas de Seguridad

La política de seguridad es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas de información y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medidas a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento.

Son los directivos, junto con los expertos en tecnologías de la información, quienes deben definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada, con lo que los procesos más importantes recibirán más protección. La seguridad debe considerarse como parte de la operativa habitual, no como un extra añadido.

El objetivo de establecer políticas, procedimientos y prácticas es evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundación, huelgas, disturbios, sabotaje, etc. y continuar en un medio de emergencia hasta que sea restaurado el servicio completo.

Las políticas de seguridad deben contener: Formulación de lineamientos generales, Formulación de lineamientos específicos en el centro de cómputo y en las unidades usuarias. , Manual de seguridad.

Además a la hora de establecer una política es necesario tener en cuenta que:

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

- Toda política de seguridad debe ser holística, es decir, debe cubrir todos los aspectos relacionados con el sistema.
- Debe proteger el sistema en todos los niveles: físico, humano, lógico y logístico.
- Debe tener en cuenta no solo los distintos componentes del sistema, tales como el hardware, software, entorno físico y usuarios, sino también la interacción entre los mismos.
- Debe tener en cuenta el entorno del sistema, es decir el tipo de compañía o entidad con que tratamos (comercial, bancaria, educativa, etc.)
- Debe adecuarse a nuestras necesidades y recursos, el valor que se le da al recurso de la información, el uso que se hace del sistema en todos los departamentos.
- Deben evaluarse los riesgos, el valor del sistema protegido y el coste de atacarlo, y las medidas de seguridad tomadas deben ser proporcionales a estos valores.
- Toda política de seguridad debe basarse fundamentalmente en el sentido común, para lo que es necesario un conocimiento del sistema a proteger y su entorno, además el conocimiento y experiencia en la evaluación de riesgos y el establecimiento de medidas de seguridad, y además un conocimiento de la naturaleza humana, de los usuarios y sus posible motivaciones.

c) Seguridad Lógica y Confidencialidad

La seguridad lógica es el conjunto de normas y medidas que se aplicarán para proteger la información de cualquier avería, transformación o pérdida, ocasionada ya sea por accidente, mal funcionamiento, mal uso de los sistemas o intenciones premeditadas.

Las computadoras son un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta.

Los sistemas de protección informática en cuanto a software se basan en el uso de contraseñas (passwords) secretas. Esas palabras clave, que deben ser obviamente difíciles de decodificar, suelen tener entre seis y ocho caracteres. Si una consta por ejemplo de tres letras y cinco números, el total de combinaciones posibles asciende a 1,757600.000. Pero sucede muy a menudo que los usuarios emplean contraseñas triviales, palabras sencillas o nombres de familiares o amigos, sus propias iniciales o números vinculados a su dirección, teléfono o fecha de nacimiento, fácilmente descubribles. Una investigación de los laboratorios Bell en Estados Unidos indicó que el 86 por ciento de los passwords podía deducirse con un mínimo esfuerzo.

Pero más allá de la complejidad de la clave está el manejo que cada uno le da. La empresa que ofrece servicios también emplea contraseñas, que sólo conocen los miembros del equipo técnico. Según su lugar en la escala jerárquica, manejan cantidad de palabras clave con las que acceden a distintos niveles de poder o permisos en materia de control del sistema, sus programas y archivos. El supervisor dispone de un password con todos los poderes, desde borrar íntegramente los discos hasta leer el correo de

cualquier persona conectada a la red. La principal fractura de seguridad ocurre cuando una persona no autorizada logra apoderarse de los privilegios de un super-usuario.

“Un método eficaz para proteger sistemas de computación es el software de control de acceso”. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes. Sin embargo los paquetes de control de acceso basados en contraseñas pueden ser eludidos por delincuentes sofisticados en computación y no podría depender de esos paquetes por si solos para brindar seguridad adecuada.

TÉCNICAS DE SEGURIDAD LÓGICA

Integridad, significa básicamente que hay que asegurarse de que el sistema sea funcionalmente correcto y este completo.

Aislamiento, en cualquier sistema en el que deba mantenerse un alto nivel de seguridad, ninguna persona o parte de la organización deberá estar en posición de armar todos los componentes o subsistemas para hacer un sistema completo, este aislamiento se conoce también como aislamiento de interfaz. Diversos procedimientos para el aislamiento son:

- Desconexión y separación, se obtiene mediante la distribución geográfica o lógica en el que ciertos elementos del sistema no están conectados.
- Acceso de menos privilegio, el privilegio asignado deberá corresponder ala autoridad de acceso mínimo necesario para realizar el proceso requerido.

- Ubicación de las terminales, en base a la ubicación se les da diferentes clasificaciones y niveles de seguridad, pero si las terminales deben reubicarse también debe cambiarse la autorización.
- Cifrado implica ocultar un mensaje de manera que una persona no autorizada no pueda leerlo.

Identificación, con base al nivel de seguridad requerido, la persona, la terminal, el archivo o el programa, deben identificarse de manera que el derecho de utilizar el sistema pueda verificarse y pueda hacerse responsable al usuario

Verificación de Autenticidad, es la acción que pretende demostrar si algo es válido o genuino, pues alguna persona puede identificarse correctamente y concederse la autoridad para acceder información o realizar alguna actividad. Sin embargo el sistema no puede asegurarse de que el usuario sea válido, especialmente si se identifica con base en lo que tiene y lo que sabe.

Periódicamente en especial para uso de archivos sensibles así como para otros recursos, el usuario deberá ser confirmado.

Monitoreo, es el acto de vigilar, verificar o cuidar algo. Esta actividad reconoce que con el tiempo , ya sea en forma accidental o intencional, los controles serán neutralizados o rotos.

d) Seguridad Física

Es el conjunto de reglas y medidas de seguridad encaminadas a proteger a la organización de cualquier atentado (robo, terrorismo, etc.) manteniendo el control de las

personas que ingresan al local, proteger el equipo, edificio y las instalaciones de cualquier atentado, catástrofe o accidente.

Lo anterior se hace con la finalidad de mantener la operatividad de la organización.

La seguridad física se aplica en los siguientes campos: vigilancia, protección de instalaciones, edificios y equipo.

Una de las técnicas para mantener la seguridad física son los controles de seguridad que ayudan a asegurar normas y desempeño en los sistemas, protegiéndolos contra fallas de hardware, software y humanas.

Los objetivos de los controles de seguridad contra los peligros pueden verse como niveles de controles. Es decir, si falla un nivel, entonces entra en acción otro nivel, y así sucesivamente.

Mecanismos de seguridad física

Control De Acceso Físico

La protección mediante el control de acceso es básica pues si una persona que pretende penetrar ilegalmente no logra obtener acceso a las instalaciones de cómputo, entonces la probabilidad de daño se reduce considerablemente.

Los siguientes aspectos ayudan a controlar el acceso:

- Guardias y escoltas especiales.
- Registro de firma de entrada / firma de salida.
- Gafetes para identificar fácil y rápidamente al personal autorizado y a los visitantes.

- Monitores de circuito cerrado.
- Trituradoras de papel para disponer de los reportes sensibles.
- Puertas de emergencia de una sola vía ya que deben usarse solo para salida en situaciones de emergencia

Ubicación Física

Es una consideración importante en la planeación de la seguridad.

- Ubicación remota, alejado de aeropuertos, equipos eléctricos, tráfico pesado, calderas de vapor, etc.
- Edificio separado; la ventaja de hacer esto es que facilita el control del acceso y reduce los riesgos generales. Si el centro de cómputo no se aloja en un edificio separado, entonces deberá colocarse en el centro del edificio, alejado de paredes exteriores, y no deberá ubicarse ni en el piso superior ni en el piso que da a la calle, a la vista de los transeúntes, ni en el sótano.
- Identificación, el sitio de instalación de computadoras no deberá contener ninguna señal que lo identifique a las personas externas.
- Ubicación de las instalaciones para el respaldo. El respaldo es el elemento clave para la recuperación por lo que debe estar suficientemente alejada de la instalación principal de manera que no este sujeta a los mismos peligros, pero lo suficientemente cerca para proporcionar una pronta recuperación, y su ubicación deberá ser confidencial.

Protección Física

En un plan general de seguridad deben considerarse dispositivos adicionales de protección como los siguientes:

- Bombas y drenajes, que ayuden a reducir los percances como inundaciones, agua en al instalación por tuberías rotas, etc.
- Planta de emergencia
- Control ambiental, deberán instalarse sistemas adecuados de aire acondicionado
- Cubiertas plásticas para el equipo, cuando no esta en uso
- Control de incendios, utilizando extintores adecuados.

En la seguridad física se deben observar las siguientes precauciones:

- Detectores de humo que indiquen la posible presencia de fuego.
- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.
- En cuanto a los extintores, se debe revisar el número de éstos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. (extintores líquidos o que producen gases que podrían perjudicar el equipo)
- Deben existir suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.

- Se debe almacenar adecuadamente como son las cintas magnéticas que, al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

Seguridad en la utilización del equipo

En la actualidad los programas y los equipos son altamente sofisticados y solo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

- 1) Se debe restringir el acceso a los programas y a los archivos
- 2) Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas y los archivos
- 3) Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados
- 4) No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales
- 5) Se deben realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos
- 6) Se deben monitorear periódicamente el uso que se les está dando a las terminales
- 7) Se deben hacer auditorias periódicas sobre el área de operación y la utilización de las terminales

- 8) El usuario es el responsable de los datos por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto solo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema
- 9) Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema
- 10) Debe controlarse la distribución de las salidas, (reportes, cintas, etc.)
- 11) Se debe guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.
- 12) Se debe tener un estricto control sobre el acceso físico de los archivos
- 13) En el caso de programas, se debe asignar a cada uno de ellos una clave que identifique al sistema, subsistema, programa y versión.

También evitará que el programador ponga nombres que no signifiquen nada y que sean difíciles de identificar lo que evitará que el programador utilice la computadora para trabajos personales. Otros de los puntos en los que hay que tener seguridad es en el manejo de información para controlar este tipo de información, se debe:

- 1) Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.
- 2) Solo el personal autorizado debe tener acceso a la información confidencial.
- 3) Controlar los listados tanto de los procesos correctos como aquellos de procesos incorrectos.

- 4) Controlar el número de copias y la destrucción de la información y del papel carbón del reporte muy confidenciales

e) Seguridad en el Personal

Esta implica la protección de la confidencialidad y la confiabilidad del personal y consiste en las medidas que se tomen para evitar la difusión o distribución no autorizadas de los datos así como el uso de equipos sin la debida capacitación y autorización, en otras palabras se refiere al acceso ilegal a información (ya sea en forma física o por infiltración en un sistema en línea) y a los equipos.

Los centros de cómputo dependen en gran medida, de la integridad, estabilidad y lealtad del personal por lo que deben definirse políticas en lo que se refiere a las siguientes actividades:

- Reclutamiento y selección de técnicos, es conveniente hacerle exámenes psicológicos, médicos y tener muy en cuenta sus antecedentes de trabajo antes de contratarlo, además se deben considerar los valores sociales y en general su estabilidad ya que normalmente son personas que trabajan bajo presión y con mucho estrés por lo que importa mucho su actitud y comportamiento.
- Gozo efectivo de vacaciones, en los centros de cómputo es normal que se trabajen horas extras con gran presión y que no haya una adecuada política de vacaciones debido a la dependencia que se tiene con algunas personas, lo cual va haciendo que se crean difíciles de sustituir, así que se

debe verificar la existencia de una adecuada política de vacaciones que nos permita evaluar la dependencia con algunas personas y evitarla.

- Rotación de personal, la adecuada política de reemplazo en caso de renuncia de alguna persona permitirá que en caso de ser necesario pueda cambiarse algún elemento sin arriesgar el funcionamiento de la organización.
- Motivación y satisfacción, también se deberá evaluar la motivación del personal, ya que un empleado motivado, normalmente tiene un alto grado de lealtad y disminuirá la posibilidad de ataques intencionados a la organización.
- Capacitación permanente, un adecuado programa de capacitación disminuye los riesgos por mal uso del equipo.
- Organización y división de responsabilidades, se refiere al establecimiento de límites para las labores normales, esto nos permite reducir el riesgo de fraude por la acción de un elemento que actúe sin autorización.

f) Elementos Técnicos y Procedimientos

Se refiere a la definición por escrito de la información necesaria para garantizar la operación y utilización segura de los equipos

Deben definirse como elementos técnicos y procedimientos: Manuales de usuario, Manuales de procedimiento (encendido, apagado, operación, entre otros), Estándares de análisis, diseño y programación, Manuales de especificaciones funcionales,

Documentación técnica (flujogramas, estructuras, diagramas, programas fuentes, entre otros), Respalos de archivos y programa, Estándares de operación y rendimiento, Revisiones periódicas del cumplimiento de normas sensibles (antivirus, licencias originales, entre otros)

g) Pólizas de Seguros

Los seguros en los equipos se dejan en segundo término aunque son de gran importancia. El problema con al adquisición de seguros es que normalmente el vendedor conoce mucho sobre riesgos comerciales, riesgos de vida, etc. Pero muy poco sobre computadoras y el personal de informática conoce mucho sobre computación pero poco sobre seguros.

Es necesario verificar las fechas de vencimiento de la póliza para evitar tener el seguro adecuado pero inservible porque esta vencido, además debe encontrarse actualizado con los equipos nuevos.

El seguro debe cubrir todo el equipo y su instalación, por lo que es probable que una sola póliza de seguro no pueda cubrir todo el equipo con las diferentes características (existe equipo que pueda ser transportado como computadoras personales y otros que no se pueden mover como unidades de disco duro)por lo que talvez convenga tener dos o más pólizas por separado, cada una con las especificaciones necesarias.

El seguro debe cubrir tanto daños causados por factores externos como internos, también se debe asegurar la perdida de los programas, de la información, de los equipos, y el costo de recuperación de lo anterior. En el caso de los programas se deberá tener en cuenta el costo de elaboración y el costo de crearlos nuevamente y su valor comercial..

En el caso del personal se pueden tener fianzas contra robo , negligencia, daños, sabotaje, acciones deshonestas, etc.

h) Plan de Contingencia

El plan de contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de computo y la información contenida en diversos medios de almacenamiento, además se debe analizar la forma de reducir su ocurrencia y los procedimientos a seguir en caso de que se presentara el problema.

Pese a todas las medidas de seguridad que se adopten puede ocurrir un desastre por tanto es necesario que el plan de contingencias incluya un plan de recuperación de desastres el cual tendrá como objetivo restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles. Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario suponer que el daño ha sido total, con la finalidad de tener un plan de contingencias lo mas completo posible.

El plan de contingencia debe incluir las siguientes actividades: Procedimientos de operación en casos de desastre, especificación de características de instalación alternativa(ambiente físico de los equipos), especificación de características de equipo alternativo (velocidad de procesamiento, capacidad de memoria primaria, capacidad de memoria secundaria, dispositivos de lectura escritura, impresoras, otros periféricos), Especificaciones del software alternativo, Priorización de los sistemas, Lista del personal necesario.

SEGURIDAD AL RESTAURAR EL EQUIPO

Es vital definir los procedimientos en caso de una posible falla o siniestro para asegurar la continuidad de operaciones y el resguardo de la información. Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con la ciencia de la computación, existe un riesgo aceptable, y es necesario analizar y entender estos factores para establecer los procedimientos que permitan analizarlos al máximo y en caso que ocurran, poder reparar el daño y reanudar la operación lo más rápidamente posible.

En una situación ideal se deberían elaborar planes para manejar cualquier contingencia que se presente.

Analizando cada aplicación se deben definir planes de recuperación y reanudación, para asegurarse que los usuarios se vean afectados lo menos posible en caso de fallo o siniestro.

Las acciones de recuperación disponible a nivel operativo pueden ser algunas de las siguientes:

- En algunos casos es conveniente no realizar ninguna acción y reanudar el proceso.
- Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.

- El procesamiento anterior complementado con un registro de las transacciones que afectaron a los archivos permitirá retroceder en los movimientos realizados a un archivo a punto de tener la seguridad del contenido del mismo a partir del reanudar el proceso.
- Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia.
- Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia deberá ser planeado y probado previamente.

Un plan de contingencia o plan de recuperación en caso de desastre es una guía para la restauración rápida y organizada de las operaciones de cómputo después de una suspensión. Especifica quien hace qué y cómo. Los objetivos de dicho plan son los de restablecer, lo más pronto posible, el procesamiento de aplicaciones críticas (aquellas necesarias para la recuperación) para posteriormente restaurar totalmente el procesamiento normal. Un plan de contingencia no duplica un entorno comercial normal (en forma inmediata), pero si minimiza la pérdida potencial de archivos y mantiene a la empresa operando, al tomar acciones decisivas basadas en la planeación anticipada.

UTILIDAD DEL PLAN DE CONTINGENCIA

Un plan de contingencia completo mitigará los efectos de esos desafortunados desastres y permitirá una respuesta rápida, una transferencia del procesamiento crítico a otras instalaciones, y una eventual recuperación.

La preparación de un plan de contingencia da a los directivos de una empresa una excelente oportunidad para aliviar o minimizar problemas potenciales que, en un momento dado, podrían interrumpir el procesamiento de datos. Razón por la cual es menester tomar conciencia de la importancia vital de la confección de dicho plan. Si durante la preparación de un plan de contingencia se identifican y documentan las funciones críticas, se desarrolla un método formal de respuesta a las emergencias, y se llevan a cabo procedimientos de respaldo y recuperación, la continuidad y el bienestar del funcionamiento del centro de cómputo en el futuro mejoraran.

Al considerar los planes de contingencia, se necesita delinear cuidadosamente los distintos tipos de desastre que pueden ocurrir:

- Destrucción completa de los recursos centralizados de procesamiento de datos.
- Destrucción parcial de los recursos centralizados de procesamiento de datos.
- Destrucción o mal funcionamiento de los recursos ambientales destinados al centro de procesamiento de datos.
- Destrucción total o parcial de los recursos descentralizados de procesamiento de datos.

- Destrucción total o parcial de los procedimientos manuales del usuario, utilizados para la captura de la información de entrada para los sistemas de cómputo.
- Pérdida del personal clave
- Interrupción por huelga

ALCANCE DE LA PLANEACION CONTRA DESASTRES

La planeación contra contingencias debe abarcar tanto las aplicaciones en proceso de desarrollo como las operativas. En el caso de las ultimas, existen ciertas áreas que necesitan protección en caso de desastre o ciertos recursos que deben estar disponibles para la recuperación:

- Documentación de los sistemas, la programación y las operaciones.
- Recursos de procesamiento que incluyen:
 - Todo tipo de equipo
 - Ambiente para el equipo
 - Datos y archivos
 - Programas
 - Papelería

Los procedimientos de planificación contra desastres tendrán que definir en forma detallada los arreglos que se hagan para cada caso, la organización y las responsabilidades para aplicarlos y un marco de trabajo para la iniciación y aplicación paso por paso de los procedimientos de recuperación.

i) Auditores Internos y Externos

La seguridad informática requiere del establecimiento de políticas, normas, y procedimientos que aseguren la protección de la información y la importancia del papel de los auditores en ello es que son los especialistas en verificar si la aplicación de los procedimientos es correcta, pero como usualmente no se ven involucrados con aspectos relacionados a la seguridad informática, se hace necesario involucrarlos desde el inicio del establecimiento de un sistema de seguridad para que se familiaricen con el mismo y les sea mas fácil realizar los controles necesarios a futuro.

Las actividades de auditoria incluye: Verificación constante de cumplimiento de políticas, Verificación periódica de las condiciones de seguridad, Evaluación de los riesgos actuales, Recomendaciones, Asesoramiento.

SEGURIDAD EN REDES Y COMUNICACIONES

La idea de que al conectar las computadoras se aumenta el potencial de pérdidas puede parecer un poco pesimista, pero no lo es, la ventaja de la comunicación entre computadoras es que se puede ganar mucho mas por la compartición electrónica de la información y la transferencia de datos, sin embargo, estas ventajas conllevan a un incremento de riesgos, según el principio natural de que “cuanto más se puede ganar mas se puede perder”.

La conexión de dos o más computadoras es un nuevo blanco de ataque, que puede usarse para obtener datos que se transfieran o para penetrar en uno o más de los sistemas interconectados.

La instalación de una red supone combinar una serie de computadoras con un hardware y software adicional. Cierta hardware de red abre nuevos frentes para ataques a la seguridad, mientras que otro puede suponer un incremento en la seguridad. En el nivel más básico, el hardware que se adquiere para crear una red representa una nueva área de pérdida potencial ante robos. Sin embargo, una combinación correcta de hardware de red puede hacer que los datos de una red sean más difíciles de robar o dañar que si estuvieran almacenados en un sistema aislado. Los principales componentes hardware de una red local se pueden agrupar de la siguiente forma:

1. CABLES, que conducen las señales entre las interfaces de red de las computadoras y el resto de la red.

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial como el que se utiliza con la televisión o la fibra óptica. La instalación de los cables de una red local puede ser una tarea muy cara y problemática, pero el valor del cable en si no es tan grande como para convertirse en objetivo de los ladrones, sin embargo el cable instalado representa una inversión significativa que necesita de la protección adecuada. Los cables se deben instalar profesionalmente de forma que se minimice el riesgo de un corte rozadura o daño accidental. Si los datos son como la sangre de la organización, los cables de la red son sus arterias. Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

- a) **Interferencia.** Los datos que viajan a través del cable se alteran por la acción de campos eléctricos. Estos pueden estar generados por cables de alimentación de maquinaria pesada. Los cables metálicos normalmente están

apantallados para evitar dichas interferencias (los cables de fibra óptica no sufren de este problema)

- b) **Corte del cable.** La conexión que establece el cable se rompe, lo que impide que el flujo de datos pase por el cable. Esto puede ocurrir cuando se mueven los equipos o se modifica la estructura que guarda los datos.
- c) **Daños en el cable.** Los daños normales por el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos, o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales, similares a los que se enfrenta una gran parte del material de oficina. Sin embargo, también se pueden ver como un medio de atacar la red si el objetivo es únicamente interferir su funcionamiento. El cable de red ofrece un nuevo frente de ataque para un intruso que intente acceder los datos, con acciones como las siguientes:

- Desviando o estableciendo una conexión no autorizada en la red (un sistema de administración y procedimiento de identificación con clave de acceso adecuados hará difícil que puedan obtener privilegios de usuario en la red, pero los datos que fluyen a través de la red pueden estar en peligro)
- Haciendo escuchas electrónicas sin establecer conexión, los datos se pueden seguir de esta forma, comprometiéndolos.

No hace falta penetrar en los cables físicamente para obtener los datos que se transportan, debido al factor EMI (interferencia electromagnética) el cable de fibra

óptica no emite radiación electromagnética, por lo tanto es inaccesible a la escucha. Sin embargo tanto los cables de fibra óptica como los de cobre pueden sufrir derivaciones. Un cable de fibra óptica que se curva demasiado puede llegar a tener fugas de luz, con pequeñas grietas en su aislante. Aunque es más difícil obtener derivaciones de un cable de fibra que de uno coaxial, es también posible. La moraleja según la *LAN Magazine* es “a la gente que no tiene por qué acceder al cable no se le debe permitir hacerlo”.

2. INTERFACES Y CONECTORES, que sirven de conexión entre el cableado de la red y la circuitería principal de la computadora, o entre los cables y las interfaces o los cables entre si.

A pesar de la creciente aceptación de las redes como un modo de incrementar la productividad de las computadoras personales, la mayoría de los modelos no vienen aun completas con una interfaz de red , lo que significa que para muchas máquinas la interfaz de red es un extra añadido, normalmente como una placa que se instala en la unidad del sistema. Las computadoras macintosh lleva incorporada una interfaz de red “Local Talk” en si, pero si se desea utilizar un tipo de red distinto como Ethernet, se habrá de añadir una interfaz Ethernet. Si la computadora no tiene espacio para una interfaz interna puede agregarse mediante un dispositivo interno como en el caso de las computadoras portátiles.

Desde el punto de vista de la seguridad, las interfaces no representan un gran problema pero las interfaces externas se convierten en otro elemento susceptible de robo, pero pueden fijarse a la mesa muy fácilmente. Las placas de red pueden jugar un papel positivo en la seguridad, al ofrecer una conexión a la red con bloqueo, el uso de la

estación de trabajo de la red se puede controlar independientemente del software de la red o el control de acceso a la estación de trabajo.

3. EXPANSIONES O PERIFÉRICOS, que ofrecen utilidades compartidas como impresión transmisión de facsímiles(fax) y conexión entre redes o a computadoras remotas(sistemas personales o grandes).

Algunos de estos componentes presentan problemas potenciales de seguridad. Por ejemplo varios usuarios de una red pueden compartir una única impresora láser donde muchos usuarios imprimen sus documentos en una impresora que no pueden ver y los documentos impresos constituyen una forma muy vulnerable de datos, no tiene sentido utilizar protección con clave de acceso si los informes van a salir en un punto de impresión en el que las personas que no los deben leer pueden hacerlo.

4. COMPONENTES DE SEGURIDAD, que ofrecen copias de seguridad, redundancia y control de acceso. Para un intruso que busque acceder los datos de la red, la línea de ataque más prometedora será una estación de trabajo por lo que se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella o incluso imprimirla. El administrador de la red debe clasificar los usuarios de red para adjudicarles el nivel de seguridad y estos básicamente son::

- Nivel de administración, aquellos que diseñan, mantienen o ponen en marcha la red.
- Usuarios fiables, aquellos competentes que cumplen las normas y cuyo trabajo se pueda beneficiar de una mayor libertad de acceso a la red.

- Usuarios vulnerables, aquellos que muestran falta de competencia, son excesivamente curiosos, o por alguna razón no se puede confiar

Protección del servidor, la parte más importante de la red es el servidor, la concentración de los datos en términos de cantidad e importancia hace que sea necesario protegerlo de todas las eventualidades.

Las copias de seguridad de un servidor es necesario hacerlas en forma regular y frecuente ya que son un elemento especialmente valioso debiendo quedar guardados en un lugar cerrado, un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro.

Tolerancia a fallos en las redes es la capacidad de continuar funcionando en caso de que se produzca un problema importante o una caída catastrófica, sin daño para los datos y sin que el funcionamiento cambie de una forma perceptible.

No todas las redes necesitan el mismo grado de tolerancia a fallos, ya que esta supone costos adicionales que deben valorarse frente a los requisitos de respuesta en tiempo, es decir evaluar las pérdidas económicas y de prestigio, si la red deja de funcionar y si se pudiese esperar una o dos horas sin tenerla funcionando o bien un tiempo largo. La tolerancia a fallos tiene varios niveles, el más usual es el nivel bajo donde solo se duplica el componente responsable de nueve décimos de los fallos en la red, es decir, el disco fijo del servidor de archivos. Esta es la parte más proclive a fallos porque es la única que tiene partes móviles, estas pueden desgastarse, romperse o sufrir cualquier otro daño. Aparte de un fallo catastrófico por casos fortuitos, los sectores del disco a menudo quedan dañados por el uso normal, quedando dañados los datos escritos en estos

sectores. La tolerancia a fallos entonces se refiere no solo a la redundancia sino a la detección de errores. En el último nivel estará el duplicado de todo hardware e incluso triplicado, para asegurar un rendimiento de la red sin interrupción.

Protección en las comunicaciones

El arma principal para proteger las redes en este campo es una comprensión clara de cómo funciona la comunicación entre computadoras. Entendiendo la tecnología relacionada, se puede ser capaz de detectar los eslabones más débiles de la cadena y tomar las medidas necesarias para reforzarlos.

Cada vez que se pone información en el aire, sea mediante ondas de radio, microondas u ondas de sonido, es posible que alguien pueda acceder a ella. Frente a la conveniencia incuestionable de las ultimas formas de comunicación (enlaces vía satélite entre otros) de voz y datos debe de ponerse la interrogación de una posible interceptación.

Para que las computadoras puedan conversar utilizando líneas telefónicas necesitan módems. Un módem convierte los datos de la computadora en señales que se transmiten a través del teléfono, en el otro extremo de la línea otro módem convierte a la inversa las señales en datos este proceso se conoce como modulación . En esencia un módem es una placa con un circuito electrónico que se puede instalar internamente en una computadora personal o puede estar en una carcasa externa que se conecta a la computadora con un cable.

La mayor parte de sistemas operativos de computadoras personales solo poseen un soporte mínimo para módems por lo que es necesario un software especial, un programa de comunicaciones, para poder controlar el módem.

Es importante hacer hincapié que nadie puede acceder a nuestra computadora a través de un módem a menos que:

- La computadora esté conectada
- El módem esté conectado a la línea telefónica
- El software de comunicaciones esté programado para controlar el teléfono.

La mayor parte de los métodos de ataque utilizados por los piratas y otros intrusos, preparados para realizar exploraciones no autorizadas en computadoras, dependen de la capacidad de violar el sistema de verificación de llamadas de la computadora receptora. A continuación se muestran los pasos seguidos para acceder a una computadora a través del teléfono:

- Localizar la computadora a la que llaman, buscando en información de la empresa, documentos, basura, empleados. Dispositivos de llamada repetitiva pueden llamar a todos los números de un área hasta que conteste una computadora.
- Hacer la llamada y comprobar la respuesta. La petición de un identificador o clave de acceso puede revelar el número de caracteres esperados o incluso el tipo de caracteres (letras o números).
- Ir probando, el pirata no duda en seguir llamando hasta que un intento de conexión cumple los parámetros esperados y descubre la información de conexión necesaria.

A partir de esto es bastante simple proponer una serie de medidas básicas:

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

- Mantenga los números secretos. A menos que se trabaje con un servicio de telefonía pública, trate los números de teléfono de las computadoras como información muy sensible, que se revela según un esquema solo cuando se necesita. Si se requiere comunicación extensiva con mucha gente, utilice un sistema de un tercero, como los servicios de información de MCI Mail o Compuserve. Estos ofrecen un forum correctamente controlado para el intercambio de información sin riesgos, para los sistemas informáticos de la información.
- Limite los intentos de acceso repetidos. no permita más de tres intentos de conexión antes de romper la conexión y obligar a que la persona que llama lo vuelva a intentar de nuevo.
- Revele lo menos posible sobre el procedimiento de conexión, esta es un área en la que no se ha de ser amigable con el usuario, por ejemplo no le pida a la persona que llama “escriba su número de identificación de seis dígitos”, un indicador críptico como «Acceso?:» será suficiente. Si alguien que llama escribe un identificador incorrecto, el mensaje: «Respuesta no válida» hay que evitar mensajes como «lo siento el número de identificación tiene demasiados dígitos». A los usuarios autorizados se les puede enseñar a utilizar el sistema sin las ventajas de estas pistas.

Además puede utilizarse las técnicas de Retrollamado y Claves de acceso temporal, las claves temporales deben modificarse periódicamente y usar combinaciones alfanuméricas difíciles. El retrollamado es una técnica muy potente que se refiere a que

“si las conexiones por llamadas son un medio sensible de interrupción entonces deben evitarse los mas posible”, para ello puede programarse que el computador central llame a determinadas horas ya programadas cuando se trata de la presentación de informes de forma repetitiva. Cuando no se puede evitar la llamada entonces se puede pedir la clave de acceso, cortar y luego rellamar para verificar el origen de la llamada.

Por otro lado la popularización de Internet y la naturaleza de su ambiente informático han inducido a la investigación y desarrollo de tecnologías que garanticen la salvaguarda de los datos que viajan por Internet y las compañías que por su operatividad deben conectar su red a Internet, deben asegurarse de resguardar sus datos, en respuesta a este riesgo surge lo que se conoce como FIREWALLS (paredes de fuego), estos son combinaciones de hardware y software que se construyen utilizando router, servidores y diversos programas. Se localizan en el punto más vulnerable entre la red corporativa e Internet, y pueden ser tan simples o complejas según se requiera. Estos firewalls permiten que cualquier usuario de la red de la compañía accese a Internet, pero impiden que los piratas informáticos (hackers y crackers) y a otros usuarios de Internet obtengan acceso a la misma y causen daños.

Los hackers son el banco de prueba para los sistemas de seguridad. A nivel mundial, es muy común que intrusos que han logrado entrar en sistemas de una empresa terminen siendo contratados por ésta como asesores, porque ellos saben mejor que nadie cómo quebrar las defensas.

La inseguridad de los datos confidenciales que viajan por Internet contribuyó a que ingenieros de software trabajaran en modos de enviar información confidencial de

manera segura. Para ello la información debe codificarse, es decir, alterarse de modo que, para todo el mundo con la excepción del destinatario previsto, tenga un aspecto incomprensible. Así mismo la información debe descodificarse, es decir el receptor y solamente el receptor, ha de convertirla nuevamente en el mensaje original. Se ha creado un gran número de complejos sistemas para permitir este tipo de proceso de codificación y decodificación, que reciben el nombre de **criptosistemas**.

La amenaza de los virus

Un virus es simplemente un programa. Una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco. De todas formas, dentro del término "virus informático" se suelen englobar varios tipos de programas, por lo que a continuación se da un pequeño repaso a cada uno de ellos poniendo de manifiesto sus diferencias. La clasificación es la siguiente:

Virus Puro, un verdadero virus tiene como características más importantes la capacidad de copiarse a sí mismo en soportes diferentes al que se encontraba originalmente, y por supuesto hacerlo con el mayor sigilo posible y de forma transparente al usuario; a este proceso de autorréplica se le conoce como "infección", de ahí que en todo este tema se utilice la terminología propia de la medicina: "vacuna", "tiempo de incubación", etc. Como soporte entendemos el lugar donde el virus se oculta, ya sea fichero, sector de arranque, partición, etc.

Un virus puro también debe modificar el código original del programa o soporte objeto de la infección, para poder activarse durante la ejecución de dicho código; al mismo tiempo, una vez activado, el virus suele quedar residente en memoria para poder infectar así de forma transparente al usuario.

Caballo de Troya, al contrario que el virus puro, un Caballo de Troya es un programa maligno que se oculta en otro programa legítimo, y que produce sus efectos perniciosos al ejecutarse este último. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

Bomba Lógica, se trata simplemente de un programa maligno que permanece oculto en memoria y que solo se activa cuando se produce una acción concreta, predeterminada por su creador: cuando se llega a una fecha en concreto (Viernes 13), cuando se ejecuta cierto programa o cierta combinación de teclas, etc.

Gusano o Worm, por último, un gusano es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la RAM, siendo ésta su única acción maligna.

La barrera entre virus puros y el resto de programas malignos es muy difusa, prácticamente invisible, puesto que ya casi todos los virus incorporan características propias de uno o de varios de estos programas: por ejemplo, los virus como el Viernes 13 son capaces de infectar otros archivos, siendo así virus puro, pero también realizan su efecto destructivo cuando se da una condición concreta, la fecha Viernes 13,

característica propia de una bomba lógica; por último, se oculta en programas ejecutables teniendo así una cualidad de Caballo de Troya. De ahí la gran confusión existente a este respecto.

Formas De Infección

Antes de nada, hay que recordar que un virus no puede ejecutarse por si solo, necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse a un programa portador necesita modificar la estructura de este, para que durante su ejecución pueda realizar una llamada al código del virus.

Las partes del sistema más susceptibles de ser infectadas son el sector de arranque de los disquetes, la tabla de partición y el sector de arranque del disco duro, y los ficheros ejecutables (*.EXE y *.COM). Para cada una de estas partes tenemos un tipo de virus, aunque muchos son capaces de infectar por sí solos estos tres componentes del sistema. En los disquetes, el sector de arranque es una zona situada al principio del disco, que contiene datos relativos a la estructura del mismo y un pequeño programa, que se ejecuta cada vez que arrancamos desde disquete. En este caso, al arrancar con un disco contaminado, el virus se queda residente en memoria RAM, y a partir de ahí, infectara el sector de arranque de todos los disquetes a los que se accedan, ya sea al formatear o al hacer un DIR en el disco, dependiendo de cómo esté programado el virus).

El proceso de infección consiste en sustituir el código de arranque original del disco por una versión propia del virus, guardando el original en otra parte del disco; a menudo el virus marca los sectores donde guarda el *boot* original como en mal estado,

protegiéndolos así de posibles accesos, esto suele hacerse por dos motivos: primero, muchos virus no crean una rutina propia de arranque, por lo que una vez residentes en memoria, efectúan una llamada al código de arranque original, para iniciar el sistema y así aparentar que se ha iniciado el sistema como siempre, con normalidad. Segundo, este procedimiento puede ser usado como técnica de ocultamiento.

Normalmente un virus completo no cabe en los 512 bytes que ocupa el sector de arranque, por lo que en éste suele copiar una pequeña parte de si mismo, y el resto lo guarda en otros sectores del disco, normalmente los últimos, marcándolos como defectuosos. Sin embargo, puede ocurrir que alguno de los virus no marquen estas zonas, por lo que al llenar el disco estos sectores pueden ser sobrescritos y así dejar de funcionar el virus.

La tabla de partición está situada en el primer sector del disco duro, y contiene una serie de bytes de información de cómo se divide el disco y un pequeño programa de arranque del sistema. Al igual que ocurre con el *boot* de los disquetes, un virus de partición suplanta el código de arranque original por el suyo propio; así, al arrancar desde disco duro, el virus se instala en memoria para efectuar sus acciones. También en este caso el virus guarda la tabla de partición original en otra parte del disco, aunque algunos la marcan como defectuosa y otros no. Muchos virus guardan la tabla de partición y a ellos mismos en los últimos sectores de disco, y para proteger esta zona, modifican el contenido de la tabla para reducir el tamaño lógico del disco. De esta forma el DOS no tiene acceso a estos datos, puesto que ni siquiera sabe que esta zona existe.

Casi todos los virus que afectan la partición también son capaces de hacerlo en el *boot* de los disquetes y en los ficheros ejecutables; un virus que actuara sobre particiones de disco duro tendría un campo de trabajo limitado, por lo que suelen combinar sus habilidades.

Con todo, el tipo de virus que más abunda es el de fichero; en este caso usan como vehículo de expansión los archivos de programa o ejecutables, sobre todo .EXE y .COM, aunque también a veces .OVL, .BIN y .OVR. AL ejecutarse un programa infectado, el virus se instala residente en memoria, y a partir de ahí permanece al acecho; al ejecutar otros programas, comprueba si ya se encuentran infectados. Si no es así, se adhiere al archivo ejecutable, añadiendo su código al principio y al final de éste, y modificando su estructura de forma que al ejecutarse dicho programa primero llame al código del virus devolviendo después el control al programa portador y permitiendo su ejecución normal.

Este efecto de adherirse al fichero original se conoce vulgarmente como "engordar" el archivo, ya que éste aumenta de tamaño al tener que albergar en su interior al virus, siendo esta circunstancia muy útil para su detección. De ahí que la inmensa mayoría de los virus sean programados en lenguaje ensamblador, por ser el que genera el código más compacto, veloz y de menor consumo de memoria; un virus no sería efectivo si fuera fácilmente detectable por su excesiva ocupación en memoria, su lentitud de trabajo o por un aumento exagerado en el tamaño de los archivos infectados. No todos los virus de fichero quedan residentes en memoria, si no que al ejecutarse es portador, éstos infectan a otro archivo, elegido de forma aleatoria de ese directorio o de otros.

Efectos Destructivos De Los Virus

Los efectos perniciosos que causan los virus son variados; entre éstos se encuentran el formateo completo del disco duro, eliminación de la tabla de partición, eliminación de archivos, ralentización del sistema hasta límites exagerados, enlaces de archivos destruidos, archivos de datos y de programas corruptos, mensajes o efectos extraños en la pantalla, emisión de música o sonidos.

Formas De Ocultamiento

Un virus puede considerarse efectivo si, además de extenderse lo más ampliamente posible, es capaz de permanecer oculto al usuario el mayor tiempo posible; para ello se han desarrollado varias técnicas de ocultamiento o sigilo. Para que estas técnicas sean efectivas, el virus debe estar residente en memoria, puesto que debe monitorizar el funcionamiento del sistema operativo. La base principal del funcionamiento de los virus y de las técnicas de ocultamiento, además de la condición de programas residentes, la intercepción de interrupciones. El DOS y los programas de aplicación se comunican entre sí mediante el servicio de interrupciones, que son como subrutinas del sistema operativo que proporcionan una gran variedad de funciones a los programas. Las interrupciones se utilizan, por ejemplo, para leer o escribir sectores en el disco, abrir ficheros, fijar la hora del sistema, etc. Y es aquí donde el virus entra en acción, ya que puede sustituir alguna interrupción del DOS por una suya propia y así, cuando un programa solicite un servicio de esa interrupción, recibirá el resultado que el virus determine.

Prevención, detección y eliminación

Una buena política de prevención y detección nos puede ahorrar sustos y desgracias. Las medidas de prevención pasan por el control, en todo momento, del software ya introducido o que se va a introducir en nuestro ordenador, comprobando la fiabilidad de su fuente. Esto implica la actitud de no aceptar software no original, ya que el pirateo es una de las principales fuentes de contagio de un virus, siendo también una práctica ilegal y que hace mucho daño a la industria del software.

Por supuesto, el sistema operativo, que a fin de cuentas es el elemento software más importante del ordenador, debe ser totalmente fiable; si éste se encuentra infectado, cualquier programa que ejecutemos resultará también contaminado. Por eso, es imprescindible contar con una copia en disquetes del sistema operativo, protegidos éstos contra escritura; esto último es muy importante, no solo con el S.O. sino con el resto de disquetes que poseamos. Es muy aconsejable mantenerlos siempre protegidos, ya que un virus no puede escribir en un disco protegido de esta forma. Por último es también imprescindible poseer un buen software antivirus, que detecte y elimine cualquier tipo de intrusión en el sistema.

Ante la infección del sector de arranque (boot sector) Windows 95 reacciona sorprendentemente bien, o al menos mucho mejor que sus antecesores. De hecho, frente a cualquier modificación del sector de arranque el sistema presenta un mensaje durante la inicialización. Nos anuncia que algo se ha cambiado y que la causa de tal hecho puede ser un virus de *boot*, aunque no necesariamente.

También debemos precisar que si hay un error remotizado en la tabla de particiones el sistema nos da el mismo aviso que en el caso anterior, lo que sin duda puede ser motivo de confusión. En general siempre que Windows 95 se dé cuenta de un fallo en el sistema de ficheros que le impida trabajar con la VFAT a pleno rendimiento, se inicia con el «Sistema de archivos en modo compatibilidad MS-DOS», sugiriendo como posible causa el ataque de un virus.

Software Antivirus

Para combatir la avalancha de virus informáticos se creó el software antivirus. Estos programas suelen incorporar mecanismos para prevenir, detectar y eliminar virus. Para la prevención se suelen usar programas residentes que alertan al usuario en todo momento de cualquier acceso no autorizado o sospechoso a memoria o a disco, por lo que resultan sumamente útiles al impedir la entrada del virus y hacerlo en el momento en que este intenta la infección, facilitándonos enormemente la localización del programa maligno. Sin embargo presentan ciertas desventajas, ya que al ser residentes consumen memoria RAM, y pueden también resultar incompatibles con algunas aplicaciones. Por otro lado, pueden llegar a resultar bastante molestos, puesto que por lo general suelen interrumpir nuestro trabajo habitual con el ordenador avisándonos de intentos de acceso a memoria o a disco que en muchos casos provienen de programas legítimos. A pesar de todo, son una medida de protección excelente y a ningún usuario debería faltarle un programa de este tipo.

A la hora de localizar virus, los programas usados sin los detectores o scanners, normalmente estos programas chequean primero la memoria RAM, después las zonas críticas del disco como el *boot* o partición, y por ultimo los ficheros almacenados en el.

Los productos antivirus han mejorado considerablemente sus algoritmos de búsqueda, aunque en la actualidad la exploración de cadenas sigue siendo la técnica más empleada. Pero el aumento imparable del número de virus y las técnicas de camuflaje y automodificación que suelen emplear hacen que la búsqueda a través de una cadena genérica sea una tarea cada vez más difícil. Por ello, cada día es más frecuente el lanzamiento de antivirus con técnicas heurísticas.

La detección heurística es una de las fórmulas más avanzadas de remotoización de virus. La búsqueda de virus mediante esta técnica se basa en el desensamblado del código del programa que se intenta analizar con el objetivo de encontrar instrucciones (o un conjunto de ellas) sospechosas. Sin duda, lo mejor es disponer de un antivirus que combine la búsqueda de cadenas características y además cuente con técnicas heurísticas.

Gracias a la heurística se buscan programas que puedan quedarse residentes o que sean capaces de capturar aplicaciones que se estén ejecutando, código preparado para mover o sobrescribir un programa en memoria, código capaz de automodificar ejecutables, rutinas de encriptación y desencriptación, y otras actividades propias de los virus.

Aunque las técnicas heurísticas han representado un gran avance en la detección de virus desconocidos, presentan un gran inconveniente: es muy alta la posibilidad de obtener

«falsos positivos y negativos». Se produce un «falso positivo» cuando el antivirus anuncia la presencia de un virus que no es tal, mientras que se llama «falso negativo» cuando piensa que el PC está limpio y en realidad se encuentra infectado.

2.1.3.3 MANUALES⁵

Concepto de manual

Es un cuerpo sistemático que indica las actividades a ser cumplidas por los miembros de una organización y la forma en que las mismas deben ser realizadas. **Henry Fayol**

"Un folleto, libro, carpeta, etc., en los que de una manera fácil de manejar (manuable) se concentran en forma sistemática, una serie de elementos administrativos para un fin concreto: orientar y uniformar la conducta que se presenta entre cada grupo humano en la empresa". **A. Reyes Ponce.**

"El manual presenta sistemas y técnicas específicas. Señala el procedimiento a seguir para lograr el trabajo de todo el personal de oficina o de cualquier otro grupo de trabajo que desempeña responsabilidades específicas. Un procedimiento por escrito significa establecer debidamente un método estándar para ejecutar algún trabajo". **Graham Kellog.**

⁵ <http://www.itlp.edu.mx/publica/tutoriales/rechuml/u3parte1.htm>

"Es un registro escrito de información e instrucciones que conciernen al empleado y pueden ser utilizados para orientar los esfuerzos de un empleado en una empresa".

Terry G. R.

"Una expresión formal de todas las informaciones e instrucciones necesarias para operar en un determinado sector; es una guía que permite encaminar en la dirección adecuada los esfuerzos del personal operativo". **Continolo G.**

El manual como medio de comunicación

La tarea de elaborar manuales administrativos se considera como una función de mantener informado al personal clave de los deseos y cambios en las actitudes de la dirección superior, al delinear la estructura organizacional y poner las políticas y procedimientos en forma escrita y permanente. Un manual correctamente redactado puede ser un valioso instrumento administrativo.

En esencia, los manuales administrativos representan un medio de comunicación de las decisiones administrativas, y por ello, que tiene como propósito señalar en forma sistemática la información administrativa.

Importancia de los Manuales

Entre las herramientas desarrolladas para ayudar en el logro de una efectiva sistematización tanto en la aplicación teórica como en la fase operativa, una de las más

importantes son los manuales, porque ofrecen un cúmulo de información que permite una correcta orientación a los empleados de las empresas.

Objetivos de los Manuales

De acuerdo con la clasificación y grado de detalle, los manuales administrativos permiten cumplir con los siguientes objetivos:

- a) Instruir al personal, acerca de aspectos tales como: objetivos, funciones, relaciones, políticas, procedimientos, normas, etc.
- b) Precisar las funciones y relaciones de cada unidad administrativa para deslindar responsabilidades, evitar duplicidad y detectar omisiones.
- c) Coadyuvar a la ejecución correcta de las labores asignadas al personal, y propiciar la uniformidad en el trabajo.
- d) Servir como medio de integración y orientación al personal de nuevo ingreso, facilitando su incorporación a las distintas funciones operacionales.
- e) Proporcionar información básica para la planeación e implementación de reformas administrativas.

Posibilidades y limitaciones de los manuales administrativos.

Los manuales administrativos ofrecen una serie de posibilidades que nos reflejan la importancia de estos. Sin embargo, tienen ciertas limitaciones, lo cual de ninguna manera le restan importancia.

Posibilidades.

- a) Es una fuente permanente de información sobre el trabajo a ejecutar.
- b) Ayudan a institucionalizar y hacer efectivo los objetivos, las políticas, los procedimientos, las funciones, las normas, etc.
- c) Evitan discusiones y mal entendidos, de las operaciones.
- d) Aseguran continuidad y coherencia en los procedimientos y normas a través del tiempo.
- e) Son instrumentos útiles en la capacitación del personal.
- f) Incrementan la coordinación en la realización del trabajo.
- g) Posibilitan una delegación efectiva, ya que al existir instrucciones escritas, el seguimiento del supervisor se puede circunscribir al control por excepción.

Limitaciones.

- a) Su deficiente elaboración provoca serios inconvenientes en el desarrollo de las operaciones.
- b) El costo de producción y actualización puede ser alto.
- c) Si no se actualiza periódicamente, pierde efectividad.
- d) Incluye solo aspectos formales de la organización, dejando de lado los informales, cuya vigencia e importancia son notorias para la misma.
- e) Muy sintética carece de utilidad: muy detallada los convierte en complicados.

Tipos de Manuales:

Los diferentes organismos (públicos o privados) tienen necesidad de manuales diferentes. El tipo de manual se determina dando respuesta al propósito que se han de lograr. En ciertos casos, sólo sirve a un objetivo: y en otros, se logran varios objetivos.

- Por su alcance

El alcance está referido al ámbito de aplicación, por lo que se dividen en:

Generales o de aplicación universal.

Se refiere a todo el organismo en su conjunto, dentro de este tenemos los siguientes:

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Manuales generales de organización.- Éste es producto de la planeación organizacional y abarca todo el organismo, indicando la organización formal y definiendo su estructura funcional.

Manual general de procedimientos.- Éste es también resultado de la planeación, contiene los procedimientos de todas las unidades orgánicas que conforman en un organismo social, a fin de uniformar la forma de operar.

Manual general de políticas.- Se refiere a presentar por escrito los deseos y actitud de la dirección superior; para toda la empresa, estas políticas generales establecen líneas de guía, un marco dentro del cual todo el personal puede actuar de acuerdo a condiciones generales.

Departamentales o de aplicación específica.

Se refiere a una parte de un área específica, entre ellos tenemos:

- **Manual específico de reclutamiento y selección.-** Se refiere a una parte de una área específica (personal) y contiene la definición uniforme respecto al reclutamiento y selección personal en una organización.
- **Manual específico de auditoria interna.-** Consiste en agrupar lineamientos, instrucciones de aplicación específica a determinados tipos de actividad, aquí se refiere a la auditoria interna en forma particular.

- **Manual específico de políticas de personal.-** Éste se enfoca a definir "políticas", pero de una área específica de la organización, señalando las guías u orientación respecto a cuestiones de personal, tales como: contratación, permisos, promociones, prestaciones, etc.
- **Manual específico de procedimientos de tesorería.-** Consiste en elaborar los procedimientos en el orden de importancia de una área específica, a fin de capitalizar las oportunidades naturales de secuencia de pasos en el trabajo, por ejemplo: ingreso a caja, pago a proveedores, etc.

De puestos o de aplicación individual

Puede referirse a tareas y trabajos individuales, ejemplo. Como operar una máquina.

- **Por su Contenido.**

Se refiere al contenido del manual para cubrir una variedad de materias, dentro de este tipo tenemos los siguientes:

Manual de historia.- Su propósito es proporcionar información histórica sobre el organismo: sus comienzos, crecimiento, logros, administración y posición actual. Esto le da al empleado un panorama introspectivo de la tradición y filosofía del organismo. Bien elaborado y aplicado contribuye a una mejor comprensión y motiva al personal a sentir que pertenece y forma parte de la organización.

Manual de organización.- Su propósito es exponer en forma detallada la estructura organizacional formal a través de la descripción de los objetivos, funciones, autoridad y responsabilidad de los distintos puestos, y las relaciones.

Manual de políticas.- Consiste en una descripción detallada de los lineamientos a ser seguidos en la toma de decisiones para el logro de los objetivos. El conocer de una organización proporciona el marco principal sobre el cual se basan todas las acciones.

Una adecuada definición de políticas y su establecimiento por escrito, permite:

- a) Agilizar el proceso de toma de decisiones
- b) Facilitar la descentralización, al suministrar lineamientos a niveles intermedios.
- c) Servir de base para una constante y efectiva revisión.

Puede elaborarse manuales de políticas para funciones operacionales tales como: producción, ventas, finanzas, personal, compras, etc.

Manual de procedimientos.- Es la expresión analítica de los procedimientos administrativos a través de los cuales se canaliza la actividad operativa del organismo. Este manual es una guía (como hacer las cosas) de trabajo al personal y es muy valiosa para orientar al personal de nuevo ingreso. La implementación de este manual sirve para aumentar la certeza de que el personal utiliza los sistemas y procedimientos administrativos prescritos al realizar su trabajo.

Manual de contenido múltiple.- Cuando el volumen de actividades, de personal o simplicidad de la estructura organizacional, no justifique la elaboración y utilización de distintos manuales, puede ser conveniente la confección de este tipo de manuales. Un ejemplo de este manual es el de "políticas y procedimientos", el de "historia y organización", en sí consiste en combinar dos o más categorías que se interrelacionan en la práctica administrativa. En organismos pequeños, un manual de este tipo puede combinar dos o más conceptos, debiéndose separar en secciones.

- **Por su función específica o área de actividad.**

Esta clasificación se refiere a una función operacional específica a tratar. Dentro de este apartado puede haber los siguientes manuales:

Manual de producción.- Consiste en abarcar la necesidad de interpretar las instrucciones sobre la base de los problemas cotidianos tendientes a lograr su mejor y pronta solución.

La necesidad de coordinar el proceso de fabricación (fabricación, inspección, ingeniería industrial, control de producción), es tan reconocida, que en las operaciones de fabricación, los manuales se aceptan y usan ampliamente.

Manual de compras.- El proceso de comprar debe estar por escrito; consiste en definir el alcance de compras, definir la función de comprar, los métodos a utilizar que afectan sus actividades.

Manual de ventas.- Consiste en señalar los aspectos esenciales del trabajo y las rutinas de información comprendidas en el trabajo de ventas (políticas de ventas, procedimientos, controles, etc.) Al personal de ventas es necesario darle un marco de referencia para tomar decisiones cotidianas.

Manual de finanzas.- Consiste en asentar por escrito las responsabilidades financieras en todos los niveles de la administración, contiene numerosas instrucciones específicas a quienes en la organización están involucrados con el manejo de dinero, protección de bienes y suministro de información financiera.

Manual de contabilidad.- Trata acerca de los principios y técnicas de la contabilidad. Se elabora como fuente de referencia para todo el personal interesado en esta actividad. Este manual puede contener aspectos tales como: estructura orgánica del departamento, descripción del sistema contable, operaciones internas del personal, manejo de registro, control de la elaboración de información financiera.

Manual de crédito y cobranzas.- Se refiere a la determinación por escrito de procedimientos y normas de esta actividad. Entre los aspectos más importantes que puede contener este tipo de manual están los siguientes: operaciones de crédito y cobranzas, control y cobro de las operaciones, entre otros.

Manual de personal.- Abarca una serie de consideraciones para ayudar a comunicar las actividades y políticas de la dirección superior en lo que se refiere a personal. Los manuales de personal podrán contener aspectos como: reclutamiento y selección, administración de personal, lineamientos para el manejo de conflictos personales, políticas de personal, uso de servicios, prestaciones, capacitación, entre otros.

Manual técnico.- Trata acerca de los principios y técnicas de una función operacional determinada. Se elabora como fuente básica de referencia para la unidad administrativa responsable de la actividad y como información general para el personal interesado en esa función. Ejemplos de este tipo de "Manual técnico de auditoria administrativa", y el "Manual técnico de sistemas y procedimientos". Estos sirven como fuente de referencia y ayudan a computar a los nuevos miembros del personal de asesoría.

Manual de adiestramiento o instructivo.- Estos manuales explican, las labores, los procesos y las rutinas de un puesto en particular, son comúnmente mas detallados que un manual de procedimientos.

El supuesto en el que se basa este tipo de manual es que el usuario tiene muy poco conocimiento previo de los temas cubiertos. Por ejemplo, un manual de adiestramiento "explica como debe ejecutarse el encendido de la terminal de la computadora y emitir su señal", mientras que un manual de procedimientos omitir esta instrucción y comenzaría con el primer paso activo del proceso. El manual de adiestramiento también utiliza

técnicas programadas de aprendizaje o cuestionarios de auto evaluación para comprobar el nivel de comprensión del contenido por el usuario.

Otra clasificación aceptada de los manuales administrativos se refiere a las necesidades que tienen las oficinas y de acuerdo a su ámbito de aplicación; pueden elaborarse manuales con una cobertura mayor o menor.

Manual de Seguridad Informática.- Se refiere a la determinación por escrito de procedimientos, normas políticas, disposiciones y acciones a seguir, para la seguridad en informática, cuyo objetivo es proteger los recursos con que cuenta esta área.

2.2. TEORÍA ADOPTADA

2.2.1 INSTITUCIONES OFICIALES AUTÓNOMAS

Se entenderá por instituciones oficiales autónomas las que funcionan dentro del campo de la administración pública y que fueron creadas por decreto de ley (Art. 121 y 122 de la constitución política de El Salvador de 1950, o el Art. 225 de la constitución actualizada en 1983). Estas pueden ser de dos tipos:

- Instituciones oficiales autónomas, financieramente autónomas respecto del gobierno central.
- Instituciones oficiales autónomas subvencionadas.

Para efectos de la investigación se entenderá por instituciones oficiales autónomas subvencionadas únicamente aquellas que funcionan dentro del campo de la administración pública, que han sido creadas por mandato constitucional y que

continuamente reciben aportes del estado, siendo así financieramente dependientes aunque en lo administrativo son autónomas.

2.2.2 INFORMACIÓN COMPUTARIZADA

Se entenderá por información computarizada toda aquella información que resulte como producto del procesamiento electrónico de datos, es decir toda información que se encuentre apoyada en elementos de Hardware, software, y recurso humano especializado, pues dichos elementos son los que hacen posible el procesamiento electrónico de datos.

2.2.3 ÁREAS QUE SE CONSIDERAN ESENCIALES EN LA PROTECCIÓN DE LA INFORMACIÓN COMPUTARIZADA

En lo referido a la seguridad de la información computarizada se considera importante incluir los aportes de diferentes fuentes como el autor José Antonio Echenique y Stephem Cobb, para lograr una combinación que abarque todos los aspectos posibles que deben considerarse para garantizar la protección de la información. En este sentido a continuación se definen las áreas que se consideran esenciales para la protección de la información:

- 1) Seguridad Física,** donde se considerará todas aquellas medidas cuyo objetivo es proteger el equipo (computadoras, impresores, UPS), de una manera preventiva y correctiva incluyendo para ello procedimientos de operación.
- 2) Seguridad Lógica y Confidencial,** donde se consideran todos los elementos de

seguridad cuyo objetivo es proteger el software, dejando fuera las evaluaciones del funcionamiento de programas, es decir que no se considera dentro de la seguridad en software investigar si un programa produce los resultados correctos, así mismo la seguridad propia de los sistemas operativos de redes, solamente serán abordados en aspectos generales, ya que las acciones específicas las proporciona cada fabricante en el momento de la adquisición de licencia. Dentro de esta área se considera necesario incluir los elementos de seguridad siguientes: Antivirus, respaldos, licencias de software, garantías de proveedores, controles de acceso lógicos, procedimientos de operación, seguros, entre otros.

3) Seguridad en el personal, en este apartado se consideran todas aquellas medidas necesarias para que el personal que opera el software y el hardware del área informática o que se vea involucrado en el manejo de la información computarizada lo haga de una manera segura, que no pueda dañar la información; así como definir un plan de contingencia que les indique que hacer en caso de desastre.

4) Elementos Técnicos, en esta área se definirán todos aquellos aspectos que se refieran a garantizar la operación y utilización segura de los equipos e información que estos almacenan tales como: respaldos, antivirus, adquisición de software, uso de licencias, garantías con proveedores, entre otros.

5) Área administrativa, este apartado debe comprender las responsabilidades de los mandos administrativos, cuya participación es importante principalmente para: el establecimiento de políticas, el análisis de riesgos, la priorización de información, definición de áreas vulnerables, la cuantificación de los riesgos y la contratación

efectiva de seguros.

6) Área de Auditoria, el cual debe considerarse como el establecimiento de responsabilidades específicas y formas de participación dentro de lo que es la seguridad de la información computarizada.

7) Plan de Contingencia, por la importancia de tener una alternativa de operación en caso de emergencia, y el trabajo que involucra la elaboración de un plan de contingencia, se considera un apartado separado de las otras áreas, el cual debe contener el planneamiento de acciones específicas a seguir en evento que no esté considerado en el proceso de planeación normal incluyendo directrices para la recuperación en caso de desastres y la restauración del servidor de computo.

2.2.4 TIPO DE MANUAL QUE SE OFRECERA

El concepto de manual que se considera más apropiado es el presentado por el autor Graham Kellog el cual dice:

“Un manual presenta sistemas y técnicas específicas. Señala el procedimiento a seguir para lograr el trabajo de todo el personal de oficina o de cualquier otro grupo de trabajo que desempeña responsabilidades específicas. Un procedimiento por escrito significa establecer debidamente un método estándar para ejecutar algún trabajo”.

El tipo de manual que se ofrecerá se define así:

Manual de seguridad Informática, se refiere a la determinación por escrito de procedimientos, normas, políticas, disposiciones y acciones a seguir por el área de informática, cuyo objetivo es proteger un recurso tan valioso como lo es la información computarizada con que cuenta una institución.

El manual de seguridad informática es de aplicación específica porque no tiene un alcance en toda la empresa, además tiene un contenido múltiple por referirse a una combinación de categorías que se interrelacionan en la práctica administrativa. La combinación de categorías se refiere a que teóricamente existen manuales solo de organización o solo de políticas o de procedimientos entre otros, sin embargo el tipo de manual que se considerara en este estudio posee varias categorías integradas, entre ellas políticas, normas y procedimientos entre otros.

CAPÍTULO III

INVESTIGACIÓN DE CAMPO REALIZADA EN LAS INSTITUCIONES OFICIALES AUTÓNOMAS SUBVENCIONADAS

El objeto de la investigación de campo esta orientado a identificar la necesidad de contar con un manual de seguridad informática para la información computarizada de las instituciones en estudio. Por lo tanto era de suma importancia fijar los objetivos de investigación para establecer lo que se quería investigar y lograr obtener información pertinente para elaborar un manual de seguridad de la información computarizada acorde a las necesidades y requerimientos propios de las Instituciones Oficiales Autónomas Subvencionadas del Órgano Ejecutivo.

3.1 OBJETIVOS DE LA INVESTIGACIÓN DE CAMPO

Los objetivos se dividieron de la forma siguiente:

3.1.1. Objetivo General

Obtener información sobre las condiciones y características de seguridad en las unidades de informática de las Instituciones Oficiales Autónomas, que permita la elaboración de un manual de seguridad informática para la información computarizada de las mismas.

3.1.2. Objetivos Específicos

- Hacer un diagnóstico sobre los elementos de seguridad que actualmente tienen las instituciones investigadas.
- Identificar las necesidades en materia de seguridad informática, que puedan ser resueltas mediante normas, políticas o procedimientos de seguridad.

- Recolectar información que permita identificar los elementos que debe contener el manual de seguridad de las Instituciones Oficiales Autónomas Subvencionadas
- Obtener información que permita establecer conclusiones y recomendaciones que coadyuven al objetivo de proporcionar seguridad a la información computarizada de las instituciones investigadas.

3.2. METODOLOGÍA DE LA INVESTIGACIÓN

La investigación se desarrolló de acuerdo a los parámetros siguientes:

3.2.1. Método

Para realizar la investigación se utilizó el método: no experimental transaccional descriptivo⁶, debido a que la investigación se llevaría a cabo sin manipular ni hacer variar los fenómenos observados, los cuales fueron descritos tal y como se dan en un contexto natural. Además se realizó en un tiempo único

3.2.2. Fuentes de Investigación

Las fuentes de investigación primarias fueron las unidades de informática de las instituciones investigadas, mientras que las fuentes secundarias fueron todos los libros, revistas y folletos relacionados con el tema de la seguridad informática, así como todos los sitios web de internet consultados.

3.2.3. Determinación del Universo

La investigación fue establecida para las Instituciones Oficiales Autónomas y dentro de éstas las de tipo subvencionadas, por tanto el universo está constituido por la totalidad de

⁶ Según Metodología de la Investigación, Roberto H. Sampieri, Carlos Fernández y Pilar Baptista

las mismas y que pertenecen al municipio de San Salvador que forman un total de 27 instituciones (ver anexo 1).

Dentro de cada institución los sujetos de investigación fueron los jefes de informática y técnicos. Los jefes de informática son los encargados de la administración del área de informática, con estudios especializados en el área de informática o con conocimientos en informática obtenidos a través de la experiencia (forma empírica) los técnicos son usualmente programadores, o analistas programadores, para los que se requiere tener estudios técnicos en herramientas de desarrollo.

3.2.4 Determinación de la muestra

La muestra se determinó de una forma no probabilística, ya que para realizar la investigación no se necesitaba representatividad de elementos del universo, sino más bien una cuidadosa y controlada elección de unidades de análisis con ciertas características específicas, conocida como muestra de sujetos-tipo⁷.

3.2.4.1 Procedimiento de selección de muestra

a) Se pretendió realizar la investigación con todo el universo, pero en algunas instituciones, no se tuvo acceso, por lo tanto, se realizó una investigación preliminar, mediante un cuestionario (ver anexo 2) enfocado a recolectar las características técnicas comunes dentro de las instituciones sujetas de estudio, las cuales permitirían obtener una muestra basada en características compartidas por las Instituciones Oficiales Autónomas.

⁷ Según Metodología de la Investigación, Roberto H. Sampieri, Carlos Fernández y Pilar Baptista

- b) Las instituciones que permitieron el acceso fueron un total de 14, en ellas se pasó la encuesta preliminar.
- c) Al procesar los resultados de la encuesta preliminar se obtuvieron los siguientes elementos comunes que se convirtieron en criterios de selección:
- Existencia de una red diferente a la red SAFI. Es necesario aclarar que todas las Instituciones Oficiales Autónomas Subvencionadas cuentan con la red SAFI⁸ la cual ya tiene establecida sus políticas y procedimientos para su protección.
 - Arquitectura de tipo Cliente-Servidor
 - Utilización del sistema operativo NT Server, para los servidores y Windows para las estaciones de trabajo.
- d) Cuando se estableció el planteamiento de la investigación se dejó como interés primordial la protección de la información computarizada, por tanto la existencia de un sistema de información computarizado se determinó como otro criterio de selección.
- e) Luego de la aplicación de todos los criterios de selección la muestra quedó constituida por un total de 10 instituciones.
- UES: Universidad Nacional de El Salvador
 - INSAFORP: Instituto Salvadoreño de Formación Profesional
 - FIS: Fondo de Inversión Social
 - INPEP: Instituto Nacional de Pensiones Públicas

⁸ SAFI: Sistema Administrativo Financiero

- CNJ: Consejo Nacional de la Judicatura
- CRS: Cruz Roja Salvadoreña
- CSSP: Consejo Superior de Salud Pública
- UTE: Unidad Técnica Ejecutiva
- FOSOFAMILIA: Fondo Solidario para la Familia Microempresaria
- ISPM: Instituto Salvadoreño de Protección al Menor

f) Con el objeto de explicar ampliamente a las 10 instituciones seleccionadas el proceso de recolección de datos, y con el objetivo de obtener autorización de alguna de ellas, para utilizarla como caso práctico (al momento de elaborar la propuesta), se realizó una visita a cada una de las instituciones en mención. Todas quedaron enteradas del proceso de recolección de los datos, pero ninguna accedió a servir como caso práctico, entre las razones que expusieron para no servir como caso practico están:

- Cuatro instituciones expresaron estar trabajando un proyecto urgente, por lo cual no tendrían tiempo para dedicárselo a los investigadores.
- Las instituciones consideran que proporcionar información sobre la seguridad informática no es conveniente por la confidencialidad de la misma.

3.2.5. Técnicas de recolección de datos

Para lo obtención de la información pertinente a la investigación se utilizaron las siguientes técnicas e instrumentos:

- Se utilizó la técnica de la encuesta, la cual consiste en investigar la opinión dominante sobre una materia a través de preguntas realizadas a un segmento de población previamente determinado.
- Como instrumento de exploración se diseñó un cuestionario el cual se estructuró en 6 partes cada una de ellas conteniendo un objetivo y un grupo de preguntas relacionadas con un área específica de la seguridad informática (ver anexo 3).
- Las preguntas contenidas en el cuestionario fueron en su mayoría cerradas, sin embargo en algunos puntos fue necesario que fuesen abiertas para profundizar en la opinión del encuestado.

3.3. RECOLECCIÓN DE LOS DATOS

El procedimiento de aplicación del instrumento fue el siguiente:

- Se contactó al encargado de informática de cada institución que se encuesta vía teléfono o email, donde se solicitó la colaboración para responder el cuestionario.
- Se visitó la institución y se le entregó el instrumento a la persona responsable del área de informática, y se acordó la fecha de entrega.
- Se recogieron llenos los cuestionarios, 4 de ellos fueron enviados vía correo electrónico.

3.4. TABULACIÓN Y ANÁLISIS DE LOS DATOS

Con el objetivo de facilitar el análisis de los datos recolectados en la investigación de campo, éstos se ordenaron y tabularon de acuerdo a cada una de las áreas definidas en el instrumento de recolección de información (cuestionario).

3.4.1. Tabulación de los datos

SEGURIDAD FÍSICA

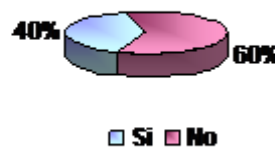
Objetivo:

Determinar si se cuentan con medidas de seguridad encaminadas a mantener el control de las personas que ingresan al local, así como la protección del equipo, edificio y las instalaciones.

Pregunta No. 1:

¿Existe una persona responsable de la seguridad física en el área de informática?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%



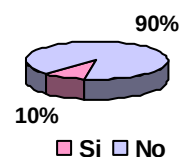
Interpretación:

Por medio de estos resultados podemos asegurar que el 60 % de las instituciones no cuenta con una persona responsable de la seguridad informática y solo el 40 % se ha preocupado por designar a alguien.

Pregunta No. 2:

¿Existe personal de vigilancia que controle el acceso al área de informática?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	1	10%
No	9	90%
Total	10	100%

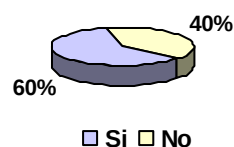
**Interpretación:**

El anterior resultado determina que el 90% de las unidades encuestadas, no cuentan con vigilancia que controle el acceso al área de Informática; solamente un 10 % cuenta con vigilancia.

Pregunta No. 3:

¿ Es restringido el acceso al área donde está el servidor o los servidores?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	6	60%
No	4	40%
Total	10	100%



“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

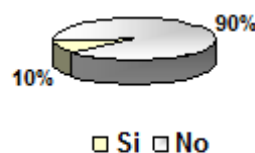
Interpretación:

Los resultados reflejan que un 40 % de las unidades encuestadas no restringe el acceso a esta área, y un 60% si está protegiendo el área de los servidores.

Pregunta No.4:

¿Se ha instruido al personal de vigilancia sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?.

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	1	10%
No	9	90%
Total	10	100%

**Interpretación:**

El anterior resultado muestra que solamente una institución, de las diez investigadas; ha instruido al personal de vigilancia, y es congruente con el resultado de la pregunta 2, debido a que solamente una de ellas tiene vigilancia para controlar el acceso a dicha área.

Pregunta No.5:

¿ Que tipo de control existe para el acceso al área de los servidores?

Alternativas	Frecuencia
1. Por identificación Personal	4
2. Por tarjeta magnética	0
3. Por claves verbales	0
4. Ninguna	5
5. Otros	1

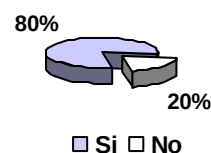
Interpretación:

Según el cuadro anterior de las diez unidades investigadas 5 de ellas han establecido algún tipo de control, para acceder el área de los servidores, donde 4 lo hacen por medio de identificación personal y una de ellas tienen otro tipo de control tales como (llaves).

Pregunta No. 6:

¿considera que las instalaciones donde están los equipos computarizados corren riesgo en caso de fuego?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	8	80%
No	2	20%
Total	10	100%

**Interpretación:**

El anterior resultado nos muestra que la mayoría no ha tomado medidas, por lo que están en riesgo en caso de fuego.

Pregunta No.7:

¿ Existe alarma para:....?.

ALTERNATIVAS	FRECUENCIA
1. Detectar fuego(calor, humo) en forma automática	1
2. Avisar en forma manual la presencia de fuego	0
3. Detectar fuga de agua	0
4. Detectar magnetos	0
5. No existe	9
Total	10

Interpretación:

Solamente una institución de la diez investigadas estaría en condiciones de detectar la presencia de fuego en las instalaciones del área de informática.

Pregunta No.8:

¿ Existe extintores de fuego?

ALTERNATIVAS	FRECUENCIA
1. Manuales	6
2. Automáticos	0
3. No existen	4
Total	10

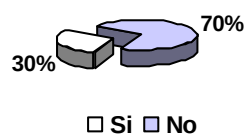
Interpretación:

El 60 % de las instituciones cuentan con extintores manuales, lo cual demuestra que se han tomado prevención caso de fuego, pero un 40 % de estas no cuentan con extintores.

Pregunta No. 9:

¿Se ha adiestrado el personal en el manejo de extintores?.

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	3	30%
No	7	70%
Total	10	100%

**Interpretación:**

El anterior resultado refleja que no obstante que 6 de las instituciones que cuentan con extintores, solamente 3 de ellas han adiestrado al personal para el uso de éstos, de donde se deduce que 3 de ellas que tienen extintores no podrían ser usados en caso de fuego.

Pregunta No. 10:

¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	2	20%
No	8	80%
Total	10	100%

**Interpretación:**

Los resultados muestran que solamente 2 instituciones están llevando a cabo revisiones de funcionamiento de extintores y el resto que cuentan con éstos, corren el riesgo de que no funcione en caso de fuego.

Pregunta No. 11:

¿La salida de emergencia sólo es posible abrirla?.

ALTERNATIVAS	FRECUENCIA
1. Desde el interior	0
2. Desde el exterior	1
3. Ambos lados	1
4. No hay salida de emergencia	8
Total	10

Interpretación:

Solamente 2 instituciones tienen salida de emergencia, de donde 8 de ellas no la tienen exponiendo con ello la seguridad del personal en caso de desastre.

Pregunta No. 12:

¿El área de informática está protegida contra fallo del fluido eléctrico con?

ALTERNATIVAS	FRECUENCIA
1. Planta de emergencia	0
2. UPS para equipo	1
3. Regulador de voltaje	0
4. Planta de emergencia y UPS	2
5. Planta de emergencia, UPS y regulador de voltaje	2
6. Planta de emergencia y regulador de voltaje	0
7. UPS y regulador de voltaje	5
8. Ninguno de los anteriores	0
Total	10

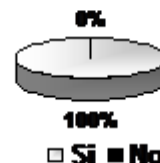
Interpretación:

Según los resultados anteriores todas las instituciones investigadas han tomado algún tipo de precaución para proteger sus equipos en caso de fallo del fluido eléctrico, pero solo dos de ellas han adoptado las tres alternativas de prevención.

Pregunta No. 13:

¿Las instalaciones eléctricas están protegidas con la polarización a tierra?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	10	100%
No	0	0%
Total	10	100%

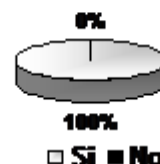
**Interpretación:**

El resultado anterior refleja que 100% de las instituciones ha protegido las instalaciones eléctricas, esto minimiza daños a los equipos y por consiguiente a la información.

Pregunta No. 14:

¿Cuentan las instalaciones donde está el equipo computarizado con aire acondicionado?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	10	100%
No	0	0%
Total	10	100%

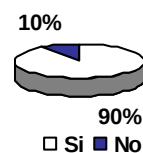
**Interpretación:**

El 100 % de las instituciones investigadas cuenta con aire acondicionado, lo que implica un buen ambiente tanto para el equipo como para el personal.

Pregunta No. 15:

¿Se protege el cableado de la red?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	9	90%
No	1	10%
Total	10	100%

**Interpretación:**

Los resultados reflejan que la mayoría que representan el 90 % ha tomado precauciones en cuanto a protección del cableado, evitando así interrupciones en la red.

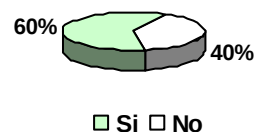
SEGURIDAD LÓGICA Y CONFIDENCIALIDAD**Objetivo:**

Determinar si existe prevención para que la información o los datos computarizados sean conocidos solamente por las personas autorizadas, para evitar que ésta sea mal utilizada, divulgada, robada, sabotada o utilizada para fraudes.

Pregunta No. 16

¿Existen políticas de confidencialidad de la información computarizada?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	6	60%
No	4	40%
Total	10	100%

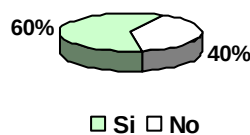
**interpretación:**

El 40 % de las instituciones investigadas no han definido políticas de confidencialidad, esto determina que existe riesgo que la información pueda ser mal utilizada.

Pregunta No.17:

¿Se tienen identificados los archivos con información confidencial?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	6	60%
No	4	40%
Total	10	100%

**Interpretación:**

Este resultado es congruente con la anterior pregunta, donde los resultados reflejan el mismo 40% que no han identificado la información confidencial.

Pregunta No. 18:

¿Se ha establecido que información puede acceder a la información confidencial ?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%

**Interpretación:**

El 60 % de las instituciones investigadas no ha definido restricciones para el acceso a la información confidencial, lo que facilita que personas no deseadas accedan la información.

Pregunta No.19:

¿Considera que la información o los datos pueden estar en riesgo, debido a que cualquier persona sin autorización acceda a los equipos donde está la información?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%



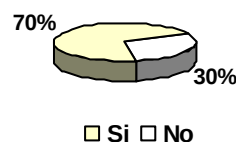
Interpretación:

El anterior resultado determina que el 40 % de las instituciones corre riesgo en cuanto a la seguridad de la información computarizada, por falta de restricciones al acceder a los equipos.

Pregunta No. 20:

Si se tienen estaciones de trabajo conectadas, ¿Se ha establecido procedimientos de operación?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	7	70%
No	3	30%
Total	10	100%

**Interpretación:**

El 30 % de las instituciones no, han establecido procedimientos de operación, para las estaciones de trabajo que están en red.

Pregunta No. 21:

¿Se verifica la identificación del que accede a la red mediante?

ALTERNATIVAS	FRECUENCIA
1. Estación de trabajo	0
2. Usuario	3
3. Ambos	7
4. No se pide identificación	0
Total	10

Interpretación:

El 100 % de instituciones verifica previamente quien accede a cada estación de trabajo, mediante de identificación del usuario, estación de trabajo o ambas.

Pregunta No. 22:

¿ Existen controles de acceso a los sistemas de información Ej. (Password, encriptamiento, menús restringidos, login, privilegios, ningún control, otros)?

ALTERNATIVAS	FRECUENCIA
Login, privilegios y password	1
Login y password	1
Privilegios y password	2
Privilegios, menús restringidos y password	1
Password, login, y menús restringidos	1
Password y menús	1
Password	3
Total	10

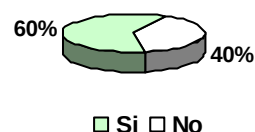
Interpretación:

El 100% de las instituciones se ha preocupado por controlar el acceso a los sistemas.

Pregunta No. 23:

¿Existe una clara definición de funciones para los puestos claves en el área de informática?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	6	60%
No	4	40%
Total	10	100%

**Interpretación:**

Los resultados reflejan que un 40 % de las instituciones, no tienen funciones definidas para puestos claves en el área de informática, lo que indica que no pueden deducir responsabilidades en caso de problemas con la confidencialidad de la información.

Pregunta No. 24:

¿Se registran las acciones de los operadores para deducir responsabilidades en acciones en contra de la confidencialidad de la información mediante:?

ALTERNATIVAS	FRECUENCIA
1. Daños a los datos	2
2. Modificaciones fraudulentas	1
3. Daños a los datos, modificaciones fraudulentas	2
4. daños a los datos, modificaciones fraudulentas y robo de información.	1
5. No se registran las acciones	4
Total	10

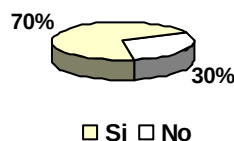
Interpretación:

El 40 % de las instituciones, no lleva ningún registro de las acciones de los operadores, que permita deducir responsabilidades en cuanto a confidencialidad de la información.

Pregunta No. 25:

¿Cuenta el área de informática con un administrador para la red?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	7	70%
No	3	30%
Total	10	100%

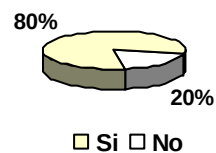
**Interpretación:**

La mayoría cuenta con una persona responsable para administrar la red, sin embargo un 30 % de las instituciones no cuentan con un administrador de red que vigile y supervise su operación.

Pregunta No. 26:

¿Para protección de la red se ha establecido reglas de seguridad basadas en (Ej. los usuarios, grupos de trabajo y direcciones IP) ?.

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	8	80%
No	2	20%
Total	10	100%

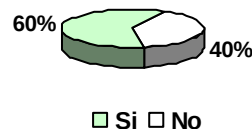
**Interpretación:**

Los resultados reflejan que un 20% de las instituciones no han establecido reglas de seguridad que procuren la protección de la red.

Pregunta No. 27:

Si hay acceso a Internet, ¿Se controla los accesos no autorizados?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	6	60%
No	4	40%
Total	10	100%

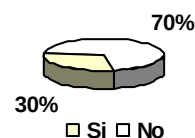
**Interpretación:**

Los resultados muestran que un 40 % de las instituciones, no se preocupa de controlar los accesos a internet.

Pregunta No. 28:

¿Al conectarse a otras redes cuentan con software o hardware que impida que usuarios no deseados accedan la información para dañarla, robarla o divulgarla?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	3	30%
No	7	70%
Total	10	100%

**Interpretación:**

Del 100% de las instituciones 70% no cuenta con software o hardware que impida accesos no deseados.

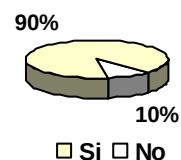
SEGURIDAD EN EL PERSONAL**Objetivo:**

Determinar si el personal de informática ha sido seleccionado por medio de un adecuado proceso de reclutamiento y selección de personal y cuenta con principios, valores y características idóneas así como con el conocimiento y la capacidad necesaria para desempeñarse adecuadamente en su trabajo, y si existen las condiciones internas de trabajo propicias que le permitan trabajar con satisfacción y motivación.

Pregunta No. 29

¿Se utilizan los procedimientos técnicos para el reclutamiento y selección de personal de informática?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	9	90%
No	1	10%
Total	10	100%

**Interpretación:**

El 90 % de las instituciones investigadas afirman que utilizan procedimientos técnicos de selección y reclutamiento de personal, y solo un 10 % no los tiene.

Pregunta No. 30:

¿El horario de trabajo del personal del área de informática es:?

ALTERNATIVAS	FRECUENCIA
1. 6 horas	0
2. 8 horas	5
3. 10horas	3
4. 12 horas	0
5. No tienen horario definido	2
6. Otros	0
Total	10

Interpretación:

De 10 instituciones investigadas 5 de ellas laboran más de 8 horas, es decir que no se observa una jornada normal de trabajo.

Pregunta No. 31:

¿Se han tomado medidas ergonómicas para el personal del área de informática en cuanto a:

ALTERNATIVAS	FRECUENCIA
1. Diseño del lugar de trabajo	0
2. El mobiliario	1
3. Los dos anteriores	0
4. Ninguno	9
Total	10

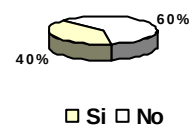
Interpretación:

El 90 % de las instituciones investigadas no han aplicado medidas ergonómicas para el personal del área de informática, por lo que las condiciones de trabajo no son satisfactorias.

Pregunta No. 32

¿Existen adecuadas políticas de vacaciones que impidan dependencia de alguna persona?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%



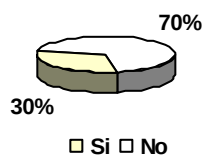
Interpretación:

El 60 % de las instituciones no cuentan con políticas de vacaciones, estas instituciones pueden llegar a depender de una sola persona para llevar a cabo ciertos trabajos.

Pregunta No. 33

¿Cuando algún miembro del área de informática renuncia o falta existe una política de reemplazo?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	3	30%
No	7	70%
Total	10	100%

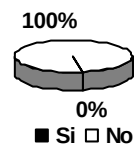
**Interpretación:**

Solamente el 30 % de las instituciones afirmaron contar con políticas de reemplazo, por lo que el resto de instituciones puede llegar a enfrentar problemas.

Pregunta No. 34

¿Cuentan con políticas de rotación del personal del área de informática en puestos de alta confianza?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	0	0%
No	10	100%
Total	10	100%

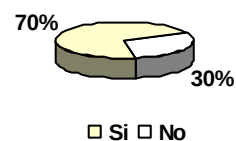
**Interpretación:**

Las 10 instituciones investigadas no cuentan con políticas de rotación de personal. Lo anterior conlleva a las instituciones a depender de una sola persona en los puestos de confianza.

Pregunta No. 35

¿Se controla el horario fuera de horarios?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	7	70%
No	3	30%
Total	10	100%

**Interpretación:**

El 30 % de instituciones no lleva un control de horarios fuera de la jornada normal de trabajo.

Pregunta No. 36:

¿Se capacita el personal del área de informática en: ejemplo (medidas de seguridad, manejo de extintores, manejo de equipo de cómputo, manejo de nuevo software, manejo de información confidencial, planes de contingencia, otros).

ALTERNATIVAS	FRECUENCIA
Medidas de Seguridad	0
Manejo de Extintores	1
Manejo de Equipo de Cómputo	1
Manejo de nuevo Software	5
Manejo de Información Confidencial	0
Planes de Contingencia	0
Otros	0
No se capacita	3
Total	10

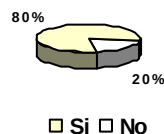
Interpretación

Un 50 % de las instituciones capacita al personal en manejo de nuevo software, un 10% en manejo de extintores y otro 10% en manejo de equipo de cómputo, las instituciones restantes no efectúan ningún tipo de capacitación. Del anterior resultado nos permite establecer que no se capacita al personal en la seguridad.

Pregunta No. 37

¿Cuenta la institución con una persona que realice la limpieza periódicamente en el área de informática?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	8	80%
No	2	20%
Total	10	100%

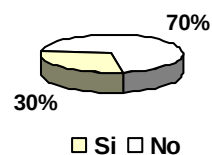
**Interpretación:**

La mayoría cuenta con personal asignado para la limpieza del área de informática, esto es importante para mantener un buen ambiente de trabajo. Sin embargo un 20 % de las instituciones no atiende adecuadamente este factor.

Pregunta No. 38

¿Cuenta la institución con prestaciones adicionales a las que la ley establece para sus empleados?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	3	30%
No	7	70%
Total	10	100%

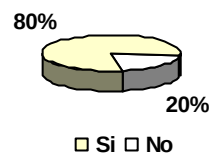
**Interpretación:**

El 70 % de las instituciones no cuentan con prestaciones adicionales a las que la ley establece, esto muchas veces conlleva a tener un personal no motivado para rendir más.

Pregunta No. 39

¿Existen políticas de otorgar permisos o adaptación de horarios para los empleados que deseen estudiar?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	8	80%
No	2	20%
Total	10	100%

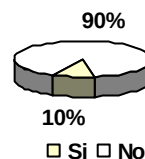
**Interpretación:**

El 80 % de las instituciones otorga permisos a los empleados que deseen seguir estudiando y el 20 % no está brindando esta prestación.

Pregunta No. 40

¿Existe una política de reconocimiento a los logros en el desempeño de los empleados?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	1	10%
No	9	90%
Total	10	100%



Interpretación:

El 90 % de las instituciones no ha establecido políticas de reconocimiento de logros en el desempeño, de donde se deduce que existe la necesidad de mejorar el clima organizacional.

Pregunta No. 41

¿Existe la oportunidad de superación dentro de la institución para el personal de informática?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	6	60%
No	4	40%
Total	10	100%

**interpretación :**

El 60 % de las instituciones está permitiendo que el personal se supere dentro del área de informática, y un 40 % no tiene ese factor de motivación.

Pregunta No. 42

¿Los aumentos salariales se efectúan en base a: (Ej. evaluación de desempeño, porcentaje anual, bonificaciones, otros o ninguno)?

ALTERNATIVAS	FRECUENCIA
Evaluaciones del desempeño	3
Porcentaje anual	1
Bonificaciones	0
Otros	0
No se efectúan aumentos	5
Aumentos anuales	1
Total	10

Interpretación:

Un 50 % de las instituciones no cuentan con políticas de aumento al salario de sus empleados, por lo que el otro 50 % sí ha establecido aumentos por medio de evaluación del desempeño, porcentaje anual o aumentos anuales.

ELEMENTOS TÉCNICOS Y PROCEDIMIENTOS**Objetivo:**

Determinar la existencia de procedimientos, políticas y acciones a seguir en caso de resguardo, recuperación y lugares donde se guarda la información, así como existencia de manuales, procedimientos para mantenimiento de equipo, acceso a la red y adquisición de licencias para software.

Pregunta No. 43

¿Con que manuales cuenta el área de informática Ej. (Manual de usuario, Manual de especificaciones técnicas, Manual de Seguridad, Manual de Procedimientos, Manual de especificaciones funcionales, otros)?

ALTERNATIVAS	FRECUENCIA
Manual de Análisis y diseño, manuales de uso de producto y lenguajes, procedimientos de operador, políticas de backups y recuperación de los mismos	1
Todos los manuales mencionados	2
Manual del usuario, manual de especificaciones técnicas y manual de especificaciones funcionales.	1
Manual del usuario	2
Manual de Especificaciones y Funciones	1
Manual del usuario, manual de especificaciones técnicas y manual de procedimientos	1
Ninguno	1
Otros	1
Total	10

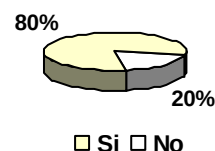
Interpretación:

El 90 % cuentan con manuales, pero se nota la ausencia de un manual de la seguridad informática en la mayoría de las instituciones investigadas. (Dentro de la alternativa de “otros” se mencionó el Manual de Análisis y Diseño.)

Pregunta No. 44

¿Existen políticas de BACKUP y de RESPALDO de la información?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	8	80%
No	2	20%
Total	10	100%

**Interpretación:**

El 80 % afirma contar con políticas de backup y de respaldo, pero no se aplican en algunas de ellas, y el otro 20 % ha descuidado tan importante medida.

Pregunta No. 45

¿Con que políticas de backup y respaldo cuenta la institución?

ALTERNATIVAS	FRECUENCIA
Copias Eventuales	1
Ejecución y Restauración	1
Copias de archivos en cintas magnéticas	1
Respaldos diarios, semanales, mensuales, etc.	4
No tiene	1
Sin respuesta	2
Total	10

Interpretación:

La mayoría lleva a cabo copia de los archivos, pero muchas veces no se verifica que éstas copias estén correctas.

Pregunta No. 46

¿Cuales de los siguientes medios utiliza la institución, para las copias de seguridad, Ej. (disquetes, CD, cintas, disco duro, otros)?

ALTERNATIVAS	FRECUENCIA
Disquetes, CD, Cintas	1
Cintas	4
CD's	1
CD'S y Cintas	3
Disquetes y disco duro	1
Total	10

Interpretación:

Todas las instituciones utilizan distintos medios de almacenamiento de BACKUP, siendo el más utilizado el de cintas y los CD's.

Pregunta No. 47

¿Según el medio utilizado para el resguardo de la información se tiene un inventario de ellos identificándoles plenamente por medio de inventario de ellos identificándoles plenamente por medio de: Ej. (No. De serie, usuario, nombre de los archivos o carpetas, fecha de respaldo, otros)?

ALTERNATIVAS	FRECUENCIA
Fecha de respaldo	2
No. De serie y fecha de respaldo	1
Fecha de respaldo y nombre del server	1
Usuario	1
Otros	3
Sin respuesta	2
Total	10

Interpretación:

El 80 % de las instituciones investigadas respondió que identifica su respaldo con los distintos tipos de identificación mencionados y el 20% se abstuvo de responder. (de los que respondieron “otros”, explicaron que lo hacen en base al nombre del server, fecha de Backups.)

Pregunta No. 48

Cada cuánto tiempo se realizan las copias de seguridad, Ej. (diario, semanal, mensual, quincenal, no se realizan copias, otros).

ALTERNATIVAS	FRECUENCIA
Diario, semanal y mensual	3
Semanal	1
Quincenal	1
Diario y mensual	1
Diario y semanal	2
Otros	2
Total	10

Interpretación:

El 100% de las instituciones afirman que hacen copias de seguridad de la información en los distintos períodos que muestra el cuadro anterior. (Los que respondieron a la alternativa de “Otros” explicaron que las copias de seguridad se realizan en forma eventual), sin embargo en la pregunta No. 44 del cuestionario dos de las instituciones declaró no contar con políticas de backup.

Pregunta No. 49

¿Dónde se guardan físicamente las copias de seguridad, para su protección Ej. (bóveda, cajas de seguridad interna, instituciones externas, en escritorios, los técnicos se las llevan a sus casas, otros)?

ALTERNATIVAS	FRECUENCIA
Escritorios y estantes	1
Caja de seguridad interna y bóveda de banco	1
Caja de seguridad interna	2
Bóveda	1
Archivador	1
Caja de seguridad Externa	1
Escritorios y caja de seguridad	1
Escritorios	2
Total	10

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Interpretación:

Según el cuadro anterior todas las instituciones investigadas, están empleando algún medio para proteger sus copias físicamente, el 80 % las guarda dentro de sus instituciones y solo un 20 % lo hace interna y externamente, considerando ésta última la recomendable.

Pregunta No. 50

¿Qué tipo de mantenimiento se le da al hardware?

ALTERNATIVAS	FRECUENCIA
1. Preventivo	2
2. Correctivo	0
3. Los dos anteriores	6
4. Ninguno	2
Total	10

Interpretación:

Según el resultado anterior el 60 % aplica mantenimiento preventivo y correctivo, un 20 por ciento lo hace solo preventivo y otro 20 % no aplica ninguno, pero este resultado no es congruente con la pregunta 51. Es obvio que ese 20% da mantenimiento correctivo, puesto que al dañarse el equipo hay que mandarlo a reparar forzosamente.

Pregunta No. 51

¿Cada cuánto tiempo se le da mantenimiento al hardware (Ej. mensual, bimensual, trimestral, anual, otros)?

ALTERNATIVAS	FRECUENCIA
Mensual	0
Bi-mensual	4
Trimestral	2
Semestral	1
Anual	1
Otros	2
Total	10

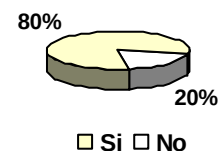
Interpretación:

Un 40 % de las instituciones, el mantenimiento del equipo lo lleva cada dos meses, y el otro 40 % ocupa períodos más largos desde tres meses a un año. (Los que respondieron “otros” que son un 20 % explicaron que el equipo recibe mantenimiento hasta que presenta una falla, esto es mantenimiento correctivo).

Pregunta No. 52

¿Existen normas para el uso de antivirus?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	8	80%
No	2	20%
Total	10	100%



Interpretación:

Según el resultado un 80 % de las instituciones cuentan con normas, para el uso de antivirus, lo que significa que un 20% no las tiene y necesita definir las.

Pregunta No. 53

¿Cuenta la institución con licencias originales tales como Ej. (antivirus, sistemas operativo, lenguajes de programación, software de oficina, otros)?

ALTERNATIVAS	FRECUENCIA
Sistemas Operativos, programas y antivirus	1
Software de Oficina	1
Todos	8
Total	10

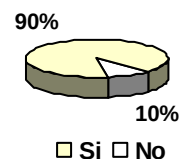
Interpretación:

El 80% de las instituciones cuentan con licencias originales para todas las alternativas, pero un 20 % no los tienen en su totalidad.

Pregunta No. 54

¿Se tienen procedimientos para el uso de antivirus?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	9	90%
No	1	10%
Total	10	100%



Interpretación:

Los resultados reflejan que solo el 10 % no ha definido procedimientos para el uso de antivirus, por lo que los riesgos pueden ser mayores para estas instituciones.

Pregunta No. 55

¿Se revisa periódicamente el cumplimiento de las normas para el uso de antivirus?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%

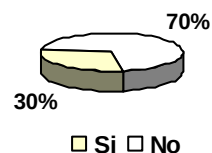
**Interpretación:**

El resultado refleja que solo 4 instituciones de 9 (según pregunta 52) que tienen normas para el uso de antivirus revisan periódicamente el cumplimiento de éstas.

Pregunta No. 56

¿Se lleva documentación por escrito de los cambios realizados en los programas de las aplicaciones?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	3	30%
No	7	70%
Total	10	100%

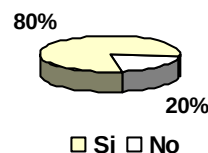
**Interpretación:**

El 70 por ciento de las instituciones investigadas no está documentando los cambios realizados en los programas. Esto puede traer como consecuencia que no se podrán deducir responsabilidades.

Pregunta No. 57

¿Se tiene por escrito el inventario de herramientas software, hardware y las funciones permitidas para cada usuario?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	8	80%
No	2	20%
Total	10	100%

**Interpretación:**

Los resultados reflejan que el 80 % de las instituciones, llevan inventario de las herramientas de software y hardware, y que un 20 % no los tiene.

Pregunta No. 58

¿Cuenta la institución con estándares de análisis y diseño de los sistemas?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	5	50%
No	5	50%
Total	10	100%

**Interpretación:**

Los resultados anteriores reflejan que solo la mitad de las instituciones ha definido estándares de análisis y diseño de los sistemas, y que el otro 50 % puede enfrentar problemas de mantenimiento de los sistemas.

Pregunta No. 59

¿Cuenta la institución con estándares para el desarrollo de las aplicaciones?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%



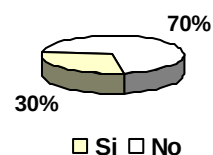
interpretación:

Sólo el 60 % de las instituciones ha estimado definir estándares de desarrollo de las aplicaciones, esto implica que el otro 40 % tendría problemas al mantenimiento de las aplicaciones.

Pregunta No. 60

¿Existen procedimientos para el mantenimiento de las aplicaciones?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	3	30%
No	7	70%
Total	10	100%

**Instituciones:**

Los resultados muestran que el 70 % no tiene procedimientos para el mantenimiento de las aplicaciones, esto no permite deducir responsabilidades en caso de daños a los datos.

Pregunta No. 61

¿Se tienen debidamente documentadas las aplicaciones?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%



Interpretación:

Este resultado es congruente con las dos preguntas anteriores ya que no cuentan con estándares ni de desarrollo ni de diseño, el no tener documentadas las aplicaciones dificulta su mantenimiento y sus correcciones.

Pregunta No. 62

¿Existen procedimientos para apagado y encendido de los equipos?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	7	70%
No	3	30%
Total	10	100%

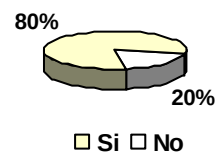
**Interpretación:**

Solamente el 70 % de las instituciones investigadas ha definido procedimientos de apagado y encendido de los equipos, el otro 30 % no cuenta con ellos esto puede llevar a que los equipos se apaguen no adecuadamente y dañe el sistema operativo o los archivos.

Pregunta No. 63

¿ Se capacita a las personas responsables de operar los sistemas en el manejo de éstos?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	8	80%
No	2	20%
Total	10	100%

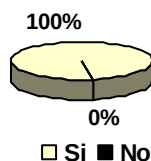
**Interpretación:**

El 80 % de las instituciones investigadas se preocupa de capacitar a los operadores de los sistemas y un 20 % no lo hace, la falta de una adecuada capacitación o de la escogitación de las personas para operar el sistema, puede redundar en problemas con los datos y no se obtengan los resultados deseados.

Pregunta No. 64

¿Cuentan con documentación técnica del software de red?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	10	100%
No	0	0%
Total	10	100%

**Interpretación:**

Los resultados reflejan que todas cuentan con la documentación técnica del software de red.

Pregunta No. 65

¿Cuentan con planos del cableado y conexiones de red?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%

**Interpretación:**

Un 60 % de las instituciones no tienen planos del cableado y conexiones de la red, de donde en algún momento pueden ocasionarse daños en el cableado y dificultar aislar el problema.

Pregunta No. 66

¿Se tienen normas de seguridad para la incorporación de nuevas estaciones de trabajo?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	5	50%
No	5	50%
Total	10	100%



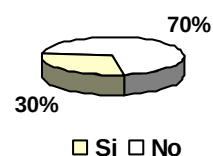
Interpretación:

Los datos reflejan que el 50 % de las instituciones no está tomando medidas de seguridad en cuanto a la incorporación de nuevas estaciones de trabajo a la red; esto puede llevar a que cualquier persona se conecte a la red y esto redunde en la confidencialidad de la información o daño de los mismos.

Pregunta No. 67

¿Se revisan permanentemente las bitácoras de acceso al sistema?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	3	30%
No	7	70%
Total	10	100%

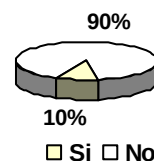
**Interpretación:**

Frecuentemente no se revisan las bitácoras de acceso al sistema, para el caso de la investigación un 70 % de las instituciones no lo hace y esto redunde en la seguridad de la información, porque se podría monitorear que personas no autorizadas hayan accedido el sistema.

Pregunta No. 68

¿Se tienen control de lo que se imprime en las impresoras remotas, en relación a información confidencial?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	1	10%
No	9	90%
Total	10	100%

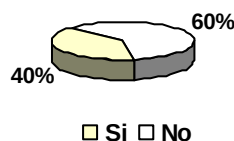
**Interpretación:**

No existe un monitoreo de que se imprime en las impresoras remotas, para el caso el 90% no lo está haciendo, esto atenta contra la confidencialidad de la información.

Pregunta No. 69

¿Se tienen datos de instalación de la red?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%

**Interpretación:**

El 40 % cuenta con datos de instalación a la red, básico para monitoreo de la red en caso de fallo de la red.

ELEMENTOS ADMINISTRATIVOS

Objetivo:

Determinar el papel de la alta administración dentro de la seguridad y su participación mediante el establecimiento de políticas y cuantificación de riesgos.

Pregunta No. 70

¿Se ha identificado aquella información que tenga un gran costo financiero en caso de pérdida?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	5	50%
No	5	50%
Total	10	100%



Interpretación:

Los resultados anteriores muestran que el 50 % de las instituciones investigadas aseguran haber identificado qué información en caso de pérdida tendría un gran impacto financiero.

Pregunta No. 71

¿Se ha identificado las aplicaciones cuya pérdida afecte la operatividad de la institución?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	6	60%
No	4	40%
Total	10	100%

**Interpretación:**

Hay un 40 % de instituciones que no han efectuado ningún análisis que les permita saber qué aplicaciones en caso de fallo podrían afectar la operatividad de la institución, de donde se determina la necesidad de hacerlo.

Pregunta No. 72

¿Se tiene identificados los factores de riesgo que afectan la unidad de informática?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	5	50%
No	5	50%
Total	10	100%

**Interpretación:**

Un 50 % de las instituciones ha identificado los factores que pueden poner en riesgo la unidad de informática.

Pregunta No. 73

Identifique los riesgos a los que está expuesta la unidad de informática de la institución

ALTERNATIVAS	FRECUENCIA BAJO	FRECUENCIA MEDIO	FRECUENCIA ALTO
TERREMOTO	1	6	3
FUEGO	2	5	3
FALLO DE EQUIPO	4	5	1
INFILTRACIÓN	4	5	1
ROBO DE DATOS	4	5	1
FRAUDE	6	3	1
EQUIVOCACIONES	2	8	-
VIRUS	5	5	-
ROBO DE EQUIPO	7	3	-
VANDALISMO	9	1	-

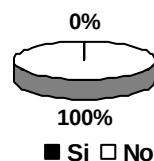
Interpretación:

El cuadro anterior refleja los resultados de un análisis sobre los riesgos ordenados de mayor a menor que las instituciones podrían estar expuestas, de donde los riesgos difieren de una institución a otra en cuanto a nivel de vulnerabilidad, dejando manifiesta la necesidad de protección en cada una.

Pregunta No. 74

¿Los altos niveles administrativos han hecho evaluaciones del impacto que pueden causar en la organización la pérdida de la información?

Alternativa	Frecuencia Absoluta	Frecuencia Relativa(%)
Si	0	0%
No	10	100%
Total	10	100%



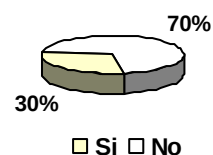
Interpretación:

Ninguna de las instituciones ha hecho evaluaciones del impacto que podría causar a su institución en caso de pérdida de la información, esto sería un parámetro para medir la importancia de la seguridad de la información en las instituciones.

Pregunta No. 75

¿La institución ha establecido procedimientos y prácticas para evitar la interrupción prolongada del servicio de procesamiento de datos debido a contingencias (terremoto, huelga, sabotaje o cortes de energía)?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	3	30%
No	7	70%
Total	10	100%

**Interpretación:**

El 70% de las instituciones, no estaría preparada para enfrentar contingencias, debido a que no cuentan con planes, ni procedimientos, que eviten interrupciones prolongadas del servicio por las causas expuestas.

Pregunta No. 76

¿Hasta cuánto tiempo podría estar la institución sin sistemas por causa de fallo?

ALTERNATIVAS	FRECUENCIA
0 horas	0
1 – 2 horas	3
2 – 4 horas	2
4 – 6 horas	2
Otra	3
Total	10

Interpretación:

Los resultados anteriores reflejan, que el 70 % de las instituciones solo pueden estar sin sistema hasta un máximo de 6 horas.

De los que respondieron “Otra”, uno especifica que la institución puede estar sin sistema un día, la segunda opinó que hasta 3 días, mientras que la última declara que depende de la falla.

Pregunta No. 77

¿Quiénes participan en definir los aspectos de seguridad informática?

ALTERNATIVAS	FRECUENCIA
Alta dirección	1
Área de informática	6
Los dos anteriores	3
Ninguno	0
Otros	0

Interpretación:

El 60 % de las instituciones, es el área de informática la que define los aspectos de seguridad y el otro 40 % tienen su participación la alta dirección.

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Pregunta No. 78

¿Si cuentan con pólizas de seguro en el área de informática Ej. (Hardware, Software, otros, ninguno)

ALTERNATIVAS	FRECUENCIA
Hardware, software y edificio	1
Hardware, Software	1
Hardware	1
Otros	1
Ninguno.	6
Total	10

Interpretación:

El 60 % de las instituciones afirman no tener pólizas de seguro para hardware y software.

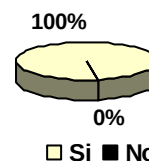
PARTICIPACIÓN DE LA AUDITORIA**Objetivo:**

Determinar el papel de la auditoría en la seguridad y su participación en el establecimiento de procedimientos que garanticen la seguridad de la información.

Pregunta No. 79

¿Existe la unidad de auditoria interna o externa en la institución?

	Fre cuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	10	100%
No	0	0%
Total	10	100%



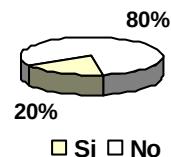
Interpretación:

Todas las instituciones afirman tener una unidad de auditoria.

Pregunta No. 80

¿Participa la auditoria en el diseño y creación de procedimientos de la seguridad:?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	2	20%
No	8	80%
Total	10	100%

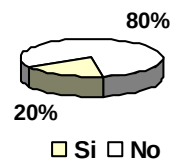
**interpretación:**

Solo un 20% afirma que la auditoria participa en la definición sobre aspectos de seguridad, mientras que el 80% restante no está involucrada dicha unidad en la definición de procedimientos de seguridad.

Pregunta No. 81

¿Participa la auditoria en el análisis y diseño de los sistemas?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	2	20%
No	8	80%
Total	10	100%



Interpretación:

El 80 % de las instituciones, la auditoria no tiene ninguna participación en el análisis y diseño de los sistemas. (Los que respondieron afirmativamente explicaron que esto se logra a través de equipos de trabajo).

Pregunta No. 82

¿Verifica la auditoria el cumplimiento de las políticas de protección de los activos de hardware y software?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	4	40%
No	6	60%
Total	10	100%

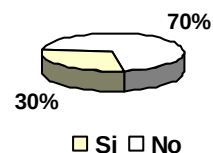
**Interpretación:**

El 40% que respondió afirmativamente explicó que las verificaciones se realizan en forma periódica y el 60 % restante no verifica el cumplimiento de tales políticas.

Pregunta No. 83

¿Verifica la auditoria el cumplimiento de las políticas de confidencialidad?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	3	30%
No	7	70%
Total	10	100%

**Interpretación:**

Según la pregunta 16 solamente 6 instituciones tienen políticas de confidencialidad y de éstas sólo tres tiene su participación la auditoría verificando el cumplimiento de éstas, el resto lo hace.

Pregunta No. 84

¿Verifica la auditoría el cumplimiento de políticas de procedimiento para el uso de licencias?

	Frecuencia	Frecuencia
Alternativa	Absoluta	Relativa(%)
Si	5	50%
No	5	50%
Total	10	100%

**Interpretación:**

Solamente el 50 % de las instituciones participa la auditoría en verificar el cumplimiento del uso de las licencias y el 50 % no lo lleva a cabo.

3.4.2. Análisis De Los Datos

3.4.2.1. Área de Seguridad Física

En esta área el punto de partida para estructurar bien la seguridad informática es contar con una persona encargada de la seguridad, sin embargo solo un 40% de las instituciones cuenta con ello, lo que podría ocasionar para el resto que existan vacíos en los elementos de seguridad necesarios o que éstos se salgan de control, puesto que nadie tiene la responsabilidad de supervisarlos.

Casi la totalidad de las instituciones no cuenta con vigilancia que controle el acceso al área de informática, lo cual eleva el riesgo de que un extraño pueda ingresar y causar daños a los equipos. Pese a que una minoría de las instituciones sí protege el acceso al área de los servidores, si no existe una persona responsable de la seguridad y no tienen vigilancia de acceso al área de informática, la vulnerabilidad a daños para los servidores es alta, especialmente porque las pocas instituciones que sí restringen el acceso se valen de únicamente identificación personal y utilización de llaves como medidas de control y esto deja el vacío que “personas amigas” de quien esté controlando el acceso en determinado momento entre y pueda causar daños incluso por ignorancia sobre el trato de éstos equipos, ello por supuesto afecta también la seguridad de la información. Es obvio que si no se han tomado medidas para restringir el acceso, tampoco existe la preocupación por parte de las instituciones de instruir al personal en caso de que alguien pretenda entrar a las instalaciones.

El 80% de las instituciones considera que en el lugar donde se encuentran las instalaciones, los equipos sí corren riesgo en caso de fuego, sin embargo sólo una de ellas cuenta con alarma que pueda detentar fuego en forma automática, el resto no cuenta con ningún tipo de alarma. Este vacío puede ocasionar que se vuelvan inútiles los extintores de fuego que sí poseen por lo menos el 60% de las instituciones, pues podría ocurrir que en ausencia de una alarma se detecte el fuego en un punto crítico ya incontrolable por medios simples especialmente si ocurre en horarios de poca presencia de personal, y además solamente 3 de éstas 6 instituciones que sí poseen extintores, han instruido al personal en su uso, y de éstas tres sólo 2 revisan el correcto funcionamiento de los extintores con su proveedor. En caso de presentarse un siniestro éstas condiciones elevan el riesgo a que los daños puedan ser más cuantiosos, no sólo materiales si no también en vidas humanas ya que solamente 2 instituciones cuentan con salida de emergencia.

Con relación a la prevención en caso de fallos eléctricos todas las instituciones han adoptado medidas esto reduce el riesgo de que se dañen los equipos por fluido eléctrico, pero dos de ellas no cuentan con regulador de voltaje y esta ausencia sí puede ocasionar daño en caso de irregularidades en el fluido eléctrico. En cuanto a las medidas comunes de protección a los equipos como son: la polarización a tierra de las instalaciones eléctricas, aire acondicionado en el lugar donde se encuentra el equipo y la protección al cableado de la red, casi la totalidad de las instituciones ha tomado dichas medidas, solo existe una que no protege el cableado de la red y esto puede ocasionar interferencia en la

comunicación de la red, así como aumenta el riesgo en cuanto al funcionamiento continuo de la red.

3.4.2.2. Área de Seguridad Lógica y Confidencialidad

Existe una debilidad en esta área en lo referente a la definición de políticas de confidencialidad, e identificación de archivos que contienen información sensible, así como el control lógico de acceso, debido a que estos aspectos representan el punto de partida para la seguridad lógica y confidencial. Sin embargo a pesar de no poseer políticas establecidas, tienen cierto grado de control en el sentido de que sí verifican la identificación de los que acceden a las estaciones de trabajo, lo cual representa una fortaleza que las instituciones poseen, pues ya utilizan ciertos controles de acceso a los sistemas tales como: login, privilegios, password y menús restringidos, entre otros. Esto permite que pueda identificarse la responsabilidad de quien ocasione daños a los sistemas en caso de ser necesario, sin embargo es importante marcar el rumbo de estos esfuerzos aislados y combinarlos estableciendo las políticas pertinentes. En relación a la protección de intrusos externos un 40% de las instituciones no cuentan con un control para los accesos no autorizados a Internet, esto constituye un alto riesgo de infección de virus, ingreso de intrusos a la red que puedan causar daños a la información, así como ocasionar fugas de información confidencial. Por otro lado es positivo que las instituciones que necesitan conectarse a otras redes poseen un software que les ayuda a proteger de daños la información computarizada.

Es necesario elevar los niveles de protección en esta área, ya que debe considerarse como posibilidad el crecimiento de la institución y posibles necesidades a futuro,

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

además es necesario integrar los esfuerzos aislados de seguridad que ya poseen.

3.4.2.3 Área de Seguridad en el Personal

Uno de los puntos claves para partir en la seguridad del personal es un buen reclutamiento de personal, utilizando procedimientos técnicos que lo garanticen, en este sentido es satisfactorio que los datos reflejen que el 90% de las instituciones utilice dichos procedimientos, ésta es una fortaleza que debe dársele continuidad con otros factores como las políticas de administración del personal que impida la dependencia de algunos elementos, sin embargo a este respecto sí existe cierta discontinuidad en la labor de administración de los recursos humanos debido a que la totalidad de las instituciones investigadas no cuentan con políticas de rotación de personal en puestos de alta confianza, así mismo un 70% de ellas carecen de políticas de reemplazo por renuncia o ausencias inesperadas, esto puede provocar que enfrenten problemas incluso de operatividad de labores.

Con relación al factor de motivación, un 70% de las instituciones no cuentan con prestaciones adicionales a las de la ley para sus empleados, pero un 80% de las instituciones otorga permisos o adaptación de horarios para empleados que deseen estudiar, este es un elemento positivo para la satisfacción de los empleados, sin embargo no puede asegurarse que este elemento responda a los intereses de todos, deben considerarse otros como la superación, donde 6 de las instituciones cuentan con oportunidades de superación internamente, sin embargo sólo una de todas las instituciones posee políticas de reconocimiento a los logros en el desempeño, lo que

significa que aunque existan oportunidades de superación dentro de la institución, las probabilidades de alcanzarlas son pocas si no se reconocen los logros, además un 50% de las instituciones no posee políticas de evaluación para basar la fijación de aumentos salariales, todos éstos aspectos pueden llegar a afectar negativamente el clima organizacional de los empleados y de ello depende en gran medida la estabilidad y lealtad del personal como también influye en el riesgo de ataque intencionados.

Por otro lado existen factores cuya presencia no causa motivación, pero su ausencia si produce desmotivación o incluso enfermedad, tal es el caso de las medidas ergonómicas donde los resultados reflejan que el 90% de las instituciones no han aplicado ninguna medida, también es el caso de las políticas de vacaciones en las cuales sólo un 40% de las instituciones las ha contemplado en la administración de los empleados, otro factor es el aseo, en el cual satisfactoriamente el 80% de las instituciones asegura contar con una persona asignada para la limpieza del área de informática.

Otro riesgo, dentro de la seguridad del personal, es el control del acceso al área informática fuera de horarios normales, por la vulnerabilidad de las instalaciones, a este respecto el 50% de las instituciones declara que trabajan más de 8 horas, o ni siquiera tienen un horario definido y un 30% de las instituciones no posee ningún control para el trabajo en horarios fuera de la jornada normal, lo que puede facilitar ataques intencionados, y lo que es peor, permite realizarlos en forma anónima, por parte del personal que por algún motivo se encuentre insatisfecho.

3.4.2.4 Área de Elementos Técnicos y Procedimientos

Existe una ausencia de un manual de seguridad en el 80% de las instituciones, aunque tienen presencia de otros manuales que ayudan en alguna medida a la seguridad, es necesario contar con el manual de seguridad para una correcta orientación a los empleados a través de una efectiva sistematización tanto en la aplicación teórica como en la operativa.

En relación a los procedimientos la mayoría de las instituciones cuenta con políticas de backup y utilizan en su mayoría cd's y disquetes con su respectiva identificación para cumplir este efecto, la frecuencia con que se hace es diario semanal y mensual, pero en cuanto al almacenaje de los backup, se realiza regularmente dentro de la misma institución, lo que aumenta el riesgo para la información en caso de un siniestro que afecte toda la institución.

En lo referente a procedimientos para el tratamiento de virus, los datos reflejan que las instituciones tienen cierto grado de conciencia, ya que el 90% de ellas han definido procedimientos para el uso de antivirus y también un 80% cuenta con licencias originales para el software que utilizan, que es una forma de disminuir riesgos de infección de virus, sin embargo solo un 40% de las instituciones revisa periódicamente el cumplimiento de normas establecidas para el uso de antivirus, lo que significa que aunque cuenten con normas y procedimientos antivirus, si no se verifica aplicación y cumplimiento es como si no se tuvieran.

Se le ha dado poca atención a la documentación y estandarización del desarrollo de las aplicaciones con que cuentan, lo cual genera dependencia del personal clave y atenta

contra la seguridad. En cuanto a los aspectos propiamente relacionados con la red la mayoría cuenta con la documentación técnica de red que se adquiere con la compra del software de red, sin embargo existe cierta deficiencia en el resto de necesidades como: planos de cableado de red, revisión de bitácoras de acceso, información de instalación de red, procedimientos de apagado y encendido de equipos y procedimientos para la incorporación de nuevas estaciones de trabajo. Los elementos técnicos para la seguridad en redes es muy importante para garantizar el correcto y continuo funcionamiento del sistema, así como la operatividad de la información, en este sentido las instituciones tienen un riesgo latente mientras no llenen esas deficiencias de seguridad.

3.4.2.5. Área de Elementos Administrativos

Con relación a los elementos administrativos los datos reflejan que la participación de la alta administración en la seguridad informática es casi nula, por ende el interés prestado a la coordinación de la seguridad, que deberían estar bajo la responsabilidad de esta área, a través del establecimiento de políticas, y cuantificación de riesgos, no existe.

Solo un 50% de las instituciones asegura haber identificado la información que tenga un representativo costo financiero en caso de pérdida, sin embargo, ninguna de las instituciones ha realizado evaluaciones sobre el impacto que podría causar a la institución la pérdida de la información. Por otro lado 6 de las instituciones declaran haber efectuado un análisis para identificar las aplicaciones que, en caso de fallo, podrían afectar su operatividad, pero sólo 3 de ellas han establecido procedimientos y prácticas en caso de interrupción por contingencias, esto significa que el 70% de las

instituciones no están preparadas con planes contingenciales ni procedimientos alternativos de operatividad en caso de siniestro; pese a ello también un 70% de las instituciones reconoce que solo pueden estar un máximo de 6 horas sin sistema (tres de ellas solo toleran un máximo de 2 horas). Estos aspectos aunados con el resultado de que solo la mitad de las instituciones ha identificado los factores de riesgo a los que está sujeta la unidad de informática, dejan en evidencia la falta de conciencia por parte de la alta administración en los aspectos de seguridad que además se refleja en el resultado de que solamente en 4 instituciones existe alguna participación de la alta dirección, este dato explica porqué solo 4 instituciones cuentan con pólizas de protección para hardware y software.

La pregunta número 72 merece una especial atención de sus resultados porque refleja una identificación rápida y sencilla de los riesgos a los que están sujetas las unidades de informática en las instituciones y esta información al cruzarse con el análisis de los factores anteriores evidencian una necesidad clara de participación y mayor interés por parte de la alta dirección en el establecimiento de políticas y adopción de herramientas que coadyuven a la seguridad informática, considerando los factores sociales de nuestro país (delincuencia, movimientos sísmicos por incidencia geográfica, irregularidad en los servicios básicos, entre otros) este vacío de seguridad en lo referente a los elementos administrativos coloca a las instituciones en un riesgo potencial muy alto de enfrentar impactos financieros por pérdida de información crítica, discontinuidad en la operatividad normal, entre otros. Es importante reiterar que el área administrativa marca el rumbo que tomara la institución en los aspectos de seguridad informática.

3.4.2.6 Área de Participación en la Auditoria

La totalidad de las instituciones cuentan con una unidad de auditoria, sin embargo esta realiza labores encaminados mas a la salvaguarda de activos que al seguimiento de procedimiento de procedimientos de seguridad informática. La participación de la auditoria en aspectos de seguridad es prácticamente nula en la mayoría de las instituciones, por lo tanto es un área que es necesario reforzar con la definición del papel que debe jugar la misma, para garantizar la verificación de la aplicación de los procedimientos de seguridad. Esta es una de las áreas más importantes con relación a la definición de un manual de seguridad por ser la encargada de retroalimentar el cumplimiento de las normas, reglas y procedimientos en las instituciones.

TABLA DE CONTENIDO

	Página No.
1. Introducción	1
2. Objetivos de Manual	3
2.1. Objetivo General	3
2.2. Objetivos Específicos	3
3. Alcance del Manual	4
4. ¿Cómo usar el Manual?	5
5. Revisiones y Recomendaciones	9
Parte I. Introducción a la seguridad de la información computarizada	10
1.1. Los riesgos y amenazas	10
1.2. La información en la institución	11
1.3. El significado de la seguridad de la información	12
1.4. El papel de la alta administración en la seguridad de La información computarizada	12
Parte II. Disposiciones acerca de la seguridad de la información computarizada	14
2.1. Políticas generales	14
2.2. Políticas específicas	15
2.2.1. Área Física	15
2.2.2. Área Lógica y Confidencialidad	17
2.2.3. Área de Personal	19

2.2.4	Elementos Técnicos y Procedimientos	20
2.2.5	Elementos Administrativos	23
2.2.6	Área de Auditoría	24
2.2.7	Plan de Contingencia	25
2.3	Normas e instrucciones para la protección de documentos	26
2.3.1	Introducción	26
2.3.2	Tipos de documentos	27
2.3.3	Clasificación y definición de categorías	27
2.3.4	Manejo de Documentos de la categoría “Solo para uso interno”	29
2.3.5	Manejo de Documentos de la categoría “Solo para uso limitado”	30
2.3.6	Manejo de Documentos de la categoría “Solo para uso confidencial”	32
2.3.7	Observaciones a la clasificación	33
Parte III.	Acciones acerca de la seguridad de la información computarizada	35
3.1	Objetivo de las medidas de seguridad	36
3.2	Consideraciones sobre seguridad	37
3.3	Acciones para la Seguridad Física	40
3.4	Acciones para la Seguridad Lógica y Confidencialidad	73
3.5	Acciones para la Seguridad en el Personal	85

3.6	Elementos Técnicos y Procedimientos	102
3.7	Elementos Administrativos	136
3.8	Auditoria Interna	150
3.9	Plan de Contingencia	166

- Glosario

- Bibliografía

- Anexos:

No. 1 Tipos de Extintores

No. 2 Ejercicios para disminuir el estrés

No. 3 Pólizas de Seguros que ofrecen Empresas Aseguradoras

De El Salvador

No. 4 Registro de incidentes informáticos

No. 5 Los incentivos

No. 6 Capacidad de Plantas Eléctricas

No. 7 Cálculo de cargas térmicas

1. INTRODUCCIÓN

La seguridad informática surge como respuesta a la necesidad de proteger la información computarizada, debido a que ésta constituye una herramienta efectiva para la toma de decisiones en todos los niveles.

Es por lo anterior que se consideró necesario elaborar un manual técnico de seguridad para la información computarizada de las Instituciones Oficiales Autónomas Subvencionadas, que contemple los objetivos, políticas, procedimientos y acciones a seguir para proteger la información computarizada. El manual técnico de seguridad debe servir como guía en la aplicación de medidas de seguridad informática a todos los niveles y áreas involucradas.

En el contenido del manual se desarrollarán cuatro partes básicas:

La primera trata de generalidades del manual como: el establecimiento de los objetivos, la explicación de cómo usarlos, revisiones y recomendaciones, entre otros.

La segunda fase cubre un área de sensibilización sobre el tema de seguridad, es decir que explica la importancia de la información computarizada y el beneficio de darle una seguridad preventiva a la misma, en lugar de incurrir en costos cuando se enfrentan problemas y se hace necesario realizar acciones correctivas para continuar o reanudar operaciones.

La tercera fase entra ya en materia de seguridad pero a nivel administrativo, y trata sobre políticas de seguridad tanto generales como específicas, cuya elaboración está bajo la responsabilidad de la alta dirección y los niveles gerenciales.

La cuarta fase trata sobre las acciones específicas a realizar por áreas, dichas áreas cubren la seguridad, de todos los recursos informáticos involucrando a todos los niveles, explicando directrices, procedimientos, responsables de las actividades, entre otros. Esta parte está estructurada en siete partes denominadas: seguridad física, seguridad lógica y confidencialidad, seguridad en el personal, elementos técnicos y procedimientos, elementos administrativos, participación de la auditoría y plan de contingencia. Cada una de ellas pretende guiar a los usuarios en la aplicación de medidas específicas necesarias para cubrir la seguridad de esa área.

Además el manual incluye un glosario de términos, anexos que complementan la comprensión de los temas abordados y la bibliografía base para su realización, que además puede servir como apoyo para profundizar más en las áreas de seguridad informática.

2. OBJETIVOS DEL MANUAL

2.1. Objetivo General

Contribuir a la protección de la información computarizada en las instituciones oficiales autónomas, a través de la promulgación de lineamientos generales y procedimientos de seguridad que sirvan de guía para el personal involucrado en el procesamiento de la información computarizada.

2.2. Objetivos Específicos

- ◆ Enfocar la Información computarizada como un activo importante para la institución.
- ◆ Concientizar al personal involucrado en el procesamiento de la información computarizada, de la necesidad de observar las medidas para el resguardo de la misma.
- ◆ Disponer de una herramienta técnica que guíe a los encargados del área de informática en la administración de la seguridad.
- ◆ Formalizar y estandarizar las Normas y Procedimientos del Área Informática en relación a la protección de los sistemas de información computarizados.
- ◆ Minimizar el riesgo de pérdida de la información y Asegurar la Confidencialidad.
- ◆ Establecer procedimientos que reduzcan el impacto de las contingencias en la información computarizada



Definir la participación de la auditoría en el ámbito de la seguridad informática

3. ALCANCE DEL MANUAL

Es una fuente de consulta escrita que está diseñado a fin de coadyuvar a la protección de la información computarizada, cuya responsabilidad es de los encargados de administrar la seguridad informática o en su defecto el encargado del área de informática.

Como guía de consulta únicamente describe políticas, normas, acciones y procedimientos para la protección de la información en las áreas de:

1. Seguridad física
2. Seguridad lógica y confidencial
3. Seguridad en el personal.
4. Elementos técnicos y procedimientos
5. Elementos administrativos.
6. Auditoría interna
7. Plan de contingencia

Este manual no incluye formas de implantación de un plan de seguridad, es decir que no contempla diseño de capacitaciones para la seguridad, si no que describe directamente los lineamientos y acciones necesarias para la protección de la información, así como las partes de la institución que deben involucrarse en su ejecución.

4. ¿CÓMO USAR EL MANUAL?

El presente manual está diseñado como guía para la seguridad del área de informática el cual puede ser denominado también de la siguiente manera:

- Manual técnico para la seguridad de la información computarizada
- Manual de políticas, normas, procedimientos y acciones a seguir para la seguridad de la información.

Presenta la descripción de un conjunto de políticas, normas, procedimientos y acciones a seguir encaminadas todas ellas a contribuir a la realización de actividades para el resguardo de la información computarizada en el área de informática.

Contar con un manual de seguridad es contar con una guía que conlleva a una importante reducción de tiempo inactivo e improvisación, por lo que generalmente es utilizado como elemento de consulta. De allí la importancia de hacer un uso efectivo del mismo, para ello a continuación se describe el cuerpo sistemático de este manual, es decir, la forma en que está estructurado y el modo correcto de buscar información dentro del mismo; con el fin de optimizar el tiempo de consulta.

4.1. Estructura del manual

El manual consta de tres partes principales que son:

PARTE I. Introducción a la seguridad de la información computarizada, en esta fase se describe brevemente el valor de la información para la institución, lo que significa su seguridad, los riesgos y amenazas a los que está expuesta la información y el papel de la alta administración en la protección de dicha información.

PARTE II. Disposiciones acerca de la seguridad de la información computarizada,

en esta fase se describen las políticas, generales o específicas que direccionan la seguridad en forma general. Aca puede encontrarse el origen de los procedimientos contenidos en el manual.

PARTE III. Acciones acerca de la seguridad de la información computarizada,

esta parte se describen los procedimientos necesarios para cubrir todas las áreas que competen a la seguridad informática y responden a los lineamientos especificados en las políticas. Cada procedimiento esta definido dentro del área de seguridad que le corresponde. Las áreas incluidas son:

1. Seguridad física, se refiere a procedimientos de seguridad para el equipo y las instalaciones.
2. Seguridad lógica y confidencial, contiene procedimientos encaminados a proteger el software, y la confidencialidad de la información.
3. Seguridad en el personal, define los procedimientos para la adecuada administración del personal, asegurando la protección de la información.
4. Elementos técnicos y procedimientos, contiene todas aquellas acciones técnicas necesarias para la protección de la información que no puede ubicarse en el área física ni lógica
5. Elementos administrativos, se refiere a los procedimientos que por su naturaleza, corresponde a la alta dirección realizarlos.
6. Auditoria interna, contiene los controles en los que ha de involucrarse la auditoria en materia de seguridad.

7. Plan de contingencia, contiene todas las acciones a seguir en caso de ocurrir cualquier suceso inesperado.

Además el manual cuenta con otros elementos que completan la información que aporta.

Tales como:

- Glosario de términos, para entender las referencias que se realicen a lo largo de su contenido.
- Anexos, que comprende aquellos documentos, imágenes, diagramas o tablas importantes para la comprensión del tema donde fueron llamados, pero que fue necesario sacarlo de contexto para no desviar la atención de la idea desarrollada.
- Bibliografía, donde se declaran los textos fuente para el manual y que son una alternativa de consulta si se quiere profundizar o ampliar mas sobre el tema consultado.

4.2. Pasos a seguir para la consulta de información

Primero, identifique su tipo de consulta, la cual puede ser:

- Una duda de conceptos
- Una consulta de lineamientos generales
- Consulta en la forma de realizar un procedimiento específico

Segundo, ubique su consulta dentro del manual:

- Si es de conceptos, podría ser sobre la información computarizada o relacionada con esta, para ello debe referirse al índice y ubicarse en la primera parte.
- Si fuese de términos, puede consultar el índice para ubicar donde inicia el glosario y luego buscar el término deseado en orden alfabético igual que en un diccionario.

- Si la consulta es sobre disposiciones, debe ubicarlos en que nivel de la institución tienen acción, es decir que si son para toda la institución estaremos hablando de políticas generales, en cambio si esta interesado en la normativa un área especial de la seguridad, debe referirse a políticas específicas.
- Si la consulta es sobre la realización de un procedimiento específico primero debe ubicarse a que área de la seguridad corresponde, para lo que puede ayudarse de cómo esta estructurado el manual, luego referirse al índice y ubicar la consulta respectiva en el área correcta.

Tercero, apoye siempre su consulta al manual con la ayuda que pueda brindarle el encargado de administrar la seguridad informática.

Simbología utilizada en el manual:



Este rombo ha sido utilizado para definir objetivos generales y específicos del manual.



Con este botón se identificarán las políticas



Este símbolo ha sido utilizado en casi todo el manual para identificar acciones, medidas, y factores de la seguridad.

5. REVISIONES Y RECOMENDACIONES

En materia de la informática los cambios tecnológicos son constantes y frecuentes, por lo que se hace necesario revisar periódicamente el contenido de este manual y su

aplicabilidad real en el momento de la revisión, afín de mantenerlo actualizado y no pierda su efectividad.

Se recomienda especialmente estar atento a las actualizaciones de antivirus y sus usos, así como todos los cambios que se den en cuanto a software que apliquen a la institución. En materia de hardware, se hará necesario revisar el manual cuando se invierta en nuevas adquisiciones del mismo, así como también si se da un crecimiento en el área de informática de la institución, será necesario revisar si el manual continua siendo funcional o necesita algunos ajustes.

PARTE I

INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN COMPUTARIZADA

La función del procesamiento de datos es un servicio de toda la institución, que apoya no solo a los sistemas de información administrativa sino también a las operaciones funcionales. La seguridad es un aspecto de mucha importancia en la correcta administración informática, lo es también de toda la institución.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y acciones que conlleven no solo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que estos se encuentren.

1.1. RIESGOS Y AMENAZAS

Cuando se habla de la función informática generalmente se tiende hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información mas consistente, entre otras.

Sin embargo se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la **“información”**.

Es muy importante conocer su significado dentro de la función informática, de forma esencial, cuando su manejo está basado en tecnología moderna, para esto se debe conocer que la información:

- Está almacenada y procesada en computadoras
- Puede ser confidencial para algunas personas o a escala institucional
- Puede ser mal utilizada o divulgada
- Puede estar sujeta a robos, sabotaje o fraudes

Los primeros puntos nos muestran que la información está centralizada y que puede tener un alto riesgo y los últimos puntos nos muestra que se puede provocar la destrucción total y parcial de la información, que incurre directamente en su disponibilidad que puede causar retrasos de alto costo.

Hay que imaginar que pasaría si se sufre un accidente en lugar donde se almacena la información. Ahora habría que preguntarse: ¿cuánto tiempo pasaría para que la institución este nuevamente operando?

Es necesario tener presente que el lugar donde se centraliza la información con frecuencia puede ser el activo más valioso y al mismo tiempo el más vulnerable.

1.2. LA INFORMACIÓN EN LA INSTITUCION

Hasta la década de los ochenta los administradores no necesitaban saber como la información se obtenía, procesaba y distribuía en sus instituciones, requiriendo un mínimo de tecnología. La información en sí no se consideraba como un activo de importancia para la empresa.

En la actualidad pocos administradores pueden darse el lujo de ignorar como se maneja la información al interior de las instituciones.

1.3. EL SIGNIFICADO DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información ha adquirido, un significado muy importante en las instituciones, siendo esta un patrimonio muy valioso susceptible de protección. Es por ello la importancia de contar con medidas de seguridad encaminadas a la protección de la información computarizada, que le permitan asegurar la continuidad del procesamiento de información necesaria, para el adecuado desempeño de las funciones institucionales.

1.4 EL PAPEL DE LA ALTA ADMINISTRACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN COMPUTARIZADA

A medida que la tecnología ha ido evolucionando y con ella la importancia de los sistemas de información la seguridad del entorno informático (hardware, software, comunicaciones, entre otros) se ha convertido en una de las grandes preocupaciones de los profesionales de esta actividad, ante esta situación los directivos de cada institución deben entender claramente su participación en materia de seguridad de esta área, ya que deben considerar las inversiones en medidas para proteger la información computarizada, que contribuyan a mantener la operatividad y rentabilidad de las empresas.

Por consiguiente la alta administración debe definir una normativa de seguridad. Esta puede definir reglas, principios y procedimientos que regulen la forma en que la

institución gestiona, protege y controla sus recursos de informática y la información que contienen.

PARTE II

DISPOSICIONES ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN COMPUTARIZADA

Entre las disposiciones acerca de la seguridad se han definido políticas de seguridad que es una declaración de intenciones de alto nivel que cubre la seguridad de la información computarizada y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

Las políticas se reflejan en una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medidas a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento.

Las políticas generales nos permiten analizar los requerimientos de seguridad de información de su organización y sus prioridades. Además definen la base para las políticas específicas, asegurando que el alcance de las mismas cumpla con las necesidades propias de la institución y que puedan ser implantadas en la práctica.

2.1. POLÍTICAS GENERALES

-  Cumplir con las regulaciones contenidas en el presente plan.
-  Todo el personal con acceso a los medios de computación existentes en el área deberá ser capacitado previamente.
-  Mantener la observancia sobre el cuidado y estado técnico del equipo y los soportes.
-  Contar con una póliza de seguro informático
-  Hacer saber a los responsables administrativos de las áreas en que existan medios de computación, que tiene la obligación de EXIGIR por el cumplimiento de las medidas de Seguridad Informática, y tomar las medidas técnicas y administrativas correspondientes ante cualquier violación detectada.
-  Contar con una bitácora de incidencias de problemas relacionados con la seguridad, así como la solución de cada uno de ellos. (ver anexo 4 del manual)
-  Mantener condiciones ambientales adecuadas, para el buen funcionamiento del equipo y rendimiento del personal.

2.2. POLÍTICAS ESPECÍFICAS

2.2.1. Área Física

El área física donde se ubica el equipo informático debe cumplir las siguientes políticas:

-  Contar con equipo de climatización para evitar el calor, humedad y la entrada de polvo.

- Poseer equipos de estabilización de voltaje para evitar las afectaciones por inestabilidad en el voltaje.
- Adecuada hermeticidad y cierre de puertas y ventanas, para evitar la entrada de agua, polvo y hurtos.
- Los locales donde se encuentran ubicadas las maquinas están provistos de seguridad en techos y paredes y las puertas habilitadas con sistema de cierre y sellaje.
- Los equipos instalados solamente podrán recibir mantenimiento y reparación por los técnicos autorizados por el encargado de seguridad informática.
- Si la reparación y mantenimiento se lleva a cabo por personas externas a la institución, deberá realizarse en presencia del responsable de la seguridad o un técnico asignado para ello.
- De producirse alguna anomalía en la computadora se procederá:
 - No se utilizará ningún equipo hasta tanto no se reporte al responsable de seguridad Informática.
 - No hacer comentarios de la situación creada.
- Para el traslado dentro y fuera del área se hará con la autorización del Responsable de Seguridad Informática y del Jefe de área.
- El personal que hace uso de los equipos deberá ser el autorizado por el jefe de área, quien se mantendrá actualizado sobre las regulaciones establecidas en el manual de seguridad informática.

-  No facilitar el acceso de personal ajeno a las tecnologías de información.
-  El acceso a los locales donde existan medios informáticos esta restringido, solamente a los especialistas y técnicos que por su trabajo están vinculados a estos medios.
-  Si por alguna razón de trabajo hiciera falta que algún técnico o especialista de otra área previamente capacitado tuviera acceso a esta área seria plasmado en el libro de incidencia de acceso de personal del área.
-  Los disquetes deben ser conservados en lugar seguro, bajo llave sin que lo afecten la humedad, radiaciones etc.
-  Las máquinas están situadas de forma que no da visibilidad desde puertas o persianas para evitar que cualquier información que se esté procesando no sea advertida por personal ajeno a la Oficina.
-  Se prohíbe terminantemente la utilización de las maquinas para jugar
-  No fumar ni ingerir alimentos dentro del área donde se encuentra el equipo.

2.2.2. Área Lógica y Confidencialidad

-  Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y cifrada.
-  Esta terminantemente prohibido ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas.

- Todo software que entre a la institución debe ser previamente chequeado y analizado por el responsable de la seguridad informática para su posterior instalación en el área que corresponda.
- La instalación de cualquier software en la entidad debe hacerse en presencia del responsable de la seguridad informática o por el mismo.
- Reportar al responsable de informática cualquier anomalía en el funcionamiento de los programas.
- Mantener en secreto las claves de acceso al software que por sus características lo requieran y las claves de acceso a la red así como sus niveles de acceso por maquina
- No permitir el uso de maquinas por personal que no tenga los conocimientos requerido para ello. Antes deben adiestrarse.
- Tener una copia de todo software de instalación y copias de todos los sistemas de la institución que se procesa en la entidad
- Mantener actualizados los software antivirus en todos lo PC
- El responsable de Seguridad informática será el encargado de mantener actualizado en toda las máquinas la última versión del sistema antivirus autorizado.
- Se deben utilizar para protección contra virus el software entregado por el encargado de la seguridad informática o por el técnico designado.
- Los disquetes que se utilicen deberán ser previamente revisados por el producto antivirus autorizado.

-  Se debe llevar un libro de incidencias donde deben plasmarse las irregularidades que pueden ser provocadas por la presencia de un virus informático, así como los mantenimientos realizados
-  Controlar los accesos a internet u otras redes
-  Debe llevarse un registro de acciones realizadas por los operadores.
-  Solo el personal autorizado debe tener acceso a la información confidencial.

2.2.3. Área de Personal

-  El personal que trabaje con el equipamiento informático deberá estar previamente capacitado y en plenitud de sus capacidades físicas y mentales acorde con las funciones que desempeñe, además de encontrarse bien identificado con los principios y políticas de la institución.
-  El personal debe mantenerse actualizado de las regulaciones establecidas en este manual de Seguridad Informática.

Reclutamiento y selección de técnicos

-  Practicarle exámenes psicológicos y médicos para considerar los valores sociales y en general su estabilidad su actitud y comportamiento bajo presión.
-  Averiguar exhaustivamente sus antecedentes de trabajo antes de contratarlo.

Administración del personal del área de informática.

-  Debe considerarse la presentación del manual de seguridad en el programa de inducción para el personal del área de informática.

- Las vacaciones del personal deben programarse al inicio de año.
- Las fechas y distribución turnos para vacaciones deberán tener aprobación del encargado de seguridad informática.
- El jefe del área de informática es el responsable de que para todos los puestos dentro del área, exista al menos dos personas capacitadas para desempeñarlo
- El jefe de informática deberá contar con un expediente alterno en caso de que algún elemento presente problemas en el desempeño laboral por cualquiera que sea el motivo, si no, deberá solicitarlo a recursos humanos.
- Para todo software nuevo o adquisición de equipo, deberá programarse una capacitación antes de utilizarlo.
- Se prohíbe al personal realizar acciones que estén fuera de los límites de sus labores normales, sin previa autorización del jefe de informática y del encargado de la seguridad.
- Si algún miembro necesita un permiso especial para estudiar, este deberá ser aprobado en primera instancia por el responsable de la seguridad informática, y luego presentarse a consideración del jefe de informática y de recursos humanos.

2.2.4. Elementos Técnicos

- Reportar al Responsable de Seguridad Informática cualquier anomalía en el funcionamiento de los programas o del equipamiento.
- Las salvaguardas de los sistemas instalados y las salvaguardas de datos se mantendrán separados del resto de los soportes, los cuales serán debidamente identificados por sistema.

- Los disquetes entregados a los especialistas y técnicos para su uso serán debidamente controlados.
- Los disquetes de uso diario deben permanecer separados y se tendrá en cuenta sea revisado por el programa antivirus actualizado.
- Los disquetes serán controlados, por el Responsable de Seguridad Informática, con etiquetas de identificación según corresponda
- Los respaldos de los sistemas diarios se realizan alternativamente en diferentes disquetes habilitado para este propósito.
- Los respaldos de sistemas que por su tamaño lo requieran serán salvadas en disco duro y en disco zip.
- Los disquetes e informaciones clasificada serán controlados y conservados por el responsable de la seguridad.
- Para utilizar disquetes de salva de información clasificada para otros usos debe ser borrado físicamente con métodos de no-recuperación de la información
- Los programas deben ser operados por los usuarios debidamente capacitados y adiestrados para ello, los que, además, garantizarán la salva de la información en disquete.
- La recepción y transmisión de datos entre redes se harán utilizando el correo electrónico de la empresa y las claves de acceso solo podrán ser de conocimiento del personal responsabilizado para ello (son intransferibles), además una copia de los mensajes que entran y salen de la empresa el sistema de correo lo deposita en

un usuario configurado como postmaster que en este caso es el responsable de seguridad Informática.

-  No se podrá trabajar con disquetes que no se hayan chequeado previamente.
-  El personal que requiera el uso de las máquinas tienen que adiestrarse adecuadamente antes de utilizar las mismas.
-  Se tendrá control específico de los recursos informáticos por parte del jefe del área con equipos instalados.
-  Se chequeará periódicamente los soportes magnéticos y discos duros con programas afines a esto como (scandisk, ndd...) para evitar almacenamiento de información en sectores erróneos.
-  Se conservará solamente la información que sea necesario ser controlada y consultada en un periodo determinado.
-  Instruir los operadores y demás usuarios de las máquinas en los procedimientos de respaldo de cada sistema en explotación.
-  Instruir a los operadores y demás usuarios de la máquina en la forma de encender y apagar los equipos.
-  Instruir a los operadores y demás usuarios en el trabajo de las máquinas en red
-  Las operaciones incorrectas que se ejecuten en las máquinas y que traigan como consecuencia la pérdida de la información parcial o total, serán objeto de análisis por una comisión integrada por: Responsable de Seguridad Informática, Jefe del área, Funcionario de Seguridad y protección.

-  Hacer saber a todo el personal que está autorizado a trabajar con las máquinas que tiene él deber de cumplir con las medidas de seguridad informática que le correspondan.
-  Se deben mantener copias de los sistemas utilizados en disco flexibles para garantizar la continuidad del procesamiento en caso de problemas en el disco duro donde se encuentren cargados.
-  Se debe tener otra copia de la salvo de los datos de los sistemas utilizados en el área del mes anterior, trimestre, semestre de la información si es acumulativo, en caso de que el disco flexible donde esté la última salva tenga problemas.
-  Realizar salvaguarda de sistema de información confidencial luego de terminado el procesamiento.
-  Llevar el Libro de Incidencia donde se plasmen todas las irregularidades de seguridad reportadas, así como las acciones tomadas.(VER ANEXO 4)

2.2.5. Elementos Administrativos

-  El responsable de la actividad de Seguridad Informática es el Jefe de Informática, el que establece las relaciones con todo el personal afín con medios informáticos, para la exigencia del cumplimiento de las medidas de seguridad.
-  El responsable de Seguridad Informática exigirá a todos los Jefes de áreas con equipos informáticos instalados, admón. etc. Por el cumplimiento de todo lo expuesto en este manual.

-  Los administrativos del área, no permitirán la entrada de ningún personal ajeno a las áreas donde existan equipos de computación.
-  Se establecerá como parte del contenido de trabajo de los operadores y demás usuarios de los medios de computación, el cumplimiento de las medidas de Seguridad Informática.
-  La prioridad en la información la tendrá la que por sus características de contenido deba ser procesada, garantizando siempre su confidencialidad, integridad y disponibilidad.
-  Todas las puertas de la oficina serán cerradas con llave al salir el último miembro del personal.
-  Se tendrá control específico de los recursos informáticos por parte del jefe del área con equipos instalados.

2.2.6. Área de Auditoria

-  Verificación mensual de cumplimiento de políticas
-  Verificación trimestral de las condiciones de seguridad.
-  Realizar una evaluación de los riesgos actuales al inicio de cada año y presentar un informe que incluya conclusiones y recomendaciones con copia a: el encargado de seguridad informática el jefe del área de informática y el representante de la alta dirección.

-  Se deben realizar mensualmente una verificación física del uso computadoras, software instalado contra el autorizado y presentar reportes obtenidos al encargado de la seguridad informática.
-  Se deben monitorear mensualmente el uso que se les está dando a las computadoras
-  Se deben hacer auditorias trimestrales sobre el área de operación y la utilización de la tecnología de información.

2.2.7. Plan de Contingencia

Las acciones de recuperación disponible a nivel operativo pueden ser algunas de las siguientes:

-  En algunos casos es conveniente no realizar ninguna acción y reanudar el proceso.
-  Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.
-  El procesamiento anterior complementado con un registro de las transacciones que afectaron a los archivos permitirá retroceder en los movimientos realizados a un archivo a punto de tener la seguridad del contenido del mismo a partir del reanudar el proceso.
-  Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia.

- Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia deberá ser planeado y probado previamente.

2.3. NORMAS E INSTRUCCIONES PARA EL RESGUARDO DE LOS DOCUMENTOS

2.3.1. INTRODUCCIÓN:

No debemos olvidar que en un mundo globalizado, como el que vivimos, la información es un recurso que tiene un valor incalculable y es de importancia crítica, y vital para el funcionamiento y competencia de toda organización sea esta productiva o de servicio.

Una de las principales preocupaciones de los administradores de sistemas y de los responsables de la seguridad informática, es que el usuario, en la generalidad desconoce la inseguridad que priva cuando se realiza el envío, recepción de información y durante el manejo de ella, tanto si están representados en papel como electrónicamente.

Con la definición de la siguiente normativa e instrucciones, es posible decidir que información debe ser protegida y que medidas, de acuerdo con la necesidad de protección, se deben observar.

Por lo que se reconocerán tres categorías de protección, además de los correspondientes criterios a aplicar, así como los controles, las reglas y las instrucciones de manejo.

2.3.2. TIPOS DE DOCUMENTOS

Se reconocerán y se denominarán “documentos” en el sentido de esta normativa a todos los soportes de información tales como: reportes, manuscritos, documentos, manuales, dibujos, gráficos y microfilm. También se incluirán los soportes de datos magnéticos y óptico Ej. tarjetas magnéticas, discos fijos o móviles y discos flexibles, en este caso el concepto de documentos se limita al conjunto de datos almacenados en ellos.

Asimismo deberán ser tratados como originales y conforme a su clasificación, documentos tales como borradores, textos taquigrafiados y esquemas, así como los soportes utilizados(papel carbón, cintas mecanográficas, entre otros)

2.3.3. CLASIFICACIÓN Y DEFINICIÓN DE LAS CATEGORÍAS

Se establece tres categorías para el manejo de los documentos, los cuales se clasifican de acuerdo a la información contenida así:

a) SOLO PARA “USO INTERNO”

Aquí se reconocen aquella información cuyo uso pertenece a un gran número de usuarios estrictamente de la institución, cuya publicación a entes externos puede acarrear, perjuicios para la institución.

b) SOLO PARA “USO LIMITADO”

El uso limitado de esta información esta determinado por el jefe de la instancia que la genera, la publicación indebida de esta información, puede afectar el logro de las metas y objetivos de la organización.

c) SOLO PARA “USO CONFIDENCIAL”

Información oficial confidencial o clasificada, es la que posee o genera el organismo, que requiere de medidas de protección definida por la ley, por contener datos o información cuyo conocimiento o divulgación no autorizada puedan ocasionar daños o entrañar riesgos a la organización o institución.

**2.3.4. MANEJO DE DOCUMENTOS DE LA
CATEGORÍA “SOLO PARA USO INTERNO”**

Ejemplo de documentos:

- . Indicaciones para actividades cotidianas

- Listas telefónicas internas
- Metas y Objetivos de la Institución
- Planificaciones organizativas
- Manuales Internos
- Circulares Internas
- Instructivos, memorandos, y notas
- Datos Generales sobre los empleados

Identificación/Clasificación

Los documentos deberán ir etiquetados con la inscripción “Solo para Uso Interno” en primera plana. Se puede prescindir de tal inscripción cuando la limitación al uso interno es obvia, por Ej.: en el caso de actas de reuniones internas.

Distribución:

La distribución y reparto solo puede efectuarse, dentro de la institución y a dependencias de esta.

Envío y transmisión:

En caso de envío de documentos a una oficina dependiente de la institución está deberá hacerse en un sobre con el logotipo de la institución.

Anulación/Destrucción

Dentro de las posibilidades deberá haber una persona o los responsables de generar la información que deberán romper los documentos y depositarlo en la papelera o en un deposito destinado para reciclaje. Cuando se trate de soportes de datos magnéticos u ópticos la anulación se dará por medio de borrado físico de la totalidad de la información.

2.3.5. MANEJO DE DOCUMENTOS DE LA CATEGORÍA “SOLO PARA USO LIMITADO”

Ejemplo de documentos:

- Información de los usuarios
- Información estadística para toma de decisiones
- Datos sobre sueldos de los altos niveles
- Comunicación sobre salarios
- Evaluaciones de personal
- Elaboración de Software (código fuente)

Identificación/Clasificación

Los documentos deberán ir etiquetados con la inscripción “Solo para Uso Limitado” en primera plana del documento. No deberá reproducirse tal información, salvo que el encargado de producirla lo autorice para los fines establecidos previamente.

Distribución:

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

La distribución y reparto solo procederá de manera limitada, esto significa que podrá entregarse a aquellas personas para quienes se produjo la información y que en el marco de sus tareas harán uso de ella.

Envío y transmisión:

En caso de envío de documentos a una oficina dependiente de la institución está deberá hacerse en un sobre con el logotipo de la institución. Y con la inscripción “Solo para uso limitado”.

Anulación/Destrucción

Dentro de las posibilidades deberá haber una persona o los responsables de generar la información que deberán romper los documentos y depositarlo en la papelería o en un depósito destinado para reciclaje. Cuando se trate de soportes de datos magnéticos u ópticos la anulación se dará por medio de borrado físico de la totalidad de la información.

2.3.6. MANEJO DE DOCUMENTOS DE LA CATEGORÍA “SOLO PARA USO CONFIDENCIAL”

Ejemplo de documentos:

- Alteraciones de la dirección y de la política de la institución antes de su publicación oficial.
- Planificaciones Económicas y Presupuestarias
- Informes sobre situaciones críticas de la institución

- Informaciones del mismo grado de confidencialidad referente a terceros y que por su competencia maneje la institución
- Planificaciones tecnológicas y estratégicas

Identificación/Clasificación

Los documentos deberán ir etiquetados en primera plana con la inscripción “Documentación Confidencial Restringida”. Además se incluirá la leyenda “Prohibida su reproducción”.

Distribución:

La distribución y reparto procederá de manera limitada, a las personas designadas y que por la naturaleza de la información solo puede ser conocida por ellas, es necesario contar con una lista de distribución o de acceso a estos documentos.

Envío y transmisión:

En caso de envío de documentos, esta deberá hacerse en sobre cerrado y sellado con el logotipo de la institución y con la leyenda “Abrir solo personalmente”. Queda prohibida su transmisión por medio de aparatos de FAX.

Conservación:

Los documentos deberán guardarse bajo llave. No deben quedar nunca a la vista y desatendidos. El acceso a documentos archivados electrónicamente deben estar protegidos.

Anulación/Destrucción

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

La anulación o destrucción de esta clase de documentos será de forma segura, lo realizará la persona designada por el autor o editor de la información.

2.3.7. OBSERVACIONES A LA CLASIFICACIÓN

Generalidades

Las descripciones que identifican cada categoría deben figurar en lugares visibles. Si se trata de soportes de datos magnéticos u ópticos es aconsejable que también figure en la funda o en el cuerpo de los mismos. Cuando el documento conste de varias partes con categorías diferentes, el conjunto poseerá la categoría más utilizada.

Cuando se da a conocer un documento públicamente, es necesario estar seguro de que no se está dando a conocer en forma negligente información susceptible de protección.

Responsabilidad

Cada documento deberá ser codificado por el autor o editor del mismo. La clasificación se rige según el valor y el significado de la información para la institución.

El autor o editor y el receptor son, por tanto, responsables en la misma medida, de que los documentos confidenciales de la institución sean manejados con una diligencia especial.

Utilización de la inscripción “Personal”

Independientemente de la categoría, se puede emplear, en documentos destinados a una persona concreta, la inscripción “Personal” o “Abrir solo personalmente”. De este modo se deje claro, que en ningún caso deberá obtener esa información, cualquier persona

ajena a la mencionada en el documento. Este tipo de inscripciones pueden evitar demoras innecesarias, el remitente deberá asegurarse de la presencia personal del destinatario, especialmente cuando se trata de documentos que establezcan un plazo.

Cuando no sea posible proceder de este modo, es aconsejable hacer uso de la inscripción “Personal o representante” para darle la oportunidad de abrir el correo entrante a una persona delegada oficialmente por el destinatario.

Reserva del derecho de autor

Los documentos están protegidos jurídicamente, ante una utilización indebida no autorizada (por Ej. reproducción), gracias al derecho de autor.

PARTE III

ACCIONES ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN COMPUTARIZADA

Un sistema de cómputo es seguro si se puede confiar en el, si su software se comporta como se espera que lo haga, y si la información almacenada en el se mantiene inalterable y accesible durante tanto tiempo como su dueño lo desee.

Sobre este aspecto, la seguridad busca consolidar la confidencialidad, integridad, autenticidad y disponibilidad de la información. De igual forma, la seguridad informática busca mantener y conservar la operatividad de la institución y de su

sistema a partir del resguardo de sus recursos.

Confidencialidad

Un sistema de computo no debe permitir que la información contenida en él sea accesible a nadie que no tenga la autorización adecuada.

Integridad y Autenticidad

Un sistema de cómputo no debe permitir modificaciones no autorizadas a los datos o la información contenida en el. Este punto comprende cualquier tipo de modificaciones:

- ◆ Por errores de hardware y/o software.
- ◆ Causadas por alguna persona de forma intencional
- ◆ Causadas por alguna persona de forma accidental

La autenticidad se maneja en cuestión de telecomunicaciones, e implica disponer de un medio para verificar quien envía la información, así como el poder comprobar que los datos no fueron modificados durante su transferencia.

Disponibilidad

La información puede estar sana y salva en el sistema, pero de poco sirve si los usuarios no tienen acceso a ella. La disponibilidad significa que los recursos del sistema. Tanto de hardware como de software, se mantendrán funcionando de forma eficiente, y que los usuarios lo podrán utilizar en el momento que lo necesiten. También significa que el sistema sea capaz de recuperarse rápidamente en caso de ocurrir un problema de cualquier especie.

3.1. OBJETIVOS DE LAS MEDIDAS DE SEGURIDAD

Pueden ser vistos como una serie de niveles de control: si un nivel falla

entonces otro nivel toma posesión u ocupa su lugar y continua con la

operación del sistema, de forma que el impacto global que pudiera ocasionar la falla se reduce. Estos objetivos son:

1. **Disuadir.** En este nivel la meta es prevenir cualquier tipo de amenaza o desastre que pueda ocurrir.
2. **Detectar.** La disuasión total generalmente no se consigue; por lo tanto en este nivel se establecen métodos de monitoreo y vigilancia que reporten cualquier riesgo o peligro y que permitan tomar las acciones correctivas pertinentes.
3. **Minimizar el impacto de pérdida o desastre.** Si un accidente o contratiempo

ocurre, deben establecerse procedimientos que ayuden a reducir la pérdida o daño.

4. **Investigar.** Si la pérdida ocurre, puede realizarse una investigación que ayude a determinar lo que pasó. La información que derive de esta investigación puede servir para futuras planeaciones de seguridad.
5. **Recuperar.** Las medidas de seguridad implican que debe de haber un plan de acción para recuperación en caso de que un accidente o desastre ocurra, sea cual fuera su causa, y hacerlo de la manera mas pronta posible.

3.2. CONSIDERACIONES SOBRE SEGURIDAD

La seguridad en informática cuesta dinero y, sobre todo, esfuerzo.

Es posible obtener en general ciertos niveles mínimos de seguridad sin hacer un gasto considerable. Pero el logro de protección adicional requiere niveles de

gastos más altos y, con frecuencia, retribuciones menores. La economía siempre resulta necesaria y es importante asegurarse de que existen una relación costo / beneficio razonable con respecto a las medidas de seguridad.

Para ello es necesario establecer prioridades. Entre éstas tenemos:

¿ Que se quiere proteger?

Es muy importante determinar el valor del hardware y las tareas que realiza, (que tan importante es para la institución en que se está trabajando). Esta valoración debe hacerse de forma individual, pues lo que es valioso para algunos no lo es para otros.

¿ Contra que se quiere proteger?

Para no incurrir en gastos innecesarios, es importante determinar cuales son los riesgos reales a los que están expuesto el equipo de cómputo.

La seguridad efectiva debe garantizar la prevención y detección de accidentes, ataques, daños por causas naturales, así como la existencia de medidas definidas para afrontar desastres y lograr el restablecimiento de las actividades.

¿ Cuanto tiempo, dinero y esfuerzo se está dispuesto a invertir ?

Se refiere a la cantidad de recursos que dispone o que está dispuesta a invertir la

institución, lo que determinará en última instancia las medidas que se van a tomar.

Estos recursos son:

Tiempo. Para tener un nivel de seguridad alto es necesario que alguien dedique tiempo a configurar los parámetros de seguridad del sistema, el ambiente de trabajo de los usuarios, revisar y fijar los permisos de acceso a los archivos, ejecutar programas de monitoreo de seguridad, revisar las bitácoras del sistema, etc.

Esfuerzo. Establecer y mantener un nivel adecuado de seguridad puede significar un esfuerzo considerable por parte del encargado sobre todo si ocurren problemas de seguridad.

Dinero. El tener a alguien que se encargue de la seguridad en forma responsable cuesta dinero. De igual forma cuesta dinero adquirir los productos de seguridad que se vayan a utilizar, ya sean programas o equipos.

Es importante también analizar los costos que tendría la pérdida o acceso no autorizado a la información. Dependiendo de esto, y en el caso de que alguien tenga acceso no autorizado,

el efecto pueden ser pérdidas monetarias o poner en peligro la seguridad nacional, solo como ejemplos drásticos.

Debido a lo anterior, las consideraciones que deben tomarse en cuenta al planear la seguridad son:

- ◆ Formulación de medidas necesarias para lograr un nivel de seguridad adecuado, es decir en equilibrio con los niveles de riesgo.
- ◆ Justificación de las medidas de seguridad en cuanto al costo que representa.

Se debe tomar en cuenta que es prácticamente imposible hacer que un sistema sea totalmente seguro, debido a que no se puede prever todas las

posibles amenazas aun cuando la seguridad se incremente a niveles muy altos, ya que siempre habrá una manera de obtener acceso no autorizado.

Para determinar la seguridad con la que debe contar el área de informática se debe considerar las siguientes áreas:

- a) Seguridad Física
- b) Seguridad Lógica y Confidencialidad
- c) Seguridad en el Personal
- d) Elementos técnicos y procedimientos
- e) Elementos Administrativos
- f) Participación de la auditoria
- g) Plan de Contingencia

3.3. ACCIONES PARA LA SEGURIDAD FÍSICA

La importancia de la seguridad física se reconoció desde hace mucho tiempo, pero resulta ser el área que menos atención tiene. En la situación actual existe protección inadecuada.

Dentro de los puntos más importantes que se deben cubrir se encuentran los siguientes:

- ◆ Ubicación física y disposición del centro de cómputo
- ◆ Instalación física del centro de cómputo u área de informática
- ◆ Control de acceso físico
- ◆ Aire acondicionado
- ◆ Instalación eléctrica
- ◆ Riesgo de inundación
- ◆ Protección, detección de incendios.
- ◆ Mantenimiento

Medidas para la ubicación física y Disposición del Centro de Computo o Área de informática.

La sala donde se ubican los equipos principales de proceso de datos debe dotarse de medidas de seguridad, acordes con los las características del equipo a proteger, su valor y su importancia.

La selección de la ubicación del Centro de Cómputo o Área de informática debe realizarse buscando la parte más conservadora y clandestina la cual debe estar lejos del área de tránsito de gran escala, tanto terrestre como aéreo, también lejos de equipos eléctricos tales como radares y equipos de microondas, etc. El objetivo es mantenerlo tan lejos como se pueda de cualquier tipo de amenaza.

En la medida de lo posible, el centro de cómputo no debe de contener señal alguna que lo identifique como tal ante la gente externa.

Entre los aspectos que se deben tomar en cuenta están: la planeación de la distribución física del equipo de cómputo, los riesgos concernientes a desastres naturales, inundaciones, fuego, fallas eléctricas, polvo, etc., así como la

luz solar, si la exposición es muy fuerte, debe evitarse el uso del vidrio; en los casos que no sea posible, pueden utilizarse persianas externas,

Partiendo de que la estructura del inmueble está hecha con capacidad y estabilidad, es conveniente considerar los tipos de riesgos o conflictos que presentan cada uno de los niveles. Tomando en cuenta los factores inherentes del local podemos determinar estos riesgosos conflictos en los diferentes niveles de un inmueble.

ACTIVIDAD	NIVEL			
	ALTO	INTERMEDIO	BAJO	SÓTANO
Acceso de máquinas	G	M	P	P
Acceso de elemento de trabajo	G	M	I	P
Carga del suelo	G	M	P	I
Filtraciones de agua	G	P	P	P
Inundación	I	P	M	G
Sabotaje	P	G	G	P

Tipo de riesgo: G = Grave M =Mediano P = Poco I = Inexistente

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Los suelos sometidos a vibraciones o la proximidad de maquinaria pesada o de vías de comunicación (ferrocarriles, puentes, etc.) pueden ocasionar daños en los discos, por el peligro del “aterrizaje” de los cabezales de lectura grabación. Por otro lado, hay que considerar la resistencia del suelo en instalaciones grandes, para evitar el riesgo de hundimientos de la estructura por sobrecarga.

En los sitios donde la información es altamente sensitiva se debe tomar en cuenta también el riesgo producido por las emanaciones electromagnéticas o acústicas del hardware, ya que éstas pueden ser interceptadas con relativa facilidad en una distancia menor a los 300 metros. Para ello, la opción es la separación de los dispositivos de los puntos potenciales de interrupción.

Consideraciones para las Instalaciones físicas del centro de cómputo

La construcción o selección del lugar es un factor determinante en el correcto funcionamiento de un centro de cómputo ya que de ella depende la mayor protección y seguridad de uno de los elementos más importantes de cualquier organización.

En la selección del local se deben considerar dos alternativas:

a) Tener la oportunidad de seleccionar todo; es decir, que considerar todas las cuestiones del medio ambiente externo que rodean el inmueble, de tal forma

que la ubicación del local destinada al equipo de cómputo sea el lugar más idóneo.

Aquí se realiza el estudio desde la localización que consiste en determinar el lugar adecuado donde sean favorables los factores naturales, de servicios y de seguridad. Estos factores se derivan de la importancia que tienen la seguridad en un centro de cómputo para salvaguardar los recursos que garantizan el funcionamiento de cualquier

organización ya instalada en el sitio o lugar seleccionado.

b) Adecuarse a lo que se tiene, lo que se da o lo que se impone: cuando en la organización ya se tenga destinado el local o espacio físico y no hay otra alternativa, se deben realizar los arreglos necesarios para la instalación. De esta forma, en base las modificaciones necesarias para la instalación del sistema y se tomarán todas las medidas correspondientes

para evitar cualquier riesgo o percance.

Para determinar si se cuenta con un buen local debemos de tener en cuenta los aspectos físicos y sus requerimientos: entre los factores a considerar están:

1. Factores inherentes a la localidad

Son aquellas condiciones del medio ambiente externo que rodean al local. Se dividen en:

Naturales: Se está expuesto a múltiples peligros cuya ocurrencia está fuera del control del hombre, como es el caso del frío, el calor, las lluvias, los sismos y el peligro del terreno (como el hundimiento del piso). Para prevenir los desastres de tipo natural se necesita una buena elección del lugar en el que se va a situar el centro, y una planificación cuidadosa de la

distribución y materiales, además de realizar un plan de recuperación. Es necesario consultar a una persona capacitada que asegure que el edificio soportará el peso de las máquinas.

Servicios: Considerar que la zona a seleccionar cuente con los servicios básicos, así como los que se requieren para el funcionamiento del lugar, que se encuentren disponibles y operen eficientemente. Entre los factores a considerar tenemos las líneas

telefónicas, la energía eléctrica, el drenaje, las facilidades de comunicación, antenas de comunicación y líneas para enlace radioeléctricas.

Seguridad: se base en que la zona sea tranquila, que no esté expuesta a riesgos de alto grado, que no sea un lugar desolado o desprotegido. También se debe prever que alrededor del edificio no existan fuentes que propicien incendios fácilmente. Se

debe considerar también el peligro de inundación, por lo que es necesario ver los niveles de la calle contra los niveles del edificio, de tal manera que estos últimos sean punto en el que desemboque los demás y que las avenidas donde se encuentre el local no estén propensas a ser ríos de agua. Entre otros factores tenemos el vandalismo, el sabotaje y el terrorismo.

2. Factores inherentes al centro de cómputo o Área de informática

La construcción del interior de la instalación de cómputo También tiene gran importancia. La división tradicional de las áreas, casi nunca es la más adecuada para la seguridad. Muchas veces las losas de los techos, catalogada como inflamable, es combustible, y las divisiones a pruebas de incendios no son las adecuadas, para algunas áreas como la biblioteca de computación.

Es importante considerar las características físicas que deben tener

las instalaciones para proporcionar seguridad. Entre los factores que encontramos están:

a) Piso falso

Se debe tener en cuenta la resistencia para soportar el peso del equipo y el personal. Entre otras consideraciones están:

- ◆ Sellado hermético
- ◆ Modularidad precisa, que los cuadros ensamblen perfectamente
- ◆ Nivelado topográfico

-
- ◆ Posibilidad de realizar cambios en la situación de unidades
 - ◆ Aterrizado para evitar cargas electrostáticas
 - ◆ Debe cubrir los cables de comunicación entre la unidad central de proceso y los dispositivos periféricos, cajas de conexiones y cables de alimentación eléctrica.
 - ◆ Deberá proporcionar seguridad al personal
 - ◆ Debe permitir que el espacio entre los dos suelos actúe como una cámara plena de aire, que facilite el reparto de cargas.
 - ◆ La altura recomendable será de 30 centímetros si el área de la sala de computo es de 100 metros cuadrados o menos, y de 40 a 60 centímetros si es mayor de 100 metros cuadrados. La altura mínima podrá ser de 18 centímetros si la sala es pequeña. Todo lo anterior es con objeto de que el aire acondicionado pueda fluir adecuadamente en la cámara plena.
 - ◆ Puede ser de acero, aluminio o madera resistente al fuego.
 - ◆ El mejor piso deberá estar soportado por pedestales o gatos mecánicos.
 - ◆ Cuando se utilice como cámara plena para el aire acondicionado, tendrá que cubrirse el piso firme con pintura antipolvo.
- b) Cableado**
- El cableado en el cuarto de computadoras se debe procurar que quede por debajo del piso falso, donde es importante ubicar los cables de forma que se aparten:
- ◆ Los cables de alto voltaje para la computadora
 - ◆ Los cables de bajo voltaje conectados a las unidades de las computadoras .
 - ◆ Los cables de telecomunicación
 - ◆ Los cables de señales para dispositivos de monitoreo o
-

detección (fuego, temperatura, humedad, etc).

puertas y ventanas de otras dependencias.

c) Paredes y techo

- ◆ Las paredes irán con pintura plástica lavable para poder limpiarlas fácilmente y evitar la erosión.
- ◆ El techo real deberá pintarse, así como las placas de falso techo y los amarres, si éste se emplea como plenum para el retorno del aire acondicionado.
- ◆ Es mejor usar placas metálicas o de madera prensada para el piso falso con soportes y amarres de aluminio.
- ◆ La altura libre entre el piso falso y el techo falso debe estar entre 2.70 y 3.30 metros para permitir la movilidad del aire.

d) Puertas de acceso

- ◆ Las puertas del local serán de doble hoja y con una anchura total de 1.40 a 1.60 cm.
- ◆ Es necesario una salida de emergencia.
- ◆ Tener en cuenta las dimensiones máximas de los equipos si hay que atravesar

e) Iluminación

- ◆ Los reactores deben estar fuera de la sala, ya que generan campos magnéticos, o en su caso deben aislarse.
- ◆ La iluminación no debe alimentarse de la misma acometida que los equipos de cómputo.
- ◆ En el área de máquinas deben mantenerse un promedio mínimo de 450 luces a 70 cm del suelo.
- ◆ Debe evitarse la luz directa para poder observar la consola y las señales.
- ◆ Del 100% de la iluminación, deberá distribuirse el 25% para la iluminación de emergencia y se conectará al sistema de fuerza ininterrumpible.

f) Filtros

- ◆ Se requieren filtros con una eficiencia del 99% sobre partículas de 3 micrones
- ◆ Si hay contaminantes, elegir los filtros adecuados.

- ♦ El aire de renovación o ventilación será tratado tanto en temperatura y humedad como en filtrado antes de entrar en la sala.
- ♦ Son recomendables los tipos de humificaciones de vapor.

g) Vibración

Si hay vibraciones superiores a las normales, es necesario estudiar antes de colocar los equipos y utilizar los dispositivos antivibratorios necesarios, ya que la vibración podría dañar el equipo.

h) Ductos

- ♦ Serán de material que no desprenda partículas con el paso del aire.
- ♦ No deberán tener revestimientos internos de fibras.

Otro punto fundamental para el desarrollo de una buena seguridad en el centro de cómputo es el acondicionamiento:

3. Acondicionamiento del local

Consiste en realizar las modificaciones necesarias a la planta o espacio que se ha asignado para la ubicación del equipo de cómputo. Se deben prever aspectos como dimensiones de puertas de acceso, situación de columnas, elevación de paredes, etc. El acondicionamiento inicia con la distribución del espacio tomando en cuenta la eficiencia operativa y la seguridad de la información.

Para adecuar el local a los requerimientos del centro de cómputo se deben distribuir los espacios del local de acuerdo a las necesidades.

Necesidades de espacio

Se determinan por las especificaciones técnicas de los equipos, las cuales se encuentran en el material que el proveedor debe proporcionar cuando se adquiera el equipo; también se deben tener en cuenta las áreas adyacentes para cinto teca, discoteca, archivo, servicio, etc.

El espacio debe tener forma y tamaño adecuado. Es preferible evitar las áreas de formas extrañas; por lo general, las mejores son las formas rectangulares. Debe considerarse la situación e columnas, con el fin de que

éstas no estorben y que el espacio se pueda adecuar de la mejor forma en el momento de realizar la distribución en la planta. Es aconsejable calcular al considerar la adaptabilidad en el mismo.

Las futuras necesidades significan algo más que sólo reservar un espacio mayor que el adecuado para las necesidades actuales. Debe tenerse presente el dónde y el cómo de los futuros cambios que alteran las cualidades y necesidades de espacio.

Distribución en Planta

Consiste en la ubicación de los equipos y elementos de trabajo en un plano de distribución en el cual se realizan pruebas –tantas como sean necesarias-, de tal forma que se vean todas la alternativas y se tomen aquéllas que sean las más adecuadas.

Para delimitar el plano de distribución es necesario hacer uso del catálogo de planos de la organización, ya que éstos constituyen una gran ayuda para determinar y conocer la ubicación de los distintos aspectos que son de suma importancia en el centro de cómputo.

Los planos que se deben considerar son los civiles y arquitectónicos, lo cuales incluyen:

- ◆ Planos de plantas: en él se localizará la planta en que se encontrará el centro de cómputo, y especifica las distribuciones de paredes, largo y ancho del lugar, ventanas, puertas, columnas, etc.
- ◆ Plano de memoria de cálculo: permite conocer la capacidad que tiene el edificio para soportar cada planta.
- ◆ Plano de corte hidráulico: con él se conocen las tomas de agua, la distribución de tuberías, los desagües, etc.
- ◆ Plano de corte sanitario: establece el paso del drenaje.
- ◆ Plano de teléfono: especifica donde se encuentran las líneas telefónicas.
- ◆ Planos de seguridad: en él se indican las salidas de emergencia, así como las vías de desalojo, colocación de mangueras y extintores, timbres, alarmas, etc.

- ◆ Plano de energía eléctrica: especifica la distribución de la corriente eléctrica.

Por último se debe dibujar el plano de distribución del Centro de computo u Área de informática, el cual debe incluir lo siguiente:

- ◆ Paredes, puertas y ventanas
- ◆ Todas las salidas de emergencia, columnas y pilares.
- ◆ Control y equipo de aire acondicionado
- ◆ Archiveros, escritorios y otros equipos de oficina.

El plano de distribución permite:

- ◆ Estudiar los desplazamientos más frecuentes de los operadores con la finalidad de evitar que se recorran largas distancias.
- ◆ Conocer los requerimientos de cable.
- ◆ Ubicar las diferentes áreas con base en sus actividades y exigencias.

Esta adecuación o acondicionamiento del local tiene como finalidad de proporcionar los servicios y accesorios necesarios para el buen funcionamiento y lograr la máxima eficiencia operativa.

Control de acceso físico

El principal elemento de control de acceso físico involucra la identificación positiva del personal que entra o sale del área bajo un estricto control. Si una persona no autorizada no tiene acceso, el riesgo se reduce.

Los controles de acceso físico varían según las distintas horas del día. Es importante asegurar que durante la

noche sean tan estrictos como durante el día. Los controles durante los descansos y cambios de turno son de especial importancia.

La evolución de los siguientes elementos es necesaria para diseñar los procedimientos de acceso en una instalación de cómputo:

Estructura y disposición del área de recepción.

En las áreas de alta seguridad donde se necesita considerar también la posibilidad de ataque físico se debe identificar y admitir tanto a los empleados como a los visitantes de uno en uno. También se pueden utilizar dispositivos magnéticos automáticos y otros recursos en el área de recepción. Si es necesario usar vidrio en la construcción de esta área, debe ser de tipo reforzado.

Acceso de terceras personas

Dentro de las terceras personas se incluye a los de mantenimiento del aire acondicionado y de computación, los visitantes y el personal de limpieza. Éstos y cualquier otro personal ajeno a la instalación deben ser:

- ◆ Identificados plenamente
- ◆ Controlados y vigilados en sus actividades durante el acceso.

El personal de mantenimiento y cualquier otra persona ajena a la instalación se debe identificar antes de entrar a ésta. El riesgo que proviene de

este personal es tan grande como de cualquier otro visitante.

Identificación del Personal

Algunos parámetros asociados típicamente a la identificación del personal son:

Algo que se porta:

Consiste en la identificación mediante algún objeto que porta tal como, tarjetas magnéticas, llaves o bolsas. Por ejemplo, las tarjetas pueden incluir un código magnético, estar codificadas de acuerdo al color (rojo para los programadores, azul para los analistas, etc.), e inclusive llevar la foto del propietario. Un problema con esta técnica, sin embargo, es la posibilidad de que el objeto que se porta sea reproducido por individuos no autorizados. Es difícil pero no imposible reproducir una tarjeta con código magnético. Es por esta razón que esta técnica se utiliza en conjunción con otros identificadores para proporcionar una identificación positiva.

Algo que se sabe:

Implica el conocimiento de algún dato específico, como el número de empleado,

algún número confidencial, contraseña o combinación, etc.

Algunas características físicas especiales

La identificación se realiza en base a una característica física única. Estas características se dividen en dos categorías:

- ♦ *Neuromuscular*: tales como firma o escritura.
- ♦ *Genética*: tales como la geometría del cuerpo (mano, iris, retina, etc), huellas digitales, reconocimiento de patrones de voz, apariencia facial, impresión de las huellas de los labios, patrones de ondas cerebrales, etc.

Por ejemplo: la utilización de las huellas digitales ha demostrado ser una característica de identificación positiva. Inicialmente se realiza un registro holográfico de las huellas digitales.

Entonces cuando un individuo pone sus huellas en un verificador, éste realiza un nuevo registro a través de una luz láser. Si ambos registros coinciden, el individuo ha sido identificado.

Asimismo pueden utilizarse los siguientes elementos:

1. Guardias y escoltas especiales

Estos pueden estar

ubicados en lugares estratégicos donde exista más vulnerabilidad. Es recomendable que todos los visitantes que tengan permisos para recorrer el centro de cómputo sean acompañados por una persona designada como escolta.

2. Registro de firma de entrada y salida

Consiste en que todas las personas que entren en el centro de cómputo firmen un registro que indique la hora de entrada, el motivo por el que entran, y la hora de salida.

Fecha	Nombre	Procedencia	Depto. Que visita	Persona Que busca	Asunto	Hora De Entrada	Firma	Hora de salida	Firma

Ejemplo de registro de firma de entrada y salida

3. Puertas con chapas de control electrónico

Estos dispositivos pueden funcionar al teclearse un código para abrirla, disponer de una tarjeta con código magnético, o tener implementado algún dispositivo para el reconocimiento de alguna característica física especial tal como la huella digital, la geometría de la mano, etc.

4. Tarjetas de acceso y gafetes de identificación

Puede tratarse de simples gafetes que identifiquen a la persona, hasta tarjetas con código magnético que permiten abrir la puerta. Asimismo, los dispositivos de lectura de las tarjetas pueden ser conectados a un computador que contenga información sobre la identidad del propietario. La autorización puede manejarse individualmente para cada puerta, y

controlar aspectos como la hora y el día de las funciones. De esta forma, la actividad puede monitorearse, y cualquier intento de entrar que no sea autorizado será detectado de inmediato.

5. Entradas de dobles puertas

De esta forma, la entrada a través de la primera puerta deja un área donde la persona queda atrapada y fuera del acceso a las computadoras. Una segunda puerta debe ser abierta para entrar al centro de cómputo.

6. Equipos de monitoreo

La utilización de dispositivos de circuito cerrado de televisión, tales como monitores, cámaras y sistemas de intercomunicación conectados a un panel de control manejado por guardias de seguridad. Estos dispositivos permiten controlar áreas grandes, concentrando la vigilancia en los puntos de entrada y salida principalmente.

7. Alarmas contra robos

Todas las áreas deben estar protegidas contra la introducción física. Las alarmas contra robos, las armaduras y el blindaje se deben usar hasta donde sea posible, en forma discreta, de manera que no se atraiga la atención sobre el hecho de que existe un dispositivo de alta seguridad. Tales medidas deben aplicarse no sólo al área de cómputo, sino también a las áreas adyacentes. La construcción de puertas y ventanas deben recibir especial atención para garantizar su seguridad.

8. Trituradores de papel

Los documentos con información confidencial nunca deben ser desechados en botes de basura convencionales. En muchos casos los espías pueden robar la información buscando en estos lugares. Es por ello que dichos documentos deben ser desmenuzados o triturados antes de desecharlos.

Existen dispositivos que desintegran el papel convirtiéndolo en pedacitos o confeti, los cuales no pueden ser reconstruidos.

Aire acondicionado

En todas las instalaciones existen grandes problemas con el aire acondicionado; el riesgo que éste implica es doble:

- ♦ El aire acondicionado es indispensable en el lugar donde la computadora trabaja; las fluctuaciones o los desperfectos de consideración pueden

ocasionar que la computadora tenga que ser apagada.

- ♦ Las instalaciones de aire acondicionado son una fuente de incendios muy frecuente, y también son muy susceptibles al ataque físico, especialmente a través de los ductos.

Para poder afrontar estos riesgos se requiere lo siguiente:

- ◆ Se deben instalar equipos de aire acondicionado de respaldo donde ya se hayan establecido las aplicaciones de alto riesgo. En centros de cómputo grandes, los intercambiadores de calor y torres de enfriamiento están a menudo ubicadas en las azoteas, y dentro del cuarto de computadoras estarán las tuberías, válvulas, bombas, unidades de enfriamiento, y otros equipos relacionados. También es recomendable instalar unidades modulares, de forma que los componentes que se puedan reemplazar fácilmente.
- ◆ Se deben instalar redes de protección en todo el sistema de ductos al interior y al exterior.
- ◆ Se deben instalar extinguidores y detectores de incendios en los ductos.
- ◆ Se deben instalar monitores y alarmas para humedad, temperatura y flujos de aire efectivos.

Aún cuando el equipo de aire acondicionado funcione adecuadamente, la habilidad de regular y dirigir el flujo de aire, representa otra dificultad ya que difícilmente alguien trabajará a gusto si la corriente de aire es muy frecuente.

Una gran dificultad que ha surgido con los sistemas de aire acondicionado, en especial en los países cálidos, es el efecto del polvo y de la exposición al sol. Las entradas de aire fresco no deben estar al nivel del suelo y deben colocarse lejos de las áreas donde hay polvo. Deben utilizarse los filtros adecuados para proporcionar aire limpio al centro de cómputo.

Para que se realice una buena instalación del aire acondicionado se debe tomar en cuenta lo siguiente:

1. Capacidad del equipo de aire acondicionado

- ◆ Disipación térmica de las máquinas
- ◆ Disipación térmica de las personas
- ◆ Cargas latentes, aire de renovación
- ◆ Pérdidas por puertas y ventanas
- ◆ Transmisión de paredes, techos y suelo
- ◆ Disipación de otros aparatos
- ◆ Las cargas caloríficas del equipo de cómputo y sus periféricos las proporcionará el proveedor; por lo

común deben especificarse en BTU/horas o en kcal/horas.

- ◆ El proveedor del equipo de cómputo también proporcionará la cantidad de aire que requieran los ventiladores de los diferentes dispositivos de cómputo, por lo regular en pies cúbicos por hora o en metros cúbicos por hora. (Ver Anexo 7)
- ◆ El aire acondicionado para la sala de cómputo deberá ser independiente del aire general del edificio.
- ◆ El calor disipado por los diferentes dispositivos de cómputo, obligan a necesitar aire frío todo el año.
- ◆ La alimentación eléctrica deberá provenir directamente desde la planta de generación de energía eléctrica para emergencia; de ninguna manera deberá conectarse a las salidas de equipos no-breake, ya que el encendido y apagado automático de motores y

compresores ocasionaría una disminución en el voltaje y ruido eléctrico al equipo de cómputo.

2. Distribución del aire en la sala

- ◆ Los componentes de las máquinas se refrigeran, normalmente, mediante la circulación rápida de aire por ventiladores.
- ◆ La entrada de aire se efectúa por debajo de las máquinas a través de las rejillas.
- ◆ El aire caliente es expulsado por la parte superior de las máquinas.
- ◆ Debe considerarse con cuidado el sistema de distribución para eliminar áreas con excesiva velocidad de aire.
- ◆ El aire de renovación o ventilación vendrá en función del volumen de la sala. Se proyectará para obtener de 1.5 a 2 renovaciones por hora y para crear una sobrepresión que evitará la entrada de polvo y suciedad por las puertas, procedentes de las zonas adyacentes.
- ◆ En las zonas contaminadas de aire de renovación deberá descontaminarse previamente,

2.1. Distribución por el techo

Por medio de este sistema:

- ◆ Se impulsa el aire frío por el techo.

- ◆ Se retorna al aire también por el techo a través de rejillas colocadas encima de las salidas de aire caliente.
- ◆ Se tratan menos volúmenes de aire.
- ◆ Tiene poca flexibilidad para cambios de posición de unidades
- ◆ Debe estudiarse para no crear corrientes de aire frío.

2.2. Distribución por el piso falso

De acuerdo con este sistema:

- ◆ El espacio entre el suelo del edificio y el piso falso se utiliza como una cámara plena de aire.
- ◆ Todo el aire de descarga en la sala a través de registros en el suelo.
- ◆ El aire retorna a la unidad acondicionadora por rejillas en el techo.
- ◆ Se necesita una cierta cantidad de recalentamiento para controlar la humedad relativa del aire en el piso falso.
- ◆ Hay que colocar cuidadosamente las rejillas y los

retornos para no crear tiros de aire frío a caliente.

2.3. Dos canalizadores

Es un sistema muy eficaz en el que:

- ◆ Una unidad de controles separados suministra aire y filtrado a las tomas de aire de los dispositivos de cómputo.
- ◆ La otra unidad suministra aire directamente a la sala por canalización diferente y absorbe el resto de la carga de calor (iluminación, personas, etc.).

Instalación Eléctrica

La instalación eléctrica en un centro de cómputo es muy importante, ya que todo el funcionamiento del mismo depende de ella, por lo que una falla en la instalación puede llegar a provocar serios daños al equipo así como detener completamente la operación del mismo.

Es necesario conocer y tener presentes los voltajes de trabajo especificados por los proveedores del equipo de cómputo del equipo de aire acondicionado y del equipo adicional. Para el equipo de cómputo y aire acondicionado se requiere corriente regulada e ininterrumpida.

Corriente regulada

Para el equipo de cómputo o algún otro equipo delicado cuyas tolerancias en las variaciones en los voltajes son mínimas para su adecuado funcionamiento, se requiere contar con un regulador de voltaje.

El regulador está diseñado para trabajar en un rango de voltaje

determinado: si el voltaje que recibe de la compañía suministradora es regular, lo deja pasar hacia la carga, pero si llega con variaciones que están dentro de sus límites de operación, lo eleva o disminuye para dar como salida un voltaje constante que alimenta a la carga siempre y cuando el voltaje de entrada no rebase las tolerancias establecidas por el fabricante del regulador.

En el mercado existen reguladores que aceptan un voltaje de entrada entre 95 y 145 voltios y dan como salida un voltaje de 115 voltios, además de que cuentan con un sistema que los desactiva automáticamente en caso de un sobrevoltaje.

Sistema de corriente ininterrumpida

Es un almacén entre una fuente de energía y una carga que requiere energía precisa sin interrupciones, la cual tiene las siguientes funciones:

- ◆ Regular la cantidad de energía eléctrica que llega al equipo de procesamiento de datos.
- ◆ Proporcionar energía eléctrica continua en caso de ocurrir una falla en el suministro de la misma por parte de la compañía

- ♦ En el caso de que exista una planta generadora de energía, esto le dará tiempo para que alcance su carga plena.

Se pueden considerar los tres tipos de sistemas de corriente ininterrumpida:

Básico

Es el que proporciona energía a un número limitado de dispositivos, incluyendo la unidad de procesamiento y los controladores de los medios de almacenamiento.

El sistema funciona por unos minutos; si la energía no regresa en un tiempo específico, debe salvarse la información y apagar el equipo.

Completo

El sistema de corriente ininterrumpida completo permite que el equipo opere en forma oportuna y ordenada. Requiere que el procesador y los controladores de los medios de almacenamiento estén conectados a él.

Redundante

El tipo redundante utiliza un sistema de corriente ininterrumpida

adicional en caso de que el sistema principal falle. Se utiliza sólo para centros que requieren de gran seguridad, ya que es muy difícil que un sistema de corriente ininterrumpida falle; sin embargo, representa un alto costo el tener dos sistemas funcionando.

Consideraciones en la planeación del uso de este sistema:

- ♦ El tiempo de interrupción en el suministro de energía eléctrica es variable.
- ♦ Proporciona operación continua para un determinado tiempo (al menos el necesario para apagar el equipo oportuna y adecuadamente).
- ♦ El costo de un sistema de corriente ininterrumpida se incrementa de acuerdo al tiempo que es capaz de soportar.
- ♦ Una vez que se ha determinado la necesidad de un sistema de corriente ininterrumpida se debe hacer un estudio para seleccionar el sistema adecuado.
- ♦ Los componentes del sistema de corriente ininterrumpida debe seleccionarse teniendo en mente la modularidad, lo que asegura una periódica y fácil reposición de partes. Entre estos componentes tenemos las

baterías (alcalinas y ácidas), el voltaje y el amperaje (corriente y resistencia) y la conexión en serie y en paralelo. En un centro de cómputo es recomendable conectar en paralelo un banco de baterías adicional con la misma capacidad del principal, para respaldarlo en caso de que éste tenga falla y deje de operar. Cada banco está compuesto por una serie de baterías, conectadas entre sí para proporcionar un voltaje total de operación.

En las especificaciones del proveedor del equipo de cómputo encontramos el tiempo de soporte que requiere cada sistema específico para ser apagado oportuna y adecuadamente en caso de falla en el suministro eléctrico.

La capacidad requerida también está en función del equipo adicional conectado al sistema de corriente ininterrumpida (carga) y a la cantidad de energía que se le suministra.

Para un sistema básico de corriente ininterrumpida, la capacidad de una

batería típica es de 5 a 10 minutos. Para un sistema completo, la capacidad varía dependiendo de los requerimientos, el tamaño de la memoria principal y la configuración del sistema. En las especificaciones del proveedor se encuentra el tiempo de soporte que requiere cada sistema específico.

La capacidad de la batería seleccionada debe tomar en cuenta la reducción de la capacidad causada por el envejecimiento de las baterías y el medio ambiente del lugar. La capacidad inicial instalada de las baterías debe permitirles alcanzar los requerimientos de la carga seleccionada al final de su vida útil. Una persona especializada debe llevar a cabo la evaluación. Es recomendable consultar al proveedor del sistema de corriente ininterrumpida para determinar la capacidad adecuada.

Las baterías no deben descargarse a un voltaje menor al mínimo recomendado por el proveedor y deben localizarse en un cuarto separado y ventilado, sobre todo si el sistema está operando cerca de sus límites de temperatura.

Cuando se selecciona el lugar del sistema de corriente ininterrumpida deben satisfacerse algunos factores, entre los que se encuentran:

1. Temperatura de las baterías.

Las baterías deben instalarse en un ambiente frío y seco con ninguna fuente de calor radiante. La temperatura ambiente de diseño para éstas es generalmente más baja que la temperatura mínima aceptable para el sistema de corriente ininterrumpida, así que debe regularse lo más cerca posible, tomando en cuenta que las temperaturas más bajas afectan su capacidad y las más altas afectan su vida.

2. Ventilación El proveedor del sistema de corriente ininterrumpida especifica la salida de calor y establece el uso de ductos o ventiladores; en su caso, determina también la altura que debe existir.

3. Nivel de acústica El proveedor indica los niveles ambientales típicos del sistema de corriente ininterrumpida, no dependiendo únicamente del ruido generado, sino

también de factores tales como absorción y reflexión de paredes.

4. Seguridad La seguridad del área de baterías es importante debido a la alta energía disponible por el ácido o los electrolitos. Es recomendable poner las baterías en un cuarto separado con llave, contar con un lavado y una regadera para cualquier accidente, además de tener un agente neutralizante cerca, así como una fuente de agua y una coladera en el piso para que se desalojen los electrolitos en caso de que se derramen. El personal debe contar con ropa de protección adecuada.

5. Capacidad de carga del piso. El piso del lugar donde se ubica el sistema de corriente ininterrumpida y las baterías puede requerir consideraciones estructurales especiales, que son determinadas por el proveedor.

6. Accesibilidad. Se debe considerar el movimiento del equipo a la instalación.

Planta generadora de energía

Dentro de las instalaciones eléctrica de un centro de cómputo se debe considerar la necesidad de contar con una planta generadora de energía para obtener una mayor seguridad tanto en los procesos

operativos, como en las instalaciones físicas y en los equipos eléctricos. (Ver Anexo 5)

La planta generadora de energía es un dispositivo que convierte energía mecánica en energía eléctrica mediante la rotación de bobinas dentro de un campo magnético.

Componentes

La mayoría de las instalaciones incluye un generador para satisfacer las necesidades de energía de un edificio o de un circuito de emergencia determinado. Algunas veces se cuenta con dos o más generadores para diferentes tipos de cargas o en otros casos se tienen dos generadores para alimentar la misma carga. En un centro de cómputo se requiere un generador exclusivo para el equipo de cómputo, sus periféricos y el aire acondicionado del centro, y un generador más para iluminación de emergencia, el elevador y otras cargas requeridas para el desalojo de la instalación, principalmente.

Debe contarse con equipo de transferencia manual o automática

para cambiar de la alimentación normal a la alimentación con la planta y viceversa. Los controles manuales son los más simples y menos costosos; pueden ser usados siempre y cuando haya alguien pendiente de las fallas, y cuando un inicio automático y una transferencia de la carga no sean un requerimiento crítico.

Para el caso de un centro de cómputo debe contarse con un dispositivo automático de transferencia (switch de transferencia). La fuente es monitoreada en forma continua, y en caso de falla, inicia automáticamente la planta de emergencia. Transfiere la carga en el momento en que la planta alcanza su energía plena y, cuando la fuente normal es restablecida, el dispositivo de transferencia automáticamente retransfiere la carga e inicia el apagado de la planta generadora.

Se pueden clasificar en base a lo que utilizan como combustible:

- a) **Diesel:** Utilizan motores de diesel que pueden alcanzar su carga máxima en menos de 10 segundos. El motor de diesel opera más eficientemente que una turbina de gas bajo carga completa. Su capacidad varia entre los 2.5. KW. El costo del combustible es considerablemente más bajo que para los

de gasolina. Los costos del motor de diesel son menores que los las turbinas de gas, pero los costos totales de instalación son comparables a los de la instalación de turbinas de gas; sin embargo, la disponibilidad de servicio de reparación para un motor de diesel es mayor que para una turbina de gas.

- b) **Gasolina:** Utiliza motores de gasolina y satisfacen necesidades de 100 Kw de salida. Inician rápido y tienen el costo inicial más bajo comparados con los de diesel. Las desventajas son los altos costos de operación, un mayor peligro debido al manejo de gasolina, corto almacenamiento del combustible y generalmente menor tiempo de mantenimiento.
- c) **Gas:** Utilizan turbinas de gas y requieren de 30 a 90 segundos para alcanzar su carga plena dependiendo de su tamaño. Se puede utilizar gas natural y gas LP. Éstos son similares en costo

a los de gasolina. Las turbinas de gas no están disponibles en tamaños menores de 500 KW, y por lo general se encuentran con capacidad de 600 KW. Para seleccionar entre gas naturales y LP se debe considerar la disponibilidad y la dependencia del suministro del combustible, especialmente en una situación de emergencia. Las turbinas de gas operan con menos ruido y vibraciones que las de diesel. Además los costos de instalación generalmente son menores.

Existen algunas consideraciones que hay que tomar en cuenta:

- ◆ Cuando se requiere sistemas bien regulados, libres de disturbios en voltaje, frecuencia o armónicos, tal como en el caso de un centro de cómputo, es necesario contar con un sistema de corriente ininterrumpida que suministrará corriente a la carga crítica, dando tiempo a que la planta generadora alcance su carga plena.
- ◆ Los sistemas de suministro de combustible deben respetar las leyes, reglamentos y requerimientos de seguridad. La capacidad de almacenamiento depende de la garantía

que ofrezca la compañía incluyendo domingos, días festivos y bajo todas las condiciones climáticas.

Sistema de conexión a tierra

La finalidad de un sistema de protección es prevenir fallas a tierra en el propio diseño, instalación, operación y mantenimiento de sistemas y equipos eléctricos. Sin embargo, la probabilidad de fallas a tierra o accidentes puede existir en la instalación eléctrica. Por tal razón, la protección debe proporcionar seguridad sobre las fallas a tierra que puedan ocurrir.

La protección para sistemas eléctricos requiere de:

1. Equipo protector de circuitos

Existen diferentes tipos de protección de circuitos. Algunos de los más comunes son los fusibles, los cortos circuitos con series, y el equipo interruptor de circuitos para dispositivos. La selección y

aplicación de un equipo protector de circuitos requiere de un análisis detallado de cada sistema y del circuito a ser protegido, incluyendo el sistema y equipo de conexión a tierra.

2. Sistema y equipo a tierra

Un sistema a tierra pertenece a la forma en cual un conductor de circuito de un sistema es intencionalmente conectado a tierra, o a algún cuerpo conductor el cual es efectivamente conectado a tierra o sustituido en lugar de tierra. El equipo a tierra es la unión de todos los circuitos conductores de cada circuito del equipo con los conductores del equipo a tierra.

Es un sistema de conductores que proporcionan una vía de retorno de baja resistencia para corrientes de fuga y falla. Por tal razón, el sistema de conexión a tierra previene y protege contra peligros de choque eléctrico.

El conductor a tierra en el cable de derivación de tres alambres de un sistema de distribución de energía es de suma importancia para la seguridad eléctrica. Las conexiones eléctricas del conductor a tierra, su condición y su capacidad de carga de

corriente con factores importantes en el suministro de una vía de baja resistencia para corrientes de fuga y falla.

En general, todo equipo eléctrico genera corriente de fuga. Normalmente la magnitud de esta corriente de fuga es demasiado pequeña para considerarse peligrosa.

Cuando la impedancia media en la vía de fuga o en la falla es extremadamente baja o de cero, existe una condición de falla, por lo que la cubierta del equipo se carga de energía. La corriente resultante fluirá a través del alambre a tierra hacia el panel de distribución de energía y operará un interruptor de falla a tierra, un disyuntor de circuito o un fusible en el circuito de energía. Esto puede pasar tan rápido que el peligro existiría sólo momentáneamente. Sin embargo, si el conductor a tierra es interrumpido o está conectado inadecuadamente, los instrumentos

de protección de sobre corriente no podrán desenergizar el equipo y la cubierta se quedará con cierto voltaje. Si un individuo toca esta cubierta mientras hace contacto con una superficie conectada a tierra, la corriente de falla fluirá a través de él, causándole posiblemente una lesión o incluso la muerte.

Un aspecto importante para la exitosa instalación de un sistema, lo constituye un adecuado sistema a tierra. Esto es debido a dos razones principales:

Seguridad

El sistema de tierra protege al personal de operación y mantenimiento, en el caso de que un bastidor del equipo tenga un alto voltaje o cuando algún cable de fase haga contacto con el bastidor accidentalmente, o debido al daño en algún componente.

Compatibilidad electromagnética

Reduce la posibilidad de interferencia proporcionando también un punto de referencia común.

En la trayectoria del conducto de tierra, no deben conectarse:

1. Tierras de estructuras metálicas (construcciones de acero, tuberías de agua, etc.

2. La tierra física para el sistema de cómputo (CPU, periféricos, terminales, discos, impresoras) debe ser única y dedicada; sólo puede ser encadenada para periféricos pequeños (módems, terminales, impresoras y videos).

3. El tipo de cable usado para la tierra física debe ser aislado y del mismo calibre que el del neutro y el de las fases.

4. Para la tierra se necesita instalar una varilla de cooperweld enterrada en el piso con una mezcla de sales; dicha varilla debe tener una longitud mínima de 2. metros y un diámetro de 2.3 centímetros.

Las razones por las que se tienen conectados a tierra el equipo eléctrico o los sistemas de instalación de alambres son debido a que:

- ♦ **Ofrece una ruta para una falla de corriente** Cuando la carga de un conductor hace contacto con la cubierta del equipo, la falla de corriente regresa al panel de distribución

por el conductor a tierra y causa un cortocircuito.

- ♦ **Garantiza la seguridad del personal.**

Por la falla descrita en el punto 1, la conexión a tierra proporciona seguridad al personal que está en contacto con el equipo, ya que el incremento de un suministro eléctrico será interrumpido rápidamente y la cubierta del equipo se mantendrá en un potencial menor que el de la carga del conductor.

- ♦ **Reduce la carga estática-** La conexión a tierra ofrece una ruta para la carga eléctrica estática que escapa del equipo – como las impresoras, terminales, procesadores y manejadores de discos-. Y asegura que la operación no se exponga y que los semiconductores no se dañen.

- ♦ **Reduce la señal eléctrica de ruido.** La conexión a tierra ofrece una ruta para señales de ruido que se deriven de cables protegidos, filtros y circuitos para asegurar la operación y evitar que se genere información falsa.

Recomendaciones:

Algunas recomendaciones para la instalación eléctrica en un centro de cómputo son las siguientes:

1. El voltaje debe mantenerse dentro del rango establecido para la operación del equipo. Las variaciones en el voltaje no deben exceder más del 15% o menos del 18% del voltaje nominal y debe regresar al rango normal de voltaje en menos de $\frac{1}{2}$ segundo.
2. La variación de voltaje entre fases no tendrá que ser mayor del 2.5% de la media aritmética de las tres fases, Por ejemplo, se tiene una fase con 124 V. Otra con 120V y otra con 121V. La media aritmética de las tres es 121.666V, el 25% es 3.04V, la variación entre las tres fases no excede este porcentaje.
3. La frecuencia de la línea debe mantenerse dentro de más o menos $\frac{1}{2}$ hertz (ciclos por segundo). Si se trabaja a 60 hertz, la frecuencia no debe ser menor de 59.5 hertz ni mayor a 60.5 hertz.
4. El contenido máximo de armónicos del voltaje de la fuente de alimentación del equipo no debe exceder más o menos 5% cuando el equipo esté en operación.
5. La acometida de energía eléctrica que alimente al equipo de cómputo debe ser independiente y no se le conectará ninguna otra carga, con el objeto de evitar interferencias.
6. La sección (área transversal) de los conductores eléctricos de la acometida debe calcularse para la potencia consumida por el equipo de cómputo, considerando un 30% adicional como margen de seguridad y posible ampliación.
7. La acometida independiente debe llegar al equipo de fuerza ininterrumpida y de ahí se alimentará a un tablero de distribución que deberá estar situado en un lugar visible y accesible. El tablero constará principalmente de un interruptor general, voltímetro para tres fases,

- indicadores luminosos e interruptores termo magnéticos para cada uno de los circuitos derivado que correspondan a los dispositivos que requieran alimentación directa, colocando a cada interruptor una etiqueta que indique cuál es la máquina que alimenta. Es los tableros deben considerarse espacios para al menos un 30% más de posiciones trifásicas, con el fin de permitir posibles ampliaciones.
8. El interruptor general del tablero puede ir en serie con uno o varios botones de emergencia distribuidos estratégicamente en la sala. Los circuitos derivados deberán salir del tablero general y terminarán cada uno de ellos debajo del piso falso, en una caja de conexiones situada en las proximidades de la máquina que va a alimentar.
9. Los conductores eléctricos deberán ir dentro de una tubería apropiada, de tal manera que se eviten los campos electromagnéticos producidos por el paso de la corriente y que pudieran provocar ruidos o interferencias.
10. Los circuitos derivados deben ir protegidos en mangueras flexibles o bajo tubo traqueal (tubo licuatite). Para calcular las secciones de estos circuitos se recomienda considerar los consumos parciales indicados en las hojas de especificaciones proporcionadas por el proveedor.
11. Cuando se utilizan cajas de conexión bajo el piso falso, éstas deben ser ancladas y aisladas, o plastificadas exteriormente, y tener una etiqueta que indique la máquina a la que están alimentando.
12. Deben existir enchufes auxiliares monofásicos a 127 v. Distribuidos en la sala y provenientes de una alimentación diferente a la del equipo de cómputo. Éstos servirán para conectar algunos aparatos eléctricos como sumadoras, cafeteras, etc.

-
13. Se debe instalar un equipo regulador donde se presenten con frecuencia las variaciones.
 14. Se debe considerar que no todos los países manejan los mismos estándares para el suministro de energía eléctrica; esto se debe a que las características de voltaje, frecuencia de onda corriente son diferentes.
 15. La elección del conductor que será utilizado como cable de alimentación principal o secundario depende de la intensidad de la corriente que deba canalizar. El diámetro de los tubos dependerá del número y sección de los conductores que llevarán dentro de ellos, sin raspar ni romper la cubierta aislante de éstos.
 16. Todos los órganos conductores deben quedar aislados de cualquier otro conductor y de los elementos adyacentes, como también de la estructura del edificio. Con el objeto de proteger el aislamiento del deterioro y evitar el riesgo del fuego, todos los conductores deben quedar encerrados en un envolvente metálico o alguna otra protección; se pueden utilizar tubos de acero rígidos o flexibles, circulares, rectangulares u ovalados.
 17. Se deben emplear los tubos rígidos de acero, los cuales pueden estar instalados en el exterior de las paredes. El tubo flexible se usa en lugares donde la instalación de tubos rígidos resulta difícil y se requiere una cubierta protectora flexible.

Riesgo de Inundación

En muchas partes del mundo, el daño y riesgo de inundación es algo común. Las computadoras no se deben colocar en sótano o en las áreas de planta baja sino,

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

de preferencia, en las partes altas de una estructura de varios pisos. Claro que la mejor opción es no colocar el centro de cómputo en áreas donde el riesgo de inundación sea evidente.

Los daños por inundación o agua han ocurrido aún cuando las instalaciones no se encuentren cerca de un río o una costa donde estuvieran expuestas a tornados, huracanes o tormentas, ni en áreas bajas.

La situación se origina por lo regular tras la ruptura de cañerías o por el

bloqueo del drenaje. Por lo tanto, la ubicación de las tuberías en la construcción de las instalaciones de cómputo es una decisión importante (no debe ponerse por encima de las áreas donde se colocan los equipos). El daño causado por el drenaje bloqueado es un riesgo seguro cuando la computadora se coloca en algún sótano. Debe instalarse, si es el caso, detectores de agua o de inundación, así como también bombas de emergencia para resolver inundaciones inesperadas.

Protección, y Detección de Incendios

La protección contra fuego es lograda de una mejor manera a través de una correcta construcción del edificio (el cual debe procurarse que sea resistente al fuego). Sin embargo, siempre habrá materiales combustibles y equipo dentro del edificio, así que es necesario asegurar que el equipo contra incendio esté disponible de forma inmediata y que se pueda controlar el fuego con relativa facilidad.

Elementos necesarios que se consideran sobresalientes:

- ♦ Las paredes del área del equipo de cómputo deben de ser de material incombustible. Si el área del equipo de cómputo tiene una o más paredes exteriores adyacentes a un edificio que sea susceptible de incendio, la instalación de ventanas irrompibles mejorará la seguridad.

-
- ◆ El techo falso debe de ser de material incombustible o resistente al fuego.
 - ◆ Todas las canalizaciones y materiales aislantes deben ser de materiales incombustibles y que no desprendan polvo.
 - ◆ El piso falso instalado sobre el piso real debe ser incombustible.
 - ◆ El techo de la sala y el área de almacenamiento de discos y cintas magnéticos deben ser impermeables.
 - ◆ Debe preverse un sistema de drenaje en el piso firme.
 - ◆ Los detectores de fuego y humo se deben colocar cuidadosamente en relación con los aparatos de aire acondicionado, ya que los conductores de éste pueden difundir el calor o el humo y no permitir que se active el detector.
 - ◆ El detector de humo que se elija debe ser capaz de detectar los distintos tipos de gases que desprendan los cuerpos en combustión. Algunos no detectan el humo o el vapor que proviene del plástico quemado que se usa como aislante en electricidad y, en consecuencia, los incendios producidos por un corto circuito tal vez no se detecten.
 - ◆ Los detectores de humo y el calor se deben instalar en la sala de cómputo, junto a las áreas de oficina y dentro del perímetro físico de las instalaciones.
 - ◆ Es necesario colocar detectores de humo y calor bajo el piso en los ductos del aire acondicionado.
 - ◆ Las alarmas contra incendios deben estar conectadas con la alarma central del lugar, o bien directamente al departamento de bomberos.
- Es importante que estos requerimientos no sólo se apliquen en la construcción de la sala de cómputo, sino también en las áreas adyacentes.
- La documentación de los sistemas, la programación y las operaciones también necesitan protección contra incendios. La destrucción de esta documentación puede imposibilitar el uso de programas o archivos de respaldo. Se deben establecer procedimientos que garanticen la actualización de toda la
-

documentación como rutina y que las copias de seguridad se almacenen en un lugar lejano, así como las copias de seguridad de los programas y los archivos.

Los sistemas de extinción del fuego son esenciales si el área contiene algo valioso, si hay un equipo importante, o si se están protegiendo funciones vitales para la compañía. Tales sistemas son destinados a detectar y suprimir el fuego dentro de los primeros segundos, reduciendo así la dependencia contra las técnicas manuales –las cuales pueden llegar demasiado tarde-.

En la mayoría de las instalaciones se utiliza gas como extintos, sin embargo existen también extintores de espuma, de agua o de polvo seco.

El uso de bióxido de carbono en algún tiempo generalizado, debe reservarse, debido al efecto letal que tiene sobre los humanos.

En la actualidad los sistemas de control de fuego utilizan preferentemente halón 1301 como agente de extinción. Este gas y el número 1301 indican que su fórmula es una parte de carbón, 3 partes

de fluorina, cero de clorina y uno de brobina. Una concentración del 5% de halón 1301 es suficiente para extinguir un fuego en un cuarto cerrado y no es considerada como peligrosa para el ser humano, ya que reduce el oxígeno del aire sólo en un 20 o 21%.

Se necesita ubicar los extinguidores apropiados en lugares de acceso inmediato y es conveniente señalizarlos. De la misma forma, todo aviso o recomendación relativo a la seguridad ha de ser claramente visible; en este caso debe de existir indicadores de prohibición de fumar. Estos extinguidores y el equipo de gas se deben revisar con regularidad para asegurar su funcionamiento efectivo.

Es necesario definir y documentar los procedimientos que deben seguirse en caso de incendio; además, se debe entrenar al personal acerca de uso. Se ha descubierto que ésta es un área débil, sobre todo en instalaciones cuyos índices de cambio de personal son altos. Con frecuencia, muchos empleados no saben exactamente qué deben hacer en caso de incendio.

La participación del cuartel de bomberos tanto en el diseño como en la aplicación de los procedimientos para detectar, prevenir y extinguir incendios podría ser muy valiosa. Sin embargo, la mayoría de las brigadas trabajan de manera tradicional y no cuentan con la instrucción adecuada para ese tipo de emergencias. Incluso en muchos casos los bomberos pueden dañar seriamente el equipo de cómputo. (Ver Anexo 1)

Mantenimiento

La empresa debe disponer de servicios de mantenimiento, ya sean propios o contratados externamente, en función de sus características y posibilidades. Estos servicios deben abarcar tanto los equipos informáticos como los equipos auxiliares (electricidad, agua, aire acondicionado, etc.) siempre considerando que el funcionamiento de los sistemas informáticos depende de su buen estado.

La limpieza de la instalación de cómputo es importante desde dos puntos de vista:

- ◆ Refleja una actividad disciplinada. La seguridad es en gran parte una actividad mental y refleja el hecho de que los procedimientos adecuados y efectivos están en uso.
- ◆ El mal mantenimiento crea las condiciones para una fractura en la seguridad, como cuando las puertas y las ventanas no cierran correctamente, o bien, cuando se propicia incendios.

Es vital mantener limpio el centro de cómputo, pero hay que recordar que el agua y el detergente pueden dañar el equipo: es por eso que debe instruirse al personal de limpieza al respecto. Es muy común en muchas empresas que el personal de limpieza utilice trapos mojados para “limpiar” el equipo, incrementando el riesgo de dañarlo.

El buen mantenimiento refleja la actividad general de las personas en una empresa: simboliza una buena administración y aumenta la seguridad en computación.

3.4. SEGURIDAD LOGICA Y CONFIDENCIALIDAD

La seguridad lógica y confidencialidad está referido al acceso de los archivos de datos y programas instalados en la computadora, solo se permitirá al personal autorizado. Existe el riesgo de que personas no autorizadas tenga acceso a los archivos y programas y efectúen cambios no autorizados a la información procesada.

Para mantener un control adecuado, las funciones de seguridad para esta área debe abarcar:

- ◆ Medidas de autenticación
- ◆ Protección Especial de la Información Confidencial
- ◆ Niveles de Acceso;
- ◆ Acceso limitado a las terminales.
- ◆ Revelación o infidencia
- ◆ Sobre el uso de los servicios de la red de datos institucional y las cuentas de usuario
- ◆ Sobre conexión a otras redes
- ◆ Uso Firewall.

Medidas y recomendaciones para la Seguridad Lógica y Confidencialidad

Medidas de Autenticación

La autenticación, que consiste en identificar a los usuarios que entran al sistema, se puede basar en posesión (llave o tarjeta), conocimiento (clave) o en un atributo del usuario (huella digital).

El mecanismo de autenticación más ampliamente usado se basa en el uso de claves o *passwords*; es fácil de entender y fácil de implementar.

Claves:

Proteja su identificación de usuario por medio de una palabra clave, siempre que no exista la posibilidad de utilizar otras medidas de seguridad, como por ej.: tarjetas magnéticas o inteligentes.

- ♦ Escoja la palabra clave de tal manera que no sea fácilmente deducir. Este tipo de palabra no debe guardar relación con su propietario.
- ♦ Considerar el largo mínimo de la clave de ocho caracteres como mínimo (ocho es considerado por los expertos generalmente como un mínimo largo respetable, para sistemas de propósito general, se recomienda el uso de letras, cifras y caracteres) y esta deberá chequearse automáticamente apenas el usuario la crea o la selecciona.
- ♦ El sistema de computación debe cerrarse después que un individuo no autorizado

falle dos veces al intentar ingresar una clave de acceso.

Modificar la palabra clave cada 90 días como máximo

- ♦ Como regla general no transmitir la clave a otros.
- ♦ Cambiar la palabra clave cuando exista indicio de haber sido divulgada
- ♦ Asegurarse que al teclear las claves, de que ninguna persona no autorizada pueda visualizarla.
- ♦ No utilizar claves antiguas para la creación de una nueva

Identificación física

Un enfoque diferente es usar un elemento físico difícil de copiar, típicamente una tarjeta con una banda magnética. Para mayor seguridad este enfoque se suele combinar con una clave (como es el caso de los cajeros automáticos). Otra posibilidad es medir características físicas particulares del sujeto: huella digital, patrón de vasos sanguíneos de la retina, longitud de los dedos. Incluso la firma sirve.

Algunas medidas básicas

- ♦ Demorar la respuesta ante claves erróneas; aumentar la demora cada

vez. Alertar si hay demasiados intentos.

- ◆ Registrar todas las entradas, cada vez que un usuario entra, chequear cuando y desde donde entro la vez anterior.
- ◆ Hacer chequeos periodicos de claves fáciles de adivinar,

procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas (por ejemplo cuando usuario está de vacaciones).

- ◆ Para los más paranoicos: poner trampas para descubrir intentos de uso no autorizado.

Protección Especial de la Información Confidencial

Una de las funciones muy importantes de los responsables de comunicación es mantener controlado el uso de los datos de la compañía y los sistemas de transmisión.

Además de controlar el uso del sistema por empleados autorizados, deben también considerarse los problemas relativos a empleados que pueden tener acceso al computador, pero que no están autorizados a usar programas o acceder a los archivos de bases de datos, así como los problemas con individuos ajenos a la organización.

Los mecanismos de protección que hemos visto hasta ahora muchas veces no son suficientes para mantener información confidencial adecuadamente resguardada. Con el uso masivo de las redes de computadores, más y más información se transmite por ella, y nadie puede estar seguro de que no hay *mirones* en el alambre. Un sistema de información puede ser causa de violación de su seguridad, debido a varios factores:

- ◆ La naturaleza de su organización y de sus operaciones.
- ◆ Los tipos de aplicaciones y de bases de datos en el sistema de proceso de datos.

- ♦ La posibilidad de beneficio económico para los delincuentes.
- ♦ El tamaño de la población de usuarios del sistema.
- ♦ El tipo de sistema y las posibilidades disponibles para los usuarios.

Para las amenazas potenciales son razones suficientes para la estimación de riesgo contra la seguridad.

uno de los principales métodos, para ofrecer protección es hacer que la información del mensaje sea ininteligible por medio de técnicas criptograficas, sin intentar ocultar la existencia del mensaje.

Encriptación:

Los métodos criptográficos son los más comúnmente usados para proteger información confidencial.

Es una técnica mediante la cual se transforman los datos de forma que no proporcionen información al ser

interceptados, puesto que tal como están almacenados o transmitidos son completamente ininteligibles.

Cada carácter es un registro reemplazado por otro carácter, así por ejemplo:

La palabra SMITH se almacena como @LAZ#

En este caso, toda S es reemplazada por el símbolo @. Etc., de este modo si alguien obtiene los datos no los entenderá, a menos que el lector sepa como descifrar la información.

La mayor aplicación de escribir los datos usando criptografía, se aprecia en la protección de los mismos cuando se transmiten a través de las líneas de comunicación.

Niveles De Acceso

Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso.

Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

- ◆ ☐ Nivel de consulta de la información no restringida o reservada.
- ◆ Nivel de mantenimiento de la información no restringida o reservada.
- ◆ Nivel de consulta de la información incluyendo la restringida o reservada.
- ◆ ☐ Nivel de mantenimiento de la información incluyendo la restringida.

a) Nivel de consulta de la información

El privilegio de lectura está disponible para cualquier usuario y sólo se requiere un conocimiento de la estructura de los datos, o del Sistema de otro usuario para lograr el acceso.

La autorización de lectura permite leer pero no modificar la base de datos.

b) Nivel de mantenimiento de la información

El concepto de mantenimiento de la información consiste en:

Ingreso. Permite insertar datos nuevos pero no se modifica los ya existentes.

Actualización. Permite modificar la información pero no la eliminación de datos.

Borrado. Permite la eliminación de datos.

Un usuario puede tener asignados todos, ninguno o una combinación de los tipos de autorización anteriores. Además de las formas de autorización de acceso de datos antes mencionadas, es posible autorizar al usuario para que modifique el esquema de la base de datos, pero es preferible que esta función sea de responsabilidad del Centro de Cómputo.

Cada palabra clave debe tener asignado uno de los niveles de acceso a la información mencionados anteriormente.

La forma fundamental de autoridad es la que se le da al administrador de la base

de datos, que entre otras cosas puede autorizar nuevos usuarios, reestructurar la base de datos, etc. Esta forma de autorización es análoga a la que se provee a un "super usuario" o al operador para un sistema operativo.

Acceso limitado a las terminales

Las terminales que son dejadas sin protección pueden ser mal usados. Cualquier terminal que puede ser utilizado como acceso a los datos de un Sistema controlado, debe ser encerrado en un área segura o guardado, de tal manera que no sean usados, excepto por aquellos que tengan autorización para ello.

Igualmente, se deberá considerar la mejor manera de identificar a los operadores de terminales del Sistema, y el uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 - 10 Min.).

Restricciones que pueden ser aplicadas:

- ◆ Determinación de los períodos de tiempo para los usuarios o las terminales.
- ◆ Designación del usuario por terminal o del terminal por usuario.
- ◆ Limitación del uso de programas para usuario o terminales.
- ◆ Límite de tentativas para la verificación del usuario.
- ◆ Tiempo de validez de las señas.

Revelación o Infidencia

La revelación o infidencia es otra forma que realizan los malos empleados, para su propio beneficio.

La información, que es de carácter confidencial, es vendida a personas ajenas a la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

Control del uso de información en paquetes abiertos o cintas y otros datos residuales

La información puede ser conocida por personas no autorizadas, cuando se dejan en paquetes abiertos o cintas que otras personas pueden usar.

Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el de

esta a aquellas personas que puedan usar mal los datos residuales de estas.

Mantener datos sensitivos fuera del trayecto de la basura

El material de papel en la plataforma de la descarga de la basura puede ser una fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Los datos sensitivos deben ser apartados de este procedimiento, para tener una mayor seguridad de protección de la información, cuando estos son descartados o eliminados, debiendo recurrirse a destructores o picadoras de papel.

Sobre el uso de los servicios de la red de datos institucionales y las cuentas de usuario

De aplicación General

- ◆ Todo funcionario que para el desempeño de sus funciones

requiera utilizar la red de datos institucional, deberá poseer una cuenta de usuario

-
-
♦ Para solicitar el servicio que requiera, deberá estar autorizado por el director del área a la que pertenezca o por la autoridad competente del servicio solicitado. ♦ La cuenta es individual e intransferible y su dueño será el responsable de mantener la confidencialidad de la contraseña de la cuenta, de hacer uso adecuado de las misma y de responder sobre todas las actividades que ocurren bajo su cuenta o contraseña ♦ Las cuentas tendrán una duración limitada y se regularán por un procedimiento específico.	♦ Administrará los servicios de la red de datos institucional de manera exclusiva, con el personal del área responsable de esta función y en los casos necesarios, con la participación de los proveedores autorizados. ♦ Administrará las cuentas de usuarios y mantendrá registros en línea o almacenados del uso de las mismas, que permitan realizar auditorías o revisiones, en caso de existir situaciones que así lo ameriten. ♦ Mantendrá control sobre el acceso de usuarios a los elementos (físicos y lógicos) de administración de la red de datos institucional. ♦ Vigilará que la infraestructura de la red sea utilizada únicamente en actividades relacionadas con los objetivos institucionales, así como actividades similares de

De Aplicación por
Parte del
Administrador (Unidad
de Informática)

aquellas entidades con las que exista un convenio vigente.

- ◆ Mantendrá información actualizada y disponible sobre el alcance y servicios de la red de datos institucional.
- ◆ Se asegurará del buen estado de la infraestructura de la red así como del cumplimiento de las normas recomendadas para este tipo de instalaciones.
- ◆ Ofrecerá los medios y mecanismos para que los usuarios obtengan productos y servicios informáticos de calidad, con los niveles de seguridad adecuados y favoreciendo el máximo aprovechamiento de los recursos informáticos y de comunicaciones disponibles. Otorgará cuentas de usuarios a personas ajenas a la Institución (personal externo) siempre y cuando la solicitud cumpla con los requisitos establecidos para

el servicio requerido y haya sido aprobado por el Director o Autoridad competente, relacionada con el área donde trabajare la persona solicitante. Estas cuentas tendrán una vigencia de 90 días y podrán ser renovadas con el envío de una nueva solicitud autorizada.

De aplicación por parte del usuario

- ◆ Hará buen uso y tendrá acceso a los recursos y servicios informáticos de acuerdo a las disposiciones y reglamentaciones que para *estos fines* existen.
- ◆ Deberá utilizar la cuenta asignado, para el acceso a los servicios que tengo autorización.
- ◆ Solo podrá utilizar la infraestructura de la red de datos institucional para aquellos servicios que se le

haya concedido acceso y únicamente para el desarrollo de actividades relacionadas con su función. Esta cuenta es de uso exclusivo y no debe ser compartida.

- ◆ No utilizará los recursos de la red de datos institucional, para anunciar, enviar por correo electrónico o por cualquier otro medio de transmisión electrónico, contenidos ilegales o confidenciales, anuncios no autorizados, materiales promocionales y mensajes que contengan virus que pongan en riesgo los bienes informáticos

y datos institucionales, lo cual estará reglamentado en las normas de uso de este servicio.

- ◆ Comprenderá que cualquier material y/o datos bajados o de otra manera obtenidos mediante el uso del servicio, sin contar con las protecciones recomendadas, es riesgo para él y la Institución, y que será exclusivamente responsable de cualquier daño al sistema o pérdida de datos que pueda resultar de recibir tal material y/o datos.

Sobre Conexión a otras redes

De Aplicación por Parte del Administrador (Unidad de Informática)

- ◆ Velara por las conexiones que se requieren entre la red de datos

institucional con redes de otras instituciones, se realicen verificando que se garanticen los niveles de seguridad exigidos por las entidades involucradas e igualmente que los niveles de riesgos de accesos indebidos se

minimicen, para lo cual cada entidad involucrará el equipamiento y los mecanismos de control de accesos que se consideren necesarios.

De Aplicación por Parte del Usuario

Sobre el uso de Firewall

Un firewall, es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada e internet, un firewall determina cual de los servicios de red pueden ser accedidos por personas que se encuentren fuera de ella. El establecimiento de un firewall de acuerdo a las condiciones propias de la unidad de informática garantiza que intrusos o personas ajenas a la organización no penetren a ella.

- ♦ Para que un firewall sea efectivo, todo tráfico de información a través de Internet deberá pasar a través del mismo para ser inspeccionado.

- ♦ Los usuarios que accedan a servicios de otras redes a través de una conexión habilitado por la institución, estarán sujetos a las normas que la institución receptora tenga estipuladas y las violaciones a las mismas, serán penalizadas de acuerdo al reglamento de cada sitio.

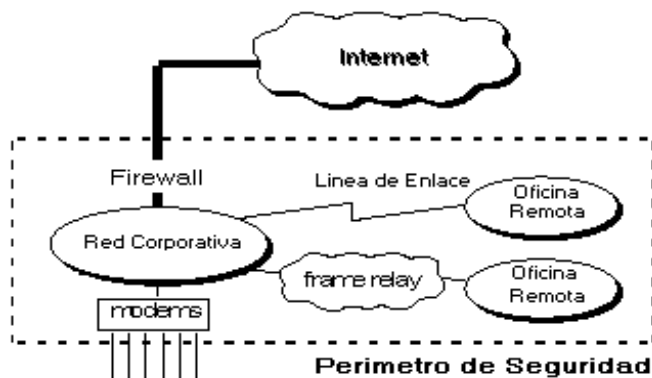
- ♦ El firewall podrá únicamente autorizar el paso del trafico y el mismo podrá ser inmune a la penetración, una vez que un agresor traspasa la protección ofrecida por un firewall, este no podrá realizar tarea alguna referente a la protección del sistema.

Objetivo de un firewall

El objetivo principal de un firewall es mantener privacidad y asegurar la autenticidad de las comunicaciones de datos que pasan las fronteras del dominio de red. Una vez que un dato entra o deja un dominio de red, está protegida de usuarios que quieran husmear o modificar información.

Físicamente un firewall se implementa en hardware, software o en ambos.

Ilustración -1 La Política De Seguridad Crea Un Perímetro De Defensa.



Esto es importante, ya que debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada, para proteger las fuentes de información. Esta política de seguridad podría incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la

red, políticas de servicios en la red, políticas de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

3.5. SEGURIDAD EN EL PERSONAL

La mayoría de las instituciones han tomado conciencia de la creciente dependencia en la integridad, estabilidad y lealtad del personal y dedican mayor atención a esta área de la seguridad. La contratación de personal inapropiada para puestos de gran responsabilidad, como las operaciones y el control, no es raro y necesariamente aumenta el riesgo de accidentes y peligros potenciales en el área de informática.

Como ya se mencionó, existe el riesgo de que se dependa de manera excesiva en esta área, es decir la de informática, y sobre todo en las instalaciones de alta seguridad, donde indagar acerca de los antecedentes del personal es

prácticamente de rutina. Estas instalaciones siempre son un blanco de ataque; la prevención de cualquier intento al respecto solo la garantiza un filtro de seguridad a toda prueba.

Para asegurar una buena administración de personal con relación a la seguridad es necesario considerar siete áreas:

- ◆ Procedimientos de contratación.
- ◆ Procedimientos para evaluar el desempeño.
- ◆ Política sobre permisos.
- ◆ Rotación de puestos
- ◆ Actitudes del personal.
- ◆ Motivación y Satisfacción
- ◆ Medidas de higiene, salubridad y ergonomía.

PROCEDIMIENTOS DE CONTRATACIÓN

Casi todas las instituciones cuentan con un procedimiento de contratación bien

estructurado y de rutina; sin embargo, en muchos casos este se aplica con

demasiada flexibilidad. Desde el punto de vista de la seguridad, las características más importantes de una política de contratación son:

- ◆ Verificación de referencias y antecedentes.
- ◆ Pruebas psicológicas.
- ◆ Exámenes médicos.

Verificación de Referencias y Antecedentes

La verificación de las referencias normalmente se pasa por alto. Muchas empresas se muestran renuentes a proporcionar referencias útiles, debido a razones legales o de otra índole. Esto representa ciertas dificultades para evaluar la aceptabilidad de un solicitante.

Aún cuando legalmente se permita que el patrón anterior proporcione información, con frecuencia este la emite de manera tan general que resulta difícil obtener datos precisos sobre la integridad del solicitante. En este caso, resulta sumamente deseable que se compile una lista de verificación detallada. Las listas estándar sobre

personal son, en general, apropiadas para esta labor y existen muchas versiones publicadas. Estas verificaciones muy rara vez pueden ser exhaustivas.

Las compañías de seguros pueden ofrecer ayuda en el proceso de verificación de referencias. La necesidad de cobertura de la garantía de fidelidad se estudia en un apartado más adelante. Cuando se requiere esta cobertura, la compañía de seguros inicia una verificación independiente, lo cual refuerza el procedimiento de verificación de referencias.

En una instalación de alta seguridad, es rutinaria la obtención de antecedentes de los agentes de seguridad. Aunque estas prácticas son en general más estrictas no pueden ser totalmente correctas.

Prueba psicológicas

El uso de pruebas psicológicas dentro del proceso de contratación constituye un importante refuerzo potencial. Las pruebas no solo sirven para evaluar aptitudes, sino también para medir actitudes, valores sociales, opiniones políticas y estabilidad general.

En muchas instalaciones de alta seguridad, estas pruebas han demostrado ser de gran valor. En la actualidad, existen servicios profesionales de alto nivel para el apoyo de los procedimientos antes mencionados.

Examen Médico

Una fase importante del procedimiento de contratación de personal son los exámenes médicos. Estos permiten evaluar no solo el estado físico de un individuo, sino también las actitudes y la estabilidad potencial del recién

contratado. En particular, se debe analizar la habilidad para laborar en situaciones de estrés, especialmente cuando este es parte de las exigencias del puesto.

Algunas instituciones han adoptado la política de realizar exámenes médicos semestrales o anuales para el personal de cómputo expuesto a mucho estrés en sus cargos. Si se descubren elementos adversos, se puede reestructurar el trabajo del empleado de manera temporal.

Procedimientos para evaluar el desempeño

Las actividades para evaluar el desempeño pueden cooperar con la seguridad en forma rutinaria. Aunque en primera instancia están destinadas a valorar la efectividad de los aspectos administrativos y de trabajo, pueden colaborar con la efectividad de la seguridad.

Al mismo tiempo, la evaluación del desempeño puede servir también para evaluar las actitudes hacia el trabajo y los sentimientos generales hacia la

institución. Aunque de ninguna manera se sugiere que los gerentes se transformen en psicólogos aficionados, el proceso de evaluación del desempeño puede identificar y ayudar al personal con problemas personales o de actitud.

En las instalaciones de alta seguridad resulta muy valioso que gerentes revisen de manera más frecuente las actitudes y el comportamiento del personal bajo su cargo, por ejemplo, unas cuatro veces al

año. Para ello, basta con una lista de unas cuatro a seis preguntas.

Política sobre permisos

El sobre tiempo excesivo es común en las instalaciones de cómputo. Al mismo tiempo, los permisos rara vez están reglamentados debido al nivel clave de los cargos del personal.

La reglamentación de los permisos es importante para asegurar que el personal expuesto al estrés descansa periódicamente de manera apropiada. El personal de cómputo es, por lo general, de inteligencia y preparación superiores al promedio, con frecuencia son personas muy sensibles y, aunque no hay estadísticas al respecto, se ha notado la incidencia de crisis nerviosas. En este aspecto, los directivos muestran una

actitud irresponsable al no reglamentar los permisos.

En todos los demás departamentos de una organización, los permisos se hallan reglamentados, en especial para los puestos de confianza. Este es también un buen sistema para detectar robos, fraudes y planes de sabotaje en potencia. La importancia y dependencia en el personal clave no debe obstruir la reglamentación de esta política en la función del procesamiento de datos.

Rotación de puestos

Es del conocimiento general que la rotación de los puestos constituye un buen antagonista de fraudes, en especial cuando se trata del personal de puestos altos de confianza. Este principio se aplica al personal de cómputo.

Se debe tener en cuenta que existe una desventaja propia de la rotación de puestos, sobre todo en un ambiente de alta seguridad. Esto es que un solo individuo tiene acceso a las actividades de un frente muy amplio. Sin embargo,

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

la rotación de los puestos es más recomendable en los niveles de responsabilidad medio y bajo, donde esa situación no se presenta. Aún así, las ventajas de la rotación generalmente sobrepasan cualquier posible desventaja.

Sustitución del personal clave

Un elemento esencial para la seguridad en computación consiste en garantizar que todo el personal clave tenga una sustitución adecuada. En la práctica no es posible asegurar la sustitución de todo el personal, por lo que necesita restringir en forma cuidadosa la definición de personal clave. Se debe brindar atención especial a la evaluación

de la importancia del personal relacionado con la programación de las aplicaciones o sistemas de carácter avanzado.

Con frecuencia se argumenta el costo cuando se plantea el problema de la sustitución. Muchas instalaciones se ajustan basándose en que el personal no es adecuado. Así los niveles de costo no contemplan la sustitución. Si la instalación requiere medidas de seguridad de alto nivel, entonces los niveles de gastos deben contemplar la sustitución y el apoyo adecuado para los puestos clave

Evaluación de las actitudes del personal

No es probable que un empleado bien motivado sea desleal. De igual manera, la posibilidad de que surjan brechas en la seguridad debido a accidentes o ataques deliberados es más alta en un ambiente donde la motivación es baja. En muchas instalaciones, especialmente las de mayor tamaño, resulta difícil vigilar las actitudes todo el tiempo. El

uso de encuestas sobre actitudes puede ser un instrumento valioso para el seguimiento de rutina en este aspecto de la política hacia el personal.

Culminación de la relación laboral

Este es un aspecto más que importante para lograr que la seguridad de una organización pueda considerarse como óptima y eficaz, puesto que todo

despido, sea por la causa que fuere, genera un cierto riesgo hacia los recursos y personas pertenecientes a la organización.

Los procedimientos a seguir para la culminación de la relación de trabajo deben:

- ◆ Proteger los activos de la compañía
- ◆ Ser revisados a los efectos de determinar si son adecuados
- ◆ Ser diseñados de acuerdo a lo que establece la ley de trabajo vigente
- Considerar todos los motivos por los cuales queda terminado el contrato según lo tratado en la ley

Algunas cuestiones fundamentales a tener en cuenta en los procedimientos son:

- ◆ Debe cerciorarse de que al personal, cuando ha sido separado de la compañía, se le pague lo debido en términos legales.
- ◆ Verificar que a los empleados que sean separados de la organización se les requiera que dejen o reintegren

todos los documentos proporcionados por la organización, particularmente los que puedan utilizarse para activar terminales o abrir puertas restringidas.

- ◆ Comprobar que al personal de sistemas, cuando es notificado de su despido, sea acompañado inmediatamente fuera de las áreas de la empresa, sin darle la oportunidad de dañar las instalaciones de cómputo o los archivos de datos en la organización.
- ◆ Vigilar que las palabras clave o cualquier otro dispositivo de acceso a las terminales o a otros recursos de computo sean cambiadas inmediatamente después de la terminación de la relación laboral.
- ◆ Revisar los procedimientos de personal para determinar si los mismos destinados al personal del área de sistemas o informática concuerdan con lo estipulado por lo detallado más arriba.

Motivación y Satisfacción de Personal

Se sabe que en la era actual, la tecnología y la información es indispensable, y están al alcance de todas las instituciones, por lo que la única ventaja competitiva que puede diferenciar una empresa de otra es la actitud y capacidad que tienen las personas dentro de la organización para adaptarse al cambio.

Sin embargo la administración de este recurso no es una tarea muy sencilla. Cada persona es un fenómeno sujeto a la influencia de muchas variables y entre ellas las diferencias en cuanto a aptitudes y patrones de comportamientos son muy diversas.

A las personas debe dárseles razones e incentivos para influir en su comportamiento. Las personas cuentan con la libertad de poder elegir cuando tener una actitud de cooperación o de resistencia hacia la autoridad. También deciden su cuota de compromiso con los objetivos de la organización y debido a que las personas no pueden controlarse

de la misma forma que las herramientas, la dirección de la administración debe preocuparse por asegurar el aporte de los esfuerzos individuales de sus miembros y una forma de lograrlo es haciendo hincapié en la motivación para lograr una satisfacción laboral que genere estabilidad y lealtad en el personal.(VER ANEXO 5 DEL MANUAL)

Diferencia entre Motivación y Satisfacción

Se puede definir a la motivación como el impulso y el esfuerzo para satisfacer un deseo o meta. En cambio, la satisfacción esta referida al gusto que se experimenta una vez cumplido el deseo. Podemos decir entonces que la motivación es anterior al resultado, puesto que esta implica un impulso para conseguirlo; mientras que la satisfacción es posterior al resultado, ya que es el resultado experimentado

Qué es la satisfacción laboral

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Es la actitud del trabajador frente a su propio trabajo, dicha actitud está basada en las creencias y valores que el trabajador desarrolla de su propio trabajo. Las actitudes son determinadas conjuntamente por las características actuales del puesto como por las percepciones que tiene el trabajador de lo que "deberían ser". Generalmente las tres clases de características del empleado que afectan las percepciones del "debería ser" (lo que desea un empleado de su puesto) son: Las necesidades, los valores y rasgos personales.

Los tres aspectos de la situación de empleo que afectan las percepciones del "debería ser" son: Las comparaciones sociales con otros empleados, Las características de empleos anteriores y Los grupos de referencia.

Las características del puesto que influyen en la percepción de las condiciones actuales del puesto son:

1. Retribución
2. Condiciones de trabajo

3. Supervisión
4. Compañeros
5. Contenido del puesto
6. Seguridad en el empleo
7. Oportunidades de progreso.

Además se puede establecer dos tipos o niveles de análisis en lo que a satisfacción se refiere: Satisfacción General indicador promedio que puede sentir el trabajador frente a las distintas facetas de su trabajo.

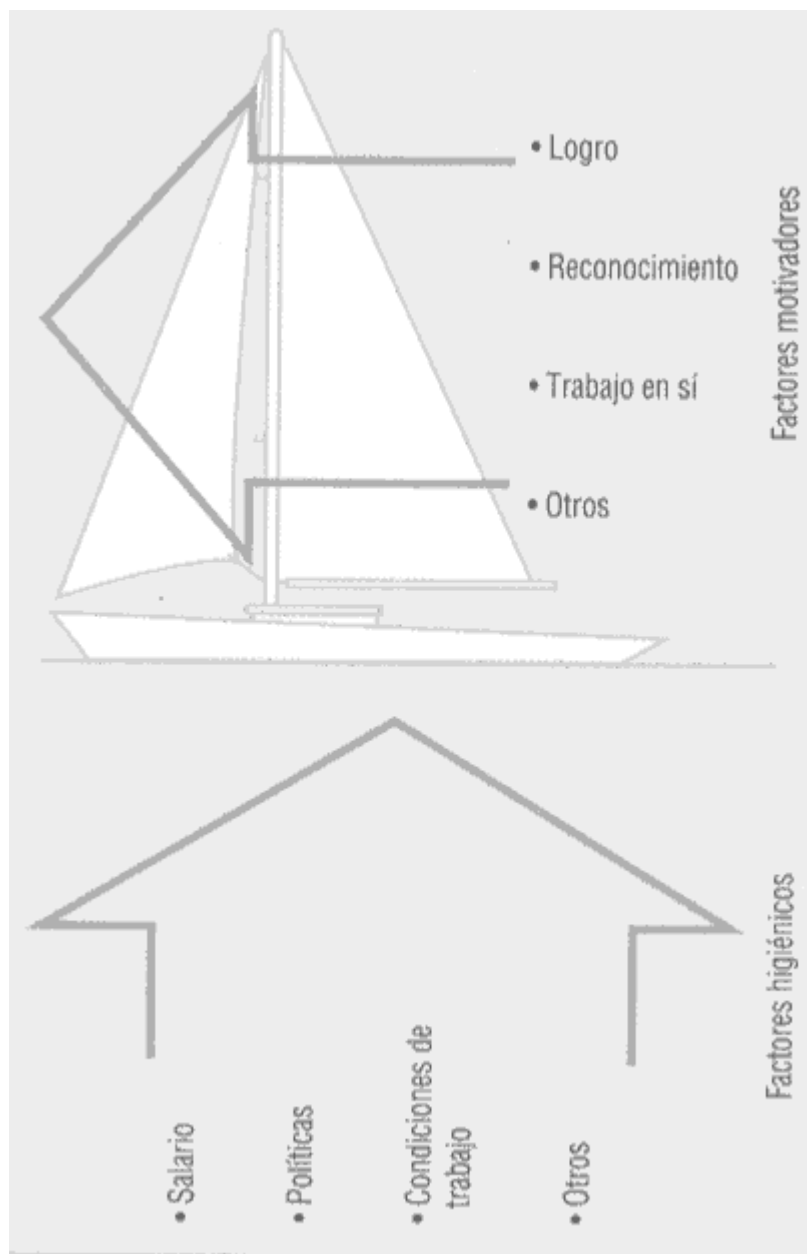
Satisfacción por facetas grado mayor o menor de satisfacción frente a aspectos específicos de su trabajo: reconocimiento, beneficios, condiciones del trabajo, supervisión recibida, compañeros del trabajo, políticas de la empresa.

La satisfacción laboral está relacionada al clima organizacional de la empresa y al desempeño laboral.

La teoría de los dos factores afirma que:

- **La satisfacción en el cargo** es función del contenido o de las actividades desafiantes y estimulantes del cargo: Estos son los llamados factores motivadores.
- **La insatisfacción en el cargo** depende del ambiente, de la supervisión, de los colegas y del contexto general del cargo: Estos son los llamados factores higiénicos.

En la vida de la organización la falta de cobertura de los factores higiénicos provocará la insatisfacción de sus miembros, impidiendo a los mismo permanecer en un estado de motivación debido a su preocupación por satisfacer necesidades de este tipo. Una vez satisfechas en forma mínima las necesidades higiénicas esto evitará que los miembros de la organización padezcan un estado de insatisfacción, pero no será suficiente para provocar una actitud motivante.



Hackman y Oldham (1975) aplicaron un cuestionario llamado Encuesta de Diagnóstico en el Puesto a varios cientos de empleados que trabajaban en

62 puestos diferentes. Se identificaron las siguiente cinco "dimensiones centrales":

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Variedad de habilidades, el grado en el cual un puesto requiere de una variedad de diferentes actividades para ejecutar el trabajo, lo que representa el uso de diferentes habilidades y talentos por parte del empleado.

Identidad de la tarea, el grado en el cual el puesto requiere ejecutar una tarea o proceso desde el principio hasta el final con un resultado visible.

Significación de la tarea, el grado en que el puesto tiene un impacto sobre las vidas o el trabajo de otras personas en la organización inmediata o en el ambiente externo.

Autonomía, el grado en el cual el puesto proporciona libertad, independencia y discreción sustanciales al empleado en la programación de su trabajo y la utilización de las herramientas necesarias para ello.

Retroalimentación del puesto mismo, el grado en el cual el desempeño de las actividades de trabajo requeridas por el puesto produce que el empleado obtenga información clara y directa acerca de la

efectividad de su actuación. Cada una de estas dimensiones incluye contenidos del puesto que pueden afectar la satisfacción del empleado en el trabajo.

SATISFACCIÓN CON LA SUPERVISIÓN

En lo que se refiere a la conducta de orientación a la tarea por parte del líder formal, tampoco hay una única respuesta, por ejemplo cuando los papeles son ambiguos los trabajadores desean un supervisor o jefe que les calare los requerimientos de su papel, y cuando por el contrario las tareas están claramente definidas y se puede actuar competentemente sin guía e instrucción frecuente, se preferirá un líder que no ejerza una supervisión estrecha. También cabe resaltar que cuando los trabajadores no están muy motivados y encuentran su trabajo desagradable prefieren un líder que no los presione para mantener estándares altos de ejecución y/o desempeño. Dentro de la participación que un gerente debe tener para fomentar la

motivación de los trabajadores se recomienda lo siguiente:

- Hacer interesante el trabajo: El gerente debe hacer un análisis minucioso de cuanto cargo tenga bajo su control. El gerente no debe olvidarse de una pregunta, la cual debe hacérsela constantemente: "¿Es posible enriquecer este cargo para hacerlo más interesante?". Hay un límite al desempeño satisfactorio que puede esperarse de personas ocupadas en tareas muy rutinarias. Es muy común que nos encontremos frente a personas que al ejecutar constantemente la misma simple operación sin cesar, desemboque rápidamente en la apatía y el aburrimiento de éstas.
- Relacionar las recompensas con el rendimiento: Hay muchas razones por las cuales los gerentes tienden a ser reacios para vincular las recompensas con el rendimiento. Primero y

principal, es mucho más fácil acordar a todos un mismo aumento de sueldo. Este enfoque suele implicar menos trájín y además requiere poca justificación. La segunda razón podría estar ligada a los convenios sindicales, los cuales suelen estipular, que a igual trabajo debe pagarse igual salario. Suele ocurrir en otros casos que la política de la organización determina que los aumentos de salarios responden a ciertos lineamientos, no vinculables con el rendimiento. Sin embargo, aún en estos casos, suele haber recompensas aparte del sueldo que pueden ser vinculadas con el rendimiento. Éstas podrían incluir la asignación a tareas preferidas o algún tipo de reconocimiento formal.

- Proporcionar recompensas que sean valoradas: Muy pocos gerentes se detienen alguna vez a pensar qué tipo de retribuciones

son más apreciadas por el personal. Habitualmente los administradores piensan que el pago es la única recompensa con la cual disponen y creen además, que no tienen nada para decir con respecto a las recompensas que se ofrecen. Como síntesis podría decirse que lo más importante para el administrador es que sepa contemplar las recompensas con las que dispone y saber además qué cosas valora el subordinado.

- Tratar a los empleados como personas: Es de suma importancia que los trabajadores sean tratados del mismo modo, ya que en el mundo de hoy tan impersonal, hay una creciente tendencia a tratar a los empleados como si fueran cifras en las computadoras.
- Alentar la participación y la colaboración: Los beneficios motivacionales derivados de la sincera participación del

empleado son sin duda muy altos.

- Ofrecer retroalimentación (feedback) precisa y oportuna: A nadie le gusta permanecer a oscuras con respecto a su propio desempeño. De hecho un juicio de rendimiento negativo puede ser preferible a ninguno. En esta situación, una persona sabrá lo que debe hacer para mejorar. La falta de retroalimentación suele producir en el empleado una frustración que a menudo tiene un efecto negativo en su rendimiento.
- Cuando se trata de grupos se deben tener en cuenta ciertos requisitos básicos para lograr la motivación:
 - Saber a quién poner en cierto grupo de trabajo
 - Desplazar a un inadaptado
 - Reconocer una mala situación grupal

- Las diversas investigaciones realizadas han demostrado que la satisfacción de las aspiraciones se maximiza cuando las personas son libres para elegir su grupo de trabajo. De la misma forma, las satisfacciones laborales de cada integrante se acentúan en tales condiciones, tal vez se debe a que cada uno trabaja con empleados a los que estima, con quienes prefiere colaborar y los ajustes del comportamiento son relativamente pequeños.

Medidas de higiene, salubridad y ergonomía

Los índices de ausentismo debido a enfermedades comunes motivadas por infecciones de tipo gastrointestinal, vías respiratorias, etc, reducen considerablemente la productividad y el desarrollo en las organizaciones, motivo por el cual los conceptos de higiene y salubridad son un factor muy importante.

La higiene se define como "Parte de la medicina que tiene por objeto la conservación de la salud y los medios de precaver las enfermedades" en consecuencia, para aplicar la higiene en el trabajo se deberá observar, establecer y vigilar las condiciones que conlleven y ayuden a conservar y mantener un

medio de trabajo lo suficientemente sano y confiable, en lo que a preservar la salud se refiere.

Aseo en el área de trabajo

Al terminar la jornada, tanto en el centro de cómputos como en las otras áreas de la empresa, el personal retirará y guardará todo el material utilizado. En el caso de equipos de cómputos, se procederá a cubrir a los mismos con sus respectivas fundas protectoras (tal es el caso de las terminales e impresoras), y para aquellos dispositivos más pequeños, guardarlos en sus lugares respectivos, tratando de evitar que el personal de limpieza, por algún

descuido o torpeza, puedan dañar cualquiera de estos elementos.

Se procederá a dejar por escrito y verbalmente, la no-ingestión de ningún tipo de comidas y bebidas en el área de trabajo, tanto para el personal de limpieza como para el personal del centro de cómputos y demás áreas.

En cuanto a los sanitarios, deberán mantenerse siempre limpios, ausentes de todo tipo de desperdicios, papeles, ropa, etc. que puedan constituir un peligro o, en ultima instancia, un foco infeccioso.

En toda compañía es deseable que exista una persona encargada del buen mantenimiento y aseo de los sanitarios, puesto que ahí es donde se padecen los mayores y más frecuentes contagios, por falta de aseo.

Aspectos de Ergonomía

El termino ergonomía se refiere a: “Una disciplina que estudia las condiciones adecuadas para que las personas trabajen con maquinas de forma más efectiva”.

En primera instancia, se refiere a "lugar, mobiliario y útiles de trabajo", pero en

realidad el concepto tiene un alcance más amplio.

En todo ámbito laboral, que se encuentre provisto de equipos de computación, éstos juegan un papel en contra para la salud de los usuarios.

Una de las principales enfermedades es conocida como el Síndrome del Túnel Carpiano. Sus síntomas son un mal funcionamiento del nervio mediano (uno de los dos que posee la mano), dando como resultado el mal funcionamiento del pulgar, el índice y el dedo meñique, con debilitamiento de los músculos.

También pueden producirse problemas en los pies. El pie posee 26 huesos, los que se combinan para soportar el peso del cuerpo. Aun cuando un trabajador esté sentado, los pies soportan el peso de las piernas y crean una tensión muscular.

Además de éstos, otras dolencias que suelen aparecer luego de largas horas de trabajo frente a una computadora son:

- ◆ Dolor de espaldas
- ◆ Ardor en los ojos
- ◆ Calambres en el cuello

♦ Dolor de cabeza

En la actualidad muchas compañías están proporcionando accesorios ergonómicos para trabajar frente a una computadora.

Pese a ello, lo más aconsejable es tener un lugar de trabajo ajustable. Es importante recordar que el lugar de trabajo debe adaptarse al trabajador y no al revés.

Algunas recomendaciones al respecto son:

- ♦ El lugar de trabajo debe ser amplio, limpio y libre de ruidos molestos.
- ♦ La iluminación debe ser buena. Un lugar de trabajo bien iluminado mantiene al usuario con mas energías.
- ♦ No tipear mas de media hora sin tomar un descanso.
- ♦ Alternar, de ser posible, el trabajo sobre la computadora con alguna actividad de escritorio.
- ♦ Asistir al médico ante el primer síntoma de dolor.
- No permanecer sentado por largos períodos sin tomarse un respiro y caminar un poco.
- Es recomendable realizar ejercicios que ayudan a disminuir el estrés. (ver anexo3)

Procedimientos de Emergencia

En el caso de aquellos accidentes que hayan ocasionado lesiones menores al personal, por ejemplo quemaduras pequeñas o cortes reducidos, es común el contar con tiempo disponible suficiente para atender los accidentes.

En los casos en que se hayan producido accidentes graves, el primer cuidado será el de buscar ayuda médica capacitada. Deberá avisarse al servicio médico de emergencia más próximo. Dicho servicio puede ser el prestado por la enfermera, el oficial médico o el servicio local de ambulancias, según sea el caso. De necesitarse una acción inmediata para minimizar el daño, o incluso evitar que se produzca la muerte del accidentado.

Es en estos casos en donde puede resultar de gran importancia la prestación de primeros auxilios por alguien entrenado para darlos.

Todo el personal que pueda, deberá asistir a un curso de primeros auxilios,

siendo esto obligatorio para todos los jefes o encargados de cada una de las áreas que integran a la compañía, y, de ser posible, mantenerse capacitados, siguiendo cursos de actualización a los intervalos especificados.

3.6 ELEMENTOS TÉCNICOS Y PROCEDIMIENTOS

Se refiere a la definición por escrito de la información necesaria para garantizar la operación y utilización segura de los equipos e información que estos almacenan, entre los que podemos definir:

- ◆ Procedimientos de Respaldo de la información
- ◆ Recomendaciones generales para mantenerse alejado de los virus
- ◆ Sobre desarrollo de sistemas y otros servicios informáticos
- ◆ Políticas y Lineamientos Específicos Sobre los Derechos de Autor, Adquisición de Software y Uso de Licencias
- ◆ Sobre los Contratos con Proveedores de Bienes o Servicios Informáticos.

RESPALDO DE INFORMACIÓN

Lo primero que debe considerar para asegurar la información diseñada es respaldarla. Muchos de los usuarios no hacen un respaldo adecuado debido al costo de tiempo y de dinero. Sin embargo, es sino hasta que se presenta un problema grave y se encuentran

sin sus datos y archivos importantes que se dan cuenta de lo valioso que resulta hacer un óptimo respaldo.

Una buena regla general para que esto no suceda es nunca dejar que el intervalo entre respaldos sea mayor al tiempo que estaría dispuesto a perder.

PROCEDIMIENTO DE RESPALDO

Respaldar archivos significa almacenarlos, normalmente se almacena en diferentes sitios, para su posterior uso.

Respaldar o archivar puede implicar hacer copias de seguridad, las cuales tienen como objetivo la seguridad e integración confiable de archivos. Por lo regular, respaldar es copiar archivos a los diferentes almacenamientos físicos o medios removibles, como: cintas magnéticas, disquetes (3½), CD gravables, discos duros etc.

Cuando respalde su sistema, debe tener presentes las opciones disponibles de software y de hardware.

Existen un gran cantidad de software en el mercado con diferentes capacidades y características. Aquí se mencionan aquellas de uso más común en respaldos en equipos con sistema operativo MS-DOS, y los servidores con sistema operativo windows NT.

RESPALDOS EN DIFERENTES MEDIOS FÍSICOS

- ◆ Respaldo en disquetes (discos flexibles)
- ◆ Respaldo en unidades de cinta
- ◆ Respaldo de disco duro a disco duro
- ◆ Respaldo en CDS.

Una manera muy común de realizar respaldos es por medio de disquetes, los cuales pueden ser muy útiles, para usuarios que suelen realizar sus trabajos en una PC. Los disquetes un medio físico de almacenamiento muy sencillo de manejar y de cuidar.

Respaldo en disquetes (discos flexibles)

Un disquete es un disco flexible que se encuentra cubierto con una capa de oxido el cual es utilizado para

almacenar información, también son conocidos como discos floppy.

Tipos de disquete

Pueden ser de dos tipos:

- ◆ El tipo de disquete más utilizado es el de alta densidad. El cual tiene una capacidad de almacenamiento de 1.44 MB.
- ◆ Disquete de doble densidad. El cual tiene una capacidad de almacenamiento de 720 k.(casi no se usan).

RespalDOS en unidades de cinta

Realizar el respaldo en un sistema de cinta es la forma más fácil y cómoda de asegurar nuestra información de computadoras.

Hacer los respaldos en cinta resulta más conveniente que hacerlo en un disco flexible, pues su capacidad es mucho mayor. Una sola cinta, de acuerdo a su formato, puede contener desde 40MB hasta 5G(giga bites) de información.

Formatos de cinta

El Quater-Inch Commitee (Comité cuarto de pulgada o QUIC) emite los estándares para aspectos tales como: adaptadores controladores de cinta-unidad, dimensiones físicas de los cartuchos y comandos comprensibles para las unidades de cinta.

La organización QIC se formó para desarrollar formatos estándares en las unidades de cinta de cartucho de datos DC-600 y DC-200, entre otros.

El tipo se selecciona dicta la capacidad de almacenamiento de la unidad de cinta. Diversos tipos de sistemas usan muy diferentes tipos de medios magnéticos, entre los estándares más utilizados son:

Cartuchos DC-200. La cinta es de 2.415x3.188x0.570 pulgadas en longitud, anchura y profundidad, con plato base de metal pesado y tiene una capacidad de 80 M.

Cartuchos DAT de 4mm (cinta de audio digital). A primera vista, este cartucho se ve como un cassette de audio normal, aunque ligeramente más pequeño. Estos cartuchos se presentan en diferentes formatos de grabación, pero el de mayor uso es el de

almacenamiento digital de datos, o DDS para abreviar.

También hay disponible otro formato denominado DataDat. La tecnología de grabación es similar a la de unidades de audio casete digitales y se lleva a cabo en un formato de rastreo helicoidal. Las cintas DAT pueden almacenar hasta 1.3 giga bites (1 giga bite equivale a 1,024M).

Cartuchos de 8mm. Estos cartuchos, que utilizan la cinta de video de 8mm desarrollada por Sony para cámaras de video, comprende uno de los sistemas disponibles de respaldo con mayor capacidad. La mayoría de las unidades de almacenamiento 2.3G. Aunque hay disponible inclusive unidades de mayor capacidad. La grabación se efectúa físicamente como un rastreo helicoidal; es decir, en forma de hélice o que se encuentra formado por varias “placas”.

Cada tipo de sistema en cinta respalda con facilidad más de un giga bite en una sola cinta y puede realizar un respaldo completo del disco entero en un poco más de tres horas. Los respaldos parciales toman sólo minutos o segundos.

Recomendaciones

Capacidad:

Se recomienda comprar las unidades de cinta con una capacidad igual o mayor del tamaño total de su disco duro, incluyendo todas las unidades lógicas en el disco. Esto permite respaldar todo el disco en una sola cinta.

Unidad de Cinta interna o externa:

Considera la utilización de las unidades de cinta externas cuando hay que respaldar varias PC que no están conectadas a red. Sin embargo, no es una solución adecuada, ya que cada PC necesita su interfaz a la unidad de cinta.

En lo relativo a la PC's no resulta muy caro agregar una interfaz para la unidad de cinta en forma de un adaptador anfitrión o soporte conector externo. Cuando se trata de una gran cantidad de PC, tiene más sentido respaldar todo en una unidad de cinta.

Estrategia de respaldo:

Cuando en unas cuantas PC descansa la administración de la dependencia es necesario respaldar diariamente.

Programas y documentos:

Los documentos y programas deben estar contenidos en distintos directorios, ya que así se realizará el respaldo de los programas que tengan cambios y de los documentos donde se haya realizado el cambio.

Respaldo de disco duro a disco duro

Otro medio físico en donde se puede realizar un respaldo es en el disco duro, puede ser tanto en un disco interno como en uno externo. Una de las grandes ventajas es que se puede realizar el respaldo total del disco que se desea respaldar a otro, siempre y cuando sea de la misma capacidad de almacenamiento o mayor.

Por ejemplo, si se tuviesen varias computadoras personales y existe la necesidad de respaldar el disco duro de una de ellas, se puede realizar este respaldo con una copia para otra de las computadoras en donde se quiera tener la información.

Para realizar el respaldo de archivos se necesita la conexión entre dos computadoras, de esta forma los archivos del disco duro de una

computadora se pueden almacenar en el disco duro o en disquetes de la otra computadora.

Respaldo en CD'S

Son considerados como los nuevos sistemas de almacenamiento. Podemos encontrar los CD's grabables y los CD's regrabables.

CD-ROM Grabable

Este medio nos permite almacenar hasta 650 megas de información. La grabación que se realiza es física, pues el rayo láser produce una pequeña hendidura en el disco. Como herramienta de respaldo, nos proporciona una mayor confiabilidad ya que la información grabada no se puede borrar de forma accidental y se puede disponer de la información de manera rápida y segura.

Una ventaja es que se puede emplear en cualquier ordenador del mundo; además de que la tecnología tiende a que se tenga en cada computadora personal una unidad de CD que tenga las características de poder escribir y leer.

El CD-ROM grabable puede ser útil para programas comerciales y archivos de datos históricos que se necesiten conservar.

CD-ROM Regrabable

Es un buen dispositivo de almacenamiento de información, el cual debe considerarse para el futuro como un apoyo importante en la manipulación de los datos.

Tiene una capacidad de almacenamiento de cerca de 660 megas; además podemos borrar y grabar datos, por lo que, en teoría, un solo disco puede almacenar miles de gigas a lo largo de su vida útil.

Cuando algo de lo grabado ya no sirve, sobre todo los backups, se borran y el disco puede volver a utilizarse. La seguridad, en el caso de equipos compartidos por muchos usuarios, es mucho mayor, que cada uno de ellos puede trabajar en su propio disco, como si fuese un disco duro, y llevárselo a casa tranquilamente.

Los CD removibles pueden servirnos para procesar el trabajo de cada día, así

como los backups y el almacenamiento de datos cambiantes.

Software de respaldo

A continuación se explicarán varias formas y comandos que se utilizan para realizar los respaldos en dos Sistemas Operativos Windows NT y MS-DOS. También se presentan algunos software con tarea específica; es decir realizan el respaldo en un medio físico especial (los medios físicos pueden ser algunos de los que se expusieron en el tema anterior).

Se describen algunas opciones en MS-DOS, por considerar que la mayoría de las computadoras personales cuentan con este sistema operativo, y los recursos que se necesitan para respaldar la información son accesibles hasta en opciones más complejas.

MS-DOS

- ◆ Copy y Xcopy
- ◆ Comprimir Archivos

Copy y Xcopy

Una forma muy común para realizar el respaldo a diskettes, desde MD-DOS es

hacerlo con el comando copy. Es recomendable utilizar el comando copy, y redireccionar la información del disco duro al disco flexible.

El comando copy se utiliza para copiar uno o más archivos en la unidad de disco que se especifique. Si el tamaño de los archivos que se desea respaldar es mayor que la capacidad de almacenamiento del disco entonces no se podrá ejecutar el comando.

¿Cómo realizar el respaldo en disquete?

Primer paso:

Verificar que el disco flexible por utilizar se encuentre con formato, así como la existencia de espacio disponible para el almacenamiento.

Segundo paso:

Verificar la ubicación del archivo que se va a guardar dentro del disco duro.

Tercer paso:

Realizar el respaldo de la siguiente forma:

C:/copy nombre del archivo origen ,
dirección destino

Ejemplo: C:/copy proyecto a:

1 archivo(s) copiado(s)

C:/contabilidad copy nomina a:

1 archivo(s) copiado(s)

De esta manera la información del archivo del disco duro es copiada al diskette.

También se podrá realizar en forma inversa, es decir de diskette a disco duro.

Otra posible solución para respaldar la información es realizar el respaldo con el comando XCOPY, el cual permite transferencias avanzadas de archivos entre disco y directorios. Se debe considerar su utilización para copias en grupos de archivos, porque generalmente es más rápido que COPY. También es conveniente para transferir archivos almacenados en varios directorios porque XCOPY maneja la selección de archivos que estén en varios lugares del disco.

La forma en que debe de llevarse a cabo el respaldo en los discos, son de la misma manera que los pasos descritos en COPY.

A continuación se describe la sintaxis y ejemplos para su uso.

C:/xcopy origen destino opciones

Ej. C:/xcopy x:/glosario/*.* a:

Reading source file(s)

C:/glosario/nombre.doc

C:/glosario/taller.doc

C:/glosario/taller1.doc

3 file(s) copied.

Comprimir archivos

Para la mayoría de los usuarios de PC, “archivar” implica empaquetar archivos pequeños en uno mayor. Gracias a los complejos algoritmos de compresión, un archivo de gran tamaño de información, actualmente puede ocupar menos espacio en el diskette a la hora de realizar un respaldo. Este proceso permite almacenar unos cuantos archivos compactos y consultarlos después ya sea desde el disco duro o diskette.

Normalmente se pueden comprimir las imágenes gráficas, resúmenes, programas, figuras y tablas, en un archivo manejable. De esta forma utilizando el programa PKZIP, por ejemplo, se puede comprimir el texto de un libro entero y se puede situar en un único archivo que ocupa menos espacio en disco.

Hay algunos programas de compactación y de almacenamiento que

se encuentran en el mercado. Uno recomendable es PKZIP. El cual permite comprimir el texto de un libro entero y se puede situar en un único archivo que ocupa menos espacio en disco.

Hay algunos programas de compactación y de almacenamiento que se encuentran en el mercado. Uno recomendable es PKZIP. El cual permite comprimir unos cuantos archivos, incluso dispersados por directorio, en un único archivo zip más manejable.

Los archivos se pueden extraer todos a la vez o de uno en uno utilizando el programa PKUNZIP. Este mismo programa permite la descompresión de los archivos y permite ver la información contenida en ella.

Utilizar el PKZIP es una forma práctica de almacenar información para que ésta no ocupe demasiado espacio en el disco duro.

La sintaxis para descomprimir un archivo en el sistema operativo ms-dos es:

C:/pkunzip archivo comprimido

Un ejemplo de descompresión de archivo es :

Ej. C:/pkunzip glosario.zip

C:/dir

Glosario

También se puede ocupar el winzip, para windows 3.x y windows 95, la

compresión de los archivos deseados es la misma pero de forma gráfica.

Se puede analizar la compresión de los archivos antes de copiarlos o respaldarlos en un diskette al utilizar COPY o XCOPY.

SOFTWARE PARA UNIDADES DE CINTAS

Es importante considerar que para realizar los respaldos con cintas magnéticas se debe contar con un software que sea compatible con la interfaz y con los medios magnéticos; en caso contrario, el software no reconocerá el formato de datos y por tanto no podrá intercambiar información entre las unidades.

Para una mayor seguridad en el respaldo es más confiable utilizar el software y hardware que, conjuntamente, nos proporciona el fabricante.

Un software que se puede utilizar para el respaldo en cintas magnéticas es el estándar denominado SYTOS (sistema operativo de cinta sytron).

Todo software para respaldo debe tener las siguientes características:

- ◆ Que pueda respaldar una partición completa de DOS (respaldo total de volumen)
- ◆ Que pueda respaldar cualquier archivo de forma individual (respaldo de archivo por archivo)
- ◆ Que pueda combinar varios respaldos en una sola cinta
- ◆ Que pueda operar el software como comandos en archivos BATCH de DOS
- ◆ Que trabaje en una red
- ◆ Que pueda dividir un disco muy grande en varias cintas
- ◆ Que se pueda verificar por completo.

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga ”

Consejos para respaldar

De preferencia tenga tres cintas para respaldar la información de las PC, la primera cinta se podrá utilizar el cuarto día que se realicen los respaldos, esto asegura que usted tendrán dos cintas de respaldo sin modificar, asegura que

tienen una cinta con la información adecuada y una más no con todas las actualizaciones (en el caso de que suceda algo a alguna de ellas).

Algunos programas permiten definir los directorios y archivos por respaldar en una determinada hora.

SOFTWARE DE RESPALDO PARA DISCO DURO A DISCO DURO

◆ Interlnk

◆ Laplink

Es un software que tiene la capacidad de poder respaldar la información de un disco duro a otro disco duro; es decir de una computadora a otra.

Ambas computadoras deben de encontrarse conectadas desde el puerto paralelo o el puerto serial y ejecutar el programa correspondiente desde el sistema operativo en cada una de las computadoras.

Un punto importante que se debe verificar es si los programas se encuentran instalados en cada una de las computadoras. El sistema operativo MSDOS tiene software que ayuda a realizar este tipo de respaldo. Será

necesario que instala el software si no se encuentra instalado en las computadoras.

Una vez que tenga conectadas ambas computadoras, una de las computadoras va a trabajar como servidor, la cual compartirá sus recursos con la computadora cliente. Cada programa lo deberá correr desde el sistema operativo.

Tipo de software

Alguna opción es utilizar INTERLNK del sistema operativo DOS o LAPLINK.

INTERLNK

Permite que una computadora utilice la información y los programas en los discos de la otra computadora.

Una vez que se establece la conexión, la computadora servidor queda temporalmente no disponible, pero la computadora cliente puede acceder los discos físicos de la computadora servidor. En esencia, es como si la computadora cliente tuviera discos en sus unidades propias más las unidades adicionales que podemos llamar pseudo unidades los cuales puede redirigirse con INTERLNK a discos reales que están físicamente ubicados en otra computadora.

Para preparar la conexión entre las dos computadoras, se necesita hacer lo siguiente:

Tener en cada computadora un puerto disponible, serial o paralelo.

Un cable adecuado para conectar los dos puertos disponibles. Este puede ser un cable paralelo un cable serial.

Por lo menos 130K de memoria disponible en la computadora servidor y por lo menos 16 k de memoria libre en la computadora cliente.

Se debe conectar el cable adecuado a los puertos del mismo tipo en cada computadora. La computadora que se planea utilizar como servidor debe tener

el programa INTERSVR/EXE disponible.

¿Cómo utilizar el INTERLNK?

Para establecer la conexión de programas entre dos computadoras se debe ingresar INTERSVR desde el llamador de comandos de la computadora servidor.

Mientras que la información en sí se transfiere mediante la conexión de computadoras; un renglón de estado, que aparecerá en la parte inferior de la pantalla, describirá el puerto en uso, así como la información de la velocidad de transferencia.

La mayor parte del trabajo real ocurrirá en la computadora-cliente desde el llamador de comandos.

Cualquiera que sea la computadora cliente, debe prepararse adecuadamente, siguiendo el procedimiento que se describe a continuación:

Primero se debe instalar la rutina controladora INTERLNK.EXW. en CONFIG.SYS y reiniciar la computadora. Utilizando las opciones adecuadas en la línea de la rutina controladora puede establecer qué

identificadores de dispositivo se utilizarán en la máquina cliente para representar las unidades físicas en el servidor. En la mayoría de los casos se pueden aceptar las opciones preestablecidas de la rutina controladora. En el archivo CONFIG.SYS deberá agregar la siguiente línea:

```
DEVICE=C:/DOS/INTERLNK.EXE
```

opciones

La rutina controladora utiliza como nombres de las pseudo unidades, las letras siguientes de las unidades ya existentes en la computadora-cliente. Las siguientes solicitudes desde la computadora-cliente respecto a los archivos en las pseudo unidades se redirigirán a través de la conexión INTERLNK-INTERSVR hacia los discos de la computadora servidor.

Una vez instalada la rutina controladora INTERLNK.EXE, puede utilizar el programa INTERLNK desde el llamador de comandos. También es posible agregar una o más líneas INTERLNK al archivo UTO EXEC.BAT lo que le permitirá establecer la conexión entre las unidades

cliente redireccionadas y las del servidor.

Podrá correr el programa INTERLNK desde el llamador de comandos solamente si durante el arranque del sistema, este se instaló correctamente como rutina controladora. Por ejemplo, para redireccionar las solicitudes de la computadora cliente hacia la unidad F: en la unidad C: servidora, deberá ingresar el siguiente comando desde el llamador en la computadora cliente:

```
INTERLNK F:=C:
```

Con esto, podrá utilizar la unidad F: en la computadora cliente además de tener disponible la unidad C: en la máquina servidor como unidad actual.

Para realizar el respaldo de un disco duro a otro solamente debe seguir los pasos del comando COPY del sistema operativo dos, el cual ya fue presentado en el tema de los respaldos de diskettes. Para abrir, correr o respaldar archivos en el disco duro de la computadora cliente debe verificar que haya sido redireccionada la información de forma correcta.

Una vez que termine el acceso a programas mediante la conexión, puede

volver a tener el control sobre la máquina servidor mientras se desconectan las dos máquinas, con sólo oprimir ALT+F4 en la computadora servidor. Puede restablecer la conexión en cualquier momento al ingresar a INTERSVT otra vez.

LAPLINK

Le permite la comunicación entre dos computadoras. Con esta conexión se podrá manipular la información y los programas que se encuentran en los discos de las computadoras.

Al realizar la conexión, la computadora-servidor quedará temporalmente sin disponibilidad; pero la computadora-cliente puede acceder los discos físicos de la computadora-servidor.

La diferencia de INTERLNK, este software le permitirá usar las computadoras tanto como servidor o como cliente, lo cual resulta importante ya que podrá compartir los recursos de ambas computadoras.

LAPLINK necesitará de las mismas características que INTERLNK para

poder realizar la conexión entre las dos computadoras.

¿Cómo funciona este software?

Deberá ingresar LAPLINK desde el sistema operativa dos con la siguiente sintaxis:

C:/LL5.EXE

C:/LL5

De esta forma aparecerá en pantalla el menú principal de LAPLINK.

En la parte superior de la pantalla de LAPLINK encontrará la BARRA de FUNCIONES. Estas funciones ayudan a la manipulación de los datos que se pretenden respaldar, entre alguna funciones encontramos file (archivo), del disk (disco), el select (selección), options (opciones), etc.

La siguiente pantalla está dividida verticalmente en dos partes, en una de ellas se encuentran los directorios y archivos, de la computadora que trabaja como servidor; y del otro lado, aparecen las opciones de conexión (cose a connection). Estas opciones son: conexión vía cable serial o paralelo, modem vía red e instalación remota, la

conexión remota es la que explicaremos más adelante.

Debajo de la función cose a connetion, aparece otra función llamada LABORATORIO (local), esta sirve para saber a qué unidad de disco se realizará el respaldo. De igual forma indicará en qué unidad de disco se va a querer hacer el respaldo.

En la computadora que se encuentra como servidor podrá elegir qué archivos desean respaldar. Para realizar este paso colóquese en los archivos o directorios que se van a respaldar, los mismos que seleccionará con la barra espaciadora.

Si quiere crear un directorio en cualquiera de las dos computadoras conectadas, siga los siguientes pasos:

Para colocar los archivos seleccionados sólo debe activar la opción DISK de la barra del menú. Posteriormente con las teclas con flechas colóquese en la opción MAKE DIRECTORY y oprima la tecla ENTER, enseguida le aparecerá una ventana donde deberá escribir el nombre del directorio. Por último, oprima la tecla enter. De esta forma habrá creado el directorio para colocar los archivos que va a respaldar. A

continuación realizará la copia de los archivos que se encuentran seleccionados, para este sólo se debe oprimir la tecla F2.

En la pantalla de LAPLINK, en la parte inferior, hay una indicación de F2 junto a la palabra copy y una flecha, esta flecha se activará cuando oprima F2, la cual indica los archivos que estará respaldando.

De este modo podrá ver en la pantalla los archivos copiados y hacia dónde, en qué lugar, fueron respaldados.

Para salir del programa sólo váyase a la barra del menú principal donde deberá colocarse en la opción EXIT y teclear ENTER.

De esta forma usted podrá realizar el respaldo de archivos en el disco duro de otra computadora, además de poder trasladar la información de la computadora que trabaja como servidor a la que trabaja como cliente.

TIP

Una de las desventajas de los disco duros es que pueden fallar o sufrir “desastres” y perder toda la información almacenada en ellos. Dada la magnitud de información almacenada en estos

dispositivos, el valor del contenido corre un riesgo mayor que el de la pérdida de un diskette. Es por ello que se debe

respaldar el disco duro periódicamente, para no correr el riesgo de perderlo.

Software de respaldo para CD's

El software que se utiliza para poder realizar los respaldos en CD's en proporcionado por el vendedor, por lo cual cada software trae consigo información de cómo poder utilizar los DC's para respaldar. De alguna forma mencionaremos los pasos más importantes que debe considerar si quiere tener un respaldo seguro.

Utilizando un CD grabable

1. Primero debe escoger la información o archivos que desea respaldar en CD
2. Utilice equipo con disco duro que almacene como mínimo la capacidad del CD que es de 650 MB.
3. La información que va a pasar el CD se debe revisar anticipadamente para conocer su:

- a) Capacidad: se lleva la cuenta del volumen de memoria que ocupan los datos, con el fin de conocer la memoria restante en el CD y para saber si se puede llevar a cabo el respaldo en un solo CD.
- b) Los archivos necesarios: debe conocer todos los archivos que se necesitarán para que una aplicación funcione de modo que sólo sea necesario instalar el CD para que funcione adecuadamente la misma.
- c) El formato con que se guardará: la información se puede guardar en solo CD, al compactar distintos archivos en un solo directorio para

que cuando necesite un archivo, este se pueda llamar desde el mismo directorio. No es recomendable juntar archivos en un solo directorio si previamente no se ha probado el correcto funcionamiento del mismo guardado en conjunto, pues estos pueden causar un error una vez que ejecute la aplicación.

- d) Software: con el fin de que las ventas incrementen su volumen, cuando adquiera el hardware para quemado de CD el proveedor le proporcionará el software de utilización del mismo.

ADAPTEC actualmente produce el software para el quemado de discos compacto, llamado: Easy Cd Creator Pro.

Algunas otras compañías producen:

- ◆ Gear
- ◆ Corel CD Creator

La elección del software generalmente depende de las características del hardware que se va a utilizar, pues este

debe ser configurado respecto al primero.

Del mismo modo puede llegar a existir un software eficiente pero, de no existir compatibilidad con el equipo utilizado, no será posible la utilización del mismo.

Guía para respaldar en CD

Las distintas aplicaciones permiten realizar respaldos en CD donde podemos especificar distintas características de respaldo; generalmente éstas se definen de la siguiente manera:

Escoja el tipo de CD, el cual puede variar entre: música, audio, datos, (música y datos).

Lo anterior significa que, previo al quemado del CD para respaldar información en el mismo, debe especificar el tipo de información que va a respaldar, esto con el fin de que la aplicación nos permita proporcionar distintos orígenes para realizar el respaldo de la información.

Utilizando archivos como origen, las posibilidades puede ser:

1. Tomar los directorios uno a uno y mandarlos
2. Tomar una sola imagen ISO y mandarla al quemado (una imagen ISO es una recopilación de distintos archivos y directorios que se realizan con anterioridad a la ejecución del quemado del CD para mandarla o respaldarla como un solo paquete de información).

Definir parámetros es una parte de suma importancia en el quemado de un CD, pues pueden ayudarnos en la corrección de errores posibles en el quemado; o en la realización de respaldo antes de que el mismo sea realizado, previniendo el gasto innecesario de recursos.

Las distintas aplicaciones de software para el quemado pueden permitirle definir parámetros como:

1. Realización de pruebas: Éstas se llevan a cabo con el fin de observar el comportamiento del CD llevando a cabo una simulación de grabado o quemado del CD. Si dichas pruebas se realizan con éxito, se procederá a realizar el respaldo,

de lo contrario daría oportunidad de corregir errores antes de quemar el mismo. La desventaja que puede traer la realización de pruebas previas al quemado, es la de multiplicar el tiempo de respaldo al doble. Sin embargo, los beneficios en el ahorro de material puede justificar este gasto de tiempo.

2. Escoger la velocidad de quemado: Aunque quiera utilizar la máxima velocidad de grabado, la decisión de ocupar una u otra no depende de la prisa que el usuario tenga por realizar un respaldo, sino por el contrario, pues la velocidad es un punto clave que dependerá del ancho de banda que maneja el hardware utilizado para quemar áreas e ir insertando información en los clusters. Ya que si la velocidad elegida va más allá de la capacidad de quemado del hardware, puede producir un error irreparable en el caso de que utilice discos de un solo

quemado o que sólo se pueden grabar una vez.

Recomendaciones

La tecnología nos ofrece nuevos y mejores dispositivos para respaldar. En el caso de los CD, se puede encontrar diversas formas para realizar los respaldos, pues existen distintos tipos de CD:

- ◆ Los que sólo se pueden grabar o quemar una sola vez
- ◆ Los que pueden ser grabados o quemados varias veces.

La elección del tipo de CD que se va a utilizar dependerá de la capacidad de compra del usuario, del software con el que actualmente cuente, lo mismo que el hardware al que tenga acceso, pues existe un tipo de hardware para cada tipo de CD.

Por otro lado es recomendable no tener procesos en background ni de ningún otro tipo ejecutándose simultáneamente, pues estos requieren tiempo de procesador lo que puede interrumpir el quemado de un disco y en consecuencia causar un fallo o error irreparable.

Desconectar la máquina de red es también una buena medida al realizar un respaldo en CD, pues del mismo modo el realizar conexiones o contestación de peticiones de otras máquinas resta tiempo de proceso lo que puede bajar la velocidad de transferencia de datos y que ocurran errores irreparables.

Lo anterior se da tomando en cuenta que el CD utilizado sea solo para escribir una vez, pues cualquier interferencia en el quemado del mismo, lo hace inservible ocasionando alza de costos y gasto de tiempo.

Respaldo del servidor con window NT

¿Qué es ArcServer?

Arcserve es un producto creado por la empresa Cheyenne, y su objetivo primordial es realizar respaldo de la información que se tiene en una computadora, este respaldo es de vital importancia ya que en cualquier situación contingencial en la cual se pierda datos se puede recuperar esta información perdida.

Arcserve tiene la facilidad de poder realizar respaldo de la máquina donde se encuentra instalado, así como también de cualquier estación que se encuentre en la misma red y que la máquina donde está instalado la vea.

Trabajos de Arcserve(JOBS)

Arcserve trabaja en base a Job's o trabajos, que se generan en el mismo

para poder realizar casi cualquier actividad. Existen varios tipos de Job, están los de respaldo de información, que son con los cuales se traslada la información que contiene la máquina a medios magnéticos. Además se realizan trabajos de restauración de información que es el proceso de recuperar información perdida desde las cintas.

El Device Management

Además el Arcserve tiene un módulo adicional llamado Device Management, este se utiliza para verificar el estado del hardware de respaldo así como poder hacer operaciones con los dispositivos como lo es el formato de las cintas, la verificación de las mismas, Etc.

Creación de Trabajos de Respaldo de Información

Dentro de los procedimientos se necesita crear trabajos de respaldo de información en el cual se almacene la

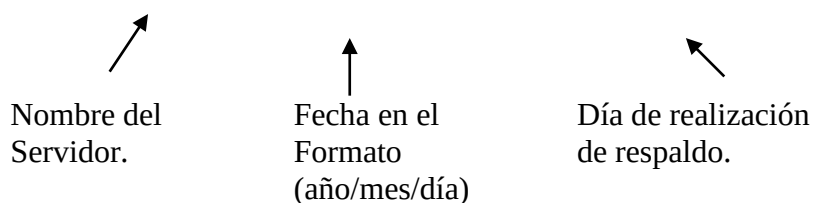
información total del servidor. A continuación se describen los procedimientos a seguir para realizar un

respaldo de la información.

Políticas de Respaldo

- ◆ De manera común los respaldos que se generan deben ser calendarizados para ser ejecutados cada determinado número de tiempo a continuación se describe paso a paso como generar un backup que debe quedar calendarizado para que se realice diariamente y el horario de ejecución será a las 6:00 p.m.
- ◆ Después de generar un respaldo éste debe ser verificado con el objeto de cerciorar que la información fue almacenada con éxito.
- ◆ Las cintas deberán estar formateadas al momento de realizar el respaldo y deberá existir únicamente una sesión de respaldo en cada una de ellas (Una cinta por cada día laborado).
- ◆ Las viñetas deberán contener información importante tal como el nombre del servidor respaldado, la fecha y día de realización del respaldo. Ejemplo, la viñeta para el respaldo del día 20 de mayo de 2001 del servidor quedaría:

MINPRE_010520_VIE

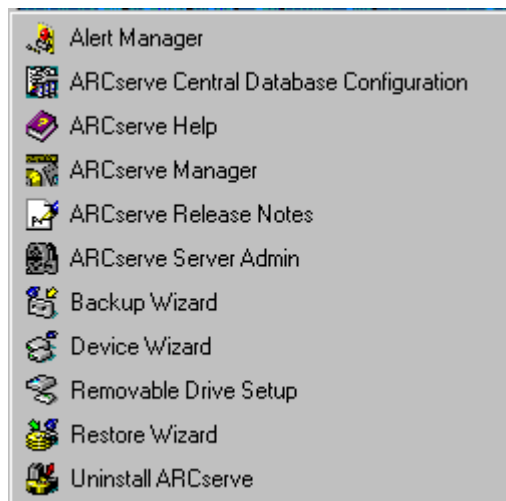


- ◆ Luego de realizar los respaldos las cintas deben ser almacenadas fuera de la institución en un lugar seguro, limpio y seco (Una opción válida puede ser la caja de seguridad de un banco)
- ◆ La política de respaldo define que es necesario realizar un backup completo diario el cual debe ser almacenado por un tiempo no menor

- ◆ a 30 días hábiles después de los cuales las cintas pueden ser recicladas o reutilizadas con un nuevo respaldo.
- ◆ Además es necesario almacenar un respaldo verificado del final de cada mes, el cual quedará de histórico por un periodo no menor a 5 años.
- ◆ Es necesario realizar limpieza de las unidades DAT, para lo cual se utilizan cintas de limpieza del tipo Cleaning Cartridge de 4mm DDS. Esta limpieza debe ser cada 3 días o antes cuando la unidad lo solicite.
- ◆ Para la realización de respaldos únicamente se utilizarán cintas del tipo DDS de 90 metros y 4mm.
- ◆ Los cuidados a tener con las cintas son similares a la de otros medios magnéticos tales como no exponer a temperaturas muy elevadas (calor) o muy bajas (frío), no exponer campos magnéticos, protegerlas de la humedad, no tocar la cinta, etc.

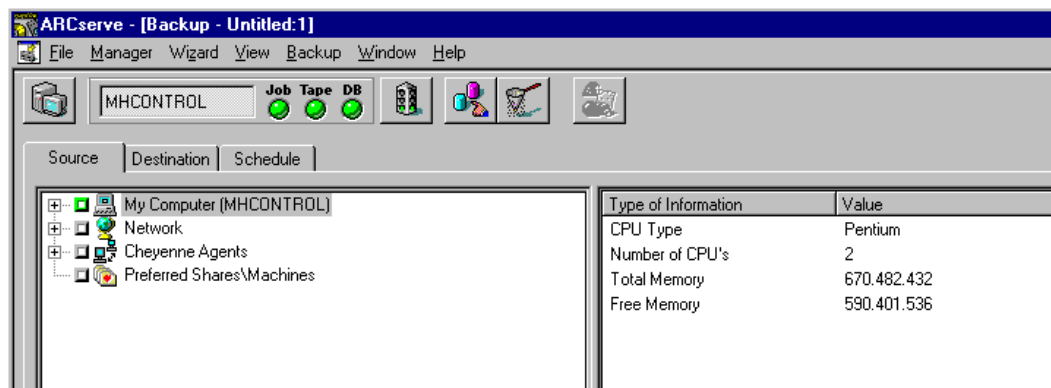
Creación de un Trabajo de Respaldo

Para cargar arcserver se selecciona la opción Arcserve Manager en el menú inicio, arcserve para Windows NT.



Luego se selecciona el Icono de Backup y aparece la pantalla para la elaboración del Job de respaldo, en esta pantalla se realizan tres pasos importantes, primero se selecciona el origen del respaldo, o sea los archivos o directorios que se van a respaldar, luego se selecciona el destino, que en nuestro caso es la unidad DAT configurada en cada servidor y como tercer y último paso se calendariza el respaldo para que este sea ejecutado cada determinado número de tiempo.

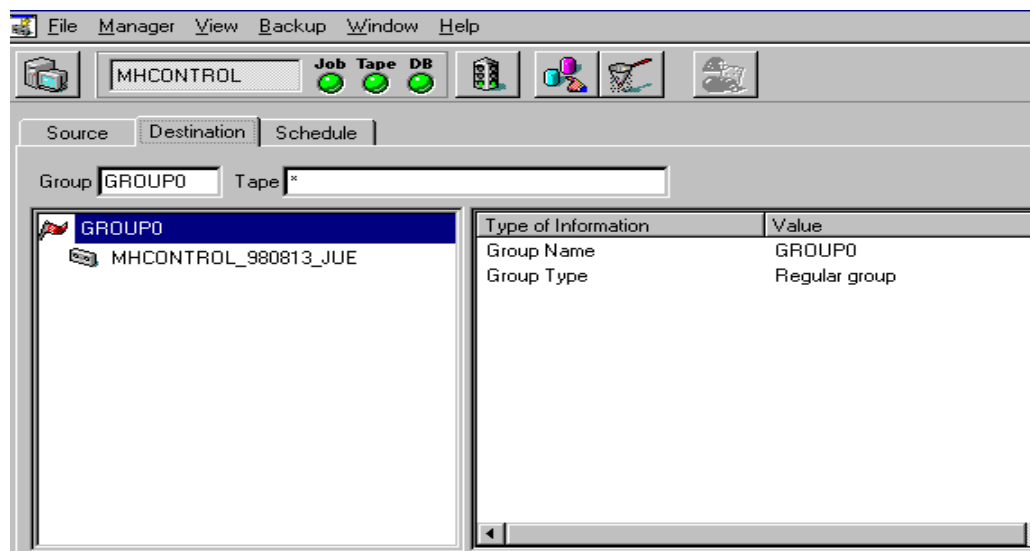
A continuación se muestran cada una de las pantallas para realizar un Job de Respaldo, en esta se muestran tres pestañas (Source, destination y Schedule) en la pestaña de origen se seleccionan los datos a los cuales se desea realizar respaldo, como se muestra en la siguiente gráfica.



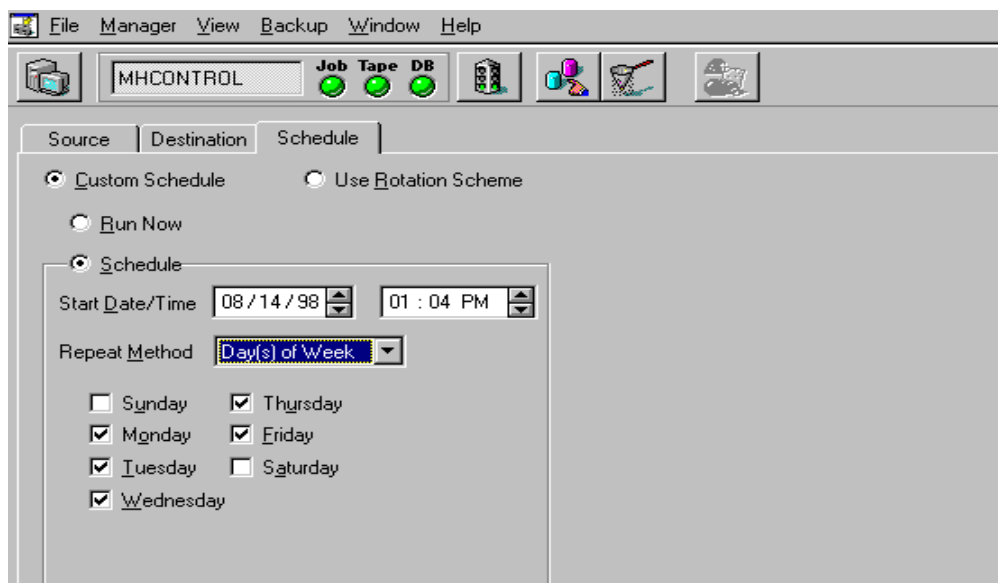
Seleccionar en la carpeta Source, My computer, con la cual se indica que se le hará respaldo a toda la información.

- Seleccionar la carpeta Destination, en la cual se indicará el destino del

respaldo, en este caso el destino se deja con *, para que el respaldo lo realice en un tape no importando la viñeta de la misma.



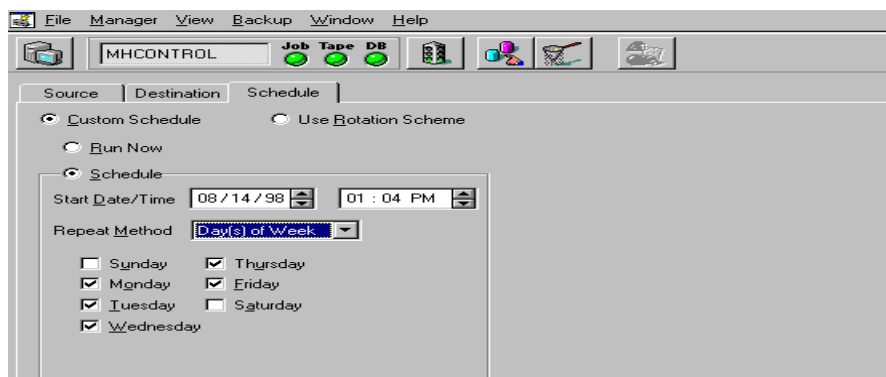
- Luego se configura la calendarización con lo cual se define que el respaldo se realizará diariamente.



En este punto se selecciona Custom Schedule, luego se marca la opción Schedule, a continuación se define el día y la hora a la cual se realizará el respaldo, s continuación se define el

repeat meted en day(s) of week, y luego se marca los días que se realizarán respaldo.

- A continuación se selecciona el icono de opciones (OPTIONS)



En la cual se selecciona la carpeta de Verification, en ella seleccionar que compare el contenido del tape contra el disco.

Para finalizar se ejecuta el Trabajo de respaldo oprimiendo el boton que representa un semaforo.

Creación de Trabajos de Restauración

Políticas de Restauración

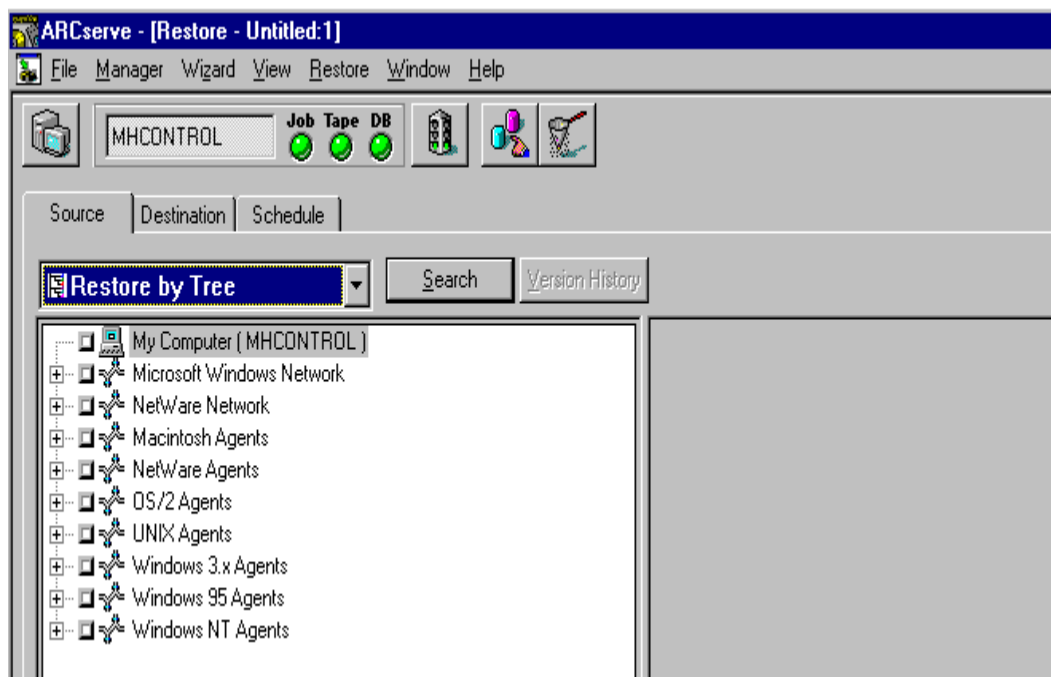
Para realizar la restauración de datos de una cinta es necesario para garantizar no sobrescribir información, crear una carpeta temporal a la cual se restaura la información, si esta información es satisfactoria se sobre escriben los archivos dañados y se borra la carpeta temporal.

Además es necesario realizar una bitácora de archivos restaurados para,

respaldar los procesos realizados y si este proceso fue correcto.

Para realizar una restauración debe haber una solicitud por parte del interesado, esta solicitud debe ser por escrito y debe contar de firma y sello de la institución. Esta documentación debe ser archivada para efectos de auditoria.

Procedimiento de Restauración.



Seleccionando el icono de restauración aparece la pantalla de restauración de archivos, esta pantalla es muy similar a la de Backup pero solicitando la información a la inversa.

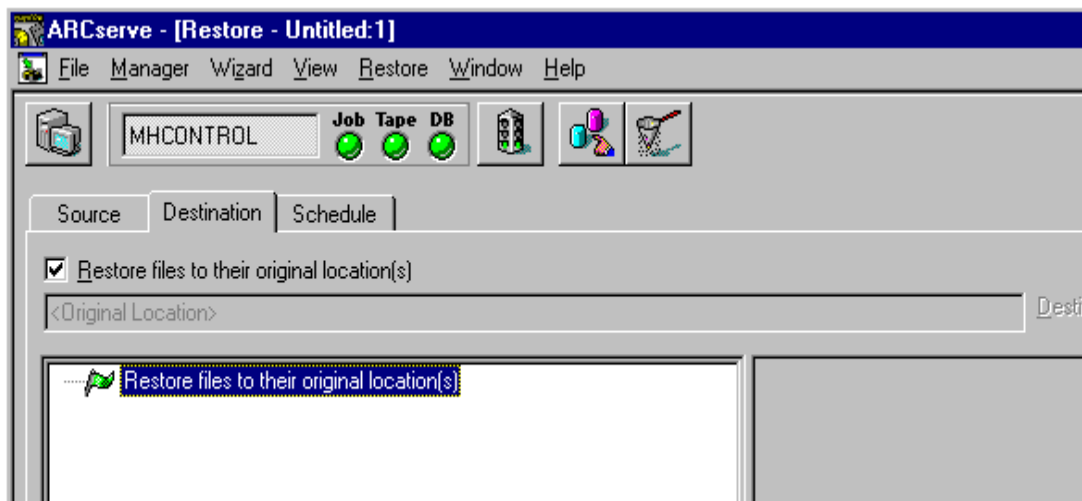
Para comenzar se selecciona el Tab de source u origen en el cual se seleccionara de donde se restaura la información, aquí hay un detalle importante pues existen diferentes maneras de realizar las restauraciones, la primera es Restore By Tree en la cual le presenta el árbol de información contenida en la base de datos y es

necesario indicarle por ultimo la fecha de los archivos a restaurar, esta opción es poco recomendada porque muestra a la vez varias versiones de un mismo archivo y se pueden dar confusiones y recuperar una fecha no adecuada. La siguiente opción es Restore By Session, esta es la opción recomendada para realizar restauraciones pues presenta la lista de respaldos realizados y al darle click sobre el respaldo presenta el árbol almacenado para ese determinado día. Y finalmente se encuentra la opción Restore by Backup Media, esta opción muestra las cintas que se encuentran en ese momento en el dispositivo de

respaldo y no presenta un árbol sino que realiza una búsqueda secuencial en toda la cinta hasta encontrar el archivo solicitado el cual debe ser especificado en la opción de filtros, caracterizada por un colador en la parte superior, en esta opción la restauración es lenta y se utiliza cuando no se cuneta con la base de datos de los respaldos o que esta se

encuentra dañada para ese determinado día.

Luego se selecciona el destino, o el lugar donde se almacenara la información que se restaure, esta información se asigna en la siguiente pantalla.



Si se encuentra marcada la opción Restaurar los archivos en su ubicación original, esta no permitirá realizar restauraciones al directorio temporal por lo que se desmarca esta opción y

aparece la estructura de árbol para indicar el lugar de la restauración.

Para finalizar se selecciona el tab de Schedule en el cual se indica la hora y el día en el cual se desean realizar las restauraciones.

Sobre el Desarrollo de Sistemas y Otros Servicios Informáticos.

De Aplicación General

- ♦ Todo desarrollo, invención o aplicación informática efectuado por funcionarios durante el desempeño de sus funciones, utilizando recursos institucionales, será propiedad intelectual de la Institución y deberá ser registrado de acuerdo a la reglamentación establecida para ello.
- ♦ Los desarrollos de aplicaciones se ejecutarán utilizando los estándares establecidos para la Institución siempre y cuando hayan sido aprobados formalmente por las autoridades correspondientes.
- ♦ Los servicios informáticos (soporte, desarrollo de sistemas informáticos, asesorías, consultorías, mantenimiento, capacitación, etc.) se brindarán de acuerdo al plan aprobado y en

función de los recursos disponibles y de las prioridades establecidas.

De Aplicación por Parte

del Administrador

(Unidad de informática)

Establecerá sobre la base de la realización de estudios técnicos sustentatorios, los estándares de las metodologías, técnicas y herramientas de desarrollo de sistemas, que serán implantados y utilizados en la institución para el desarrollo de sus aplicaciones.

- ♦ Todo desarrollo e implantación de sistemas informáticos deberá estar considerado en los planes y cronogramas de trabajo de la Unidad de Informática y se ejecutará de acuerdo a las prioridades que establezcan las autoridades de la institución.

- ◆ Definirá los recursos requeridos para los planes de automatización de la institución considerando los componentes tecnológicos y de recursos humanos y financieros necesarios e incorporará en el presupuesto los montos correspondientes y su ejecución será con la unidad beneficiaria.
- ◆ Brindará los servicios informáticos a la Institución y a las entidades que lo soliciten, procurando el máximo nivel de calidad, eficacia y eficiencia.
- ◆ Evaluará periódicamente el comportamiento de los sistemas y el nivel de conformidad de los usuarios.

De Aplicación por Parte

del Usuario.

- ◆ Participará activamente en todos y cada una de las etapas del proceso de desarrollo de sistemas informáticos.
- ◆ Se responsabilizará del contenido y actualización de los datos fuente que sean requeridos por los sistemas o servicios informáticos que le sean provistos.

Recomendaciones Generales par a mantenerse alejados de los virus

Un virus, es u pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este, ataca los archivos o sectores de "boot", y se replica a si mismo para continuar su

esparcimiento. Cuando un equipo de cómputo realiza operaciones de procesamiento más lento, los programas tardan más tiempo que lo usual en cargarse, los programas empiezan a acceder por momentos hacia la lectora

de discos o disco duro, hay una disminución no justificada del tamaño de la memoria RAM o Disco Duro o aparecen algunos programas residentes en memoria desconocidos, pueden ser síntomas de que nuestro equipo está infectado con algún virus.

Los virus depende su característica pueden realizar algunos problemas menores, daños triviales o menores, sin embargo existen algunos de ellos que realizan daños mayores o severos a nuestra información, por lo que es necesario que tengamos una serie de precauciones para asegurar la permanencia de nuestra información:

- ◆ Tener un disco de sistema
- ◆ Por lo menos un programa antivirus actualizado
- ◆ Una fuente de información sobre virus específicos

- ◆ Un programa de respaldo de áreas críticas
- ◆ Tener respaldos
- ◆ Discos nuevos
- ◆ Revisar a préstamo o prestados
- ◆ Revisar todos los programas que se obtengan por módem o redes
- ◆ Revisar periódicamente la computadora

Recomendaciones, para mantener alejado de su computadora cualquier riesgo de virus:

- ◆ Usar regularmente un programa antivirus (siempre se recomienda no confiar en uno solo, pero usar más de uno no significa que hay que tenerlos a todo instalaos), simplemente se ejecuta ese antivirus en su opción de escaneo,

sobre la carpeta que contenga los archivos a revisar. Y por supuesto, de nada vale usar algún antivirus sino se mantiene actualizado con los upgrades, Updates o add-ons correspondientes. Actualmente las actualizaciones son diarias, No existen los “virus demasiado nuevos y sin antidoto “, la reacción de las casas de antivirus es inmediata en todos los casos. Pero mejor pregúntese, si la suya también lo es a la hora de actualizarse.

- ◆ No abrir ningún mensaje ni archivo recibido a través del correo electrónico de fuentes desconocidas o muy poco conocidas. En el caso de personas conocidas, se deben igualmente tomar las precauciones correspondientes. Asegurese con esa personas del envío (“Melisssa” y otros pueden ser enviados por conocidos que ignoran estar mandando el virus

en sus mensajes), y nunca ejecutarlos, sino guardarlos en una carpeta temporal y pasarle a es a carpeta dos o tres antivirus actualizados antes de tomar la opción de ejecutarlos(.EXE) o abrirlos (.DOC, .RTF, etc.). Pero ante cualquier duda simplemente se debe optar por borrar el mensaje(y archivos adjuntos).

- ◆ Este informado de cómo operan los virus, y de las novedades sobre estos, alertas y anuncios críticos.
- ◆ No bajar nada de sitios Web de los que no tenga referencia de seriedad, o que no sean mediante conocidos. Y si se bajan archivos, proceder como los archivos adjuntos. Copiarlos a una carpeta y revisarlos con dos o tres antivirus actualizados antes de optar por ejecutarlos o abrirlos.

Políticas y Lineamientos Específicos

Sobre los Derechos de Autor, Adquisición de Software y Uso de Licencias

De Aplicación General

- ◆ En todos los bienes, informáticos de la entidad, queda prohibido el uso de software o programas que no cuenten con la licencia correspondiente.
- ◆ No debe instalarse o utilizarse software o programas de entretenimiento (juegos), con excepción de aquellas unidades que por la naturaleza de la función que desempeñan lo requiera .
- ◆ Solamente se permite la reproducción de software o programas como copias de respaldo.
- ◆ La inobservancia de estas políticas también puede dar lugar a la aplicación de las sanciones legales y administrativas establecidas en la Ley de Derecho de Autor.

De Aplicación por Parte del Administrador del área de Informática)

- ◆ Llevará el Inventario y control de las licencias de software y el medio magnético en el que se encuentran, adquiridas por la Institución así como se responsabilizará de su custodia, considerando licencias individuales, en uso, software preinstalado y corporativo. Asimismo, deberá informar al usuario de las licencias y programas instalados en el bien informática a su cargo.
- ◆ Establecerá los estándares para la adquisición, uso, normalización y licenciamiento de los paquetes informáticos a nivel institucional, considerando las

necesidades y compatibilidad tecnológica existente.

- ♦ La instalación del software aprobado, lo realizará solamente el personal autorizado.

De Aplicación por Parte del Usuario

- ♦ Controlará el uso de software o programas comerciales que no requieren de licencias de uso (freeware), o que son de prueba (shareware), estableciendo lo finalidad de su uso, período de utilización y autorizaciones del fabricante.
- ♦ Revisará y de ser necesario autorizará las solicitudes sobre el uso de software o programas diferentes a los establecidos como estándares.
- ♦ Quién disponga de bienes informáticos provistos por la Institución, es responsable de controlar que el software y programas instalados en su equipo, cuenten con la debida autorización.

Sobre los Contratos con Proveedores de Bienes o Servicios Informáticos.

De Aplicación por Parte del Administrador (Area de Informática)

seguimiento a lo establecido en los contratos correspondientes.

- ♦ Coordinará con la Dirección de Administración y Finanzas la revisión y ejecución de controles que permitan dañe un adecuado
- ♦ Vigilará que se cumplan los procedimientos establecidos pare los servicios de mantenimiento correctivo y preventivo que se

- ♦ pudiesen haber contratado dentro del calendario establecido y en *los casos* que sea necesario, autorizará cambios en las fechas.

3.7. ELEMENTOS ADMINISTRATIVOS

Para garantizar el más alto nivel de seguridad computacional o seguridad de la información, varios elementos deben estar continuamente activos y trabajar en conjunto, los cuales son:

- ♦ Análisis y cuantificación de los riesgos para la seguridad en el área de informática
- ♦ Organización y División de las responsabilidades
- ♦ Seguros

Análisis y cuantificación de los riesgos para la seguridad en el área de informática

La seguridad depende, fundamentalmente, de la integridad de los individuos que conforman una instancia. No existe una seguridad total y cada institución depende de su personal, para lograr los niveles de seguridad requeridos.

No todas las instalaciones de computación tienen las mismas exigencias de seguridad, pues algunas son mayores que otras.

Cuando se establece el grado de riesgo, es importante considerar

primero los tipos de riesgos a los que están expuestas las instalaciones de computación. Entre los riesgos principales encontramos los accidentes causados por el mal manejo y ataques deliberados en forma de robo, fraude, sabotaje o huelga.

La seguridad efectiva en la computación debe garantizar la prevención y detección de un accidente o ataque, la existencia de medidas claramente definidas para afrontar el desastre cuando ocurra y, si

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga

existe una interrupción del procesamiento. Algunas instituciones de computación y sus aplicaciones son de alto riesgo, ya que la interrupción del procesamiento durante un período prolongado causa un impacto material en la institución o en la comunidad. Otras no forman parte material o integral de una organización y se pueda respaldar fácilmente mediante procedimientos manuales. Por lo tanto, resulta evidente que no tiene sentido exagerar el nivel de los procedimientos de seguridad en las instituciones de bajo riesgo, por el contrario, donde existe un riesgo alto se debe dar protección equivalente. Sin embargo, la cuantificación del riesgo parece ser, a primera vista, un aspecto subjetivo, lo cual hace difícil su formulación en términos comerciales comunes y, en consecuencia, muchas instituciones evaden el problema o bien desisten en forma prematura a la cuantificación del riesgo.

procesamiento restablecerlo.

La cuantificación de los riesgos para la seguridad en las computadoras es quizá la parte mas importante del método que una institución adopte sobre la seguridad en computación.

La cuantificación de los riesgos de seguridad implica ciertas acciones:

- ◆ Clasificación general de las instalaciones en términos de riesgos alto, medio y bajo.
- ◆ Identificación de las aplicaciones que constituyen riesgos altos.
- ◆ Cuantificación del procesamiento en las aplicaciones de alto riesgo.
- ◆ Formulación de las medidas necesarias para lograr un nivel de seguridad adecuados, es decir, en equilibrio con los niveles de riesgo.
- ◆ Justificación de las medidas de seguridad en cuanto al costo que representan.

Clasificación general de las instalaciones

El primer paso consiste en establecer en términos generales si se trata de una instalación de riesgo alto, medio o bajo.

Instalaciones de alto riesgo:

Las instalaciones de alto riesgo tienen las siguientes características:

- ◆ Datos o programas que contienen información confidencial de interés nacional o que poseen valor competitivo alto en el mercado.
- ◆ Pérdida financiera potencial considerable para la comunidad a causa de un desastre o de un gran impacto sobre los miembros del público.
- ◆ Pérdida potencial considerable para la institución y, en consecuencia, una amenaza potencial alta para su subsistencia

Todas las instalaciones de riesgo alto presentan una o mas de esas características. Por ello, resultará generalmente fácil identificarlas.

En la práctica no es tan importante hacerlo, pues lo que en realidad interesa es el impacto sobre el buen estado o la subsistencia de la empresa en caso una interrupción prolongada del procesamiento.

Instalación de riesgo medio:

Son aquellas con aplicaciones cuya interrupción prolongada causa grandes inconvenientes y posiblemente el incremento de los costos; sin embargo se obtiene poca pérdida material.

Instalaciones de bajo riesgo:

Son aquellas con aplicaciones cuyo procesamiento retardado tiene poco impacto material en la institución en términos de costos o de reposición del servicio interrumpido.

Elaboración de una lista de aplicaciones por orden de riesgo

Todas las aplicaciones se deben arreglar en forma tabular y en orden descendente de acuerdo con la importancia del riesgo.

Es recomendable anotar los siguientes datos en cada aplicación:

- ♦ Valor competitivo en el mercado debido al carácter único de los aspectos computacionales o su escala y complejidad.
- c) Información de los archivos; también de esta manera
 - ♦ Aspectos secretos o de interés nacional
 - ♦ Confidencialidad interna o de valor de mercado
 - ♦ Nivel de riesgo (alto, medio o bajo) y una evaluación general sobre las consecuencias en caso de abuso o desastre.

Cuantificación Del Riesgo

El método más práctico para resolver el problema es comenzar por pasar revista a todos los directivos afectados por una suspensión en el procesamiento y pedirles que cuantifiquen el impacto causado por la situación. Las respuestas iniciales

- a) Título o descripción de la aplicación
- b) Programas claves y naturaleza del riesgo, es decir,

- ♦ Aspectos secretos o de interés nacional.

tal vez varíen en gran medida. Algunos mencionarán pérdidas mínimas debido a procedimientos de apoyo manuales, mientras otros indicarán pérdidas altas. Pero cuando los directivos comiencen a emitir juicios como “creo que es un gran riesgo”, se les debe pedir que indiquen con más claridad lo que quieren decir con esa frase, esto lleva a la pregunta final que es la cuantificación del impacto. En este momento ya se contará con una serie de expresiones cuantificadas sobre los niveles de riesgo de seguridad.

Obtención Del Consenso Sobre Los Niveles De Riesgo

Este paso permite lograr el compromiso de la dirección con el nivel de riesgo definido.

Se debe programar una reunión de los directivos correspondientes, en la cual se informará sobre las expresiones de riesgos debidamente tabuladas. El

propósito de la reunión será lograr el consenso sobre los niveles de riesgo, que por lo general se presentan como rangos mas que como cifras absolutas. El riesgo permite justificar de manera objetiva el costo de las medidas de seguridad.

En la etapa de revisión preliminar de la seguridad en computación, no es posible obtener todas las recomendaciones detalladas. Esto se logrará una vez que se lleve acabo la revisión a fondo de la seguridad en computación. Sin embargo es posible definir la estrategia global que se debe seguir para afrentar los niveles de riesgo definidos. Esta estrategia incluye:

- ◆ Aplicaciones, programas y archivos específicos.
- ◆ Planes de detección y métodos para prevenir abusos o desastres.
- ◆ Prioridades que son acciones que se requieren a corto plazo y los elementos que se deben considerar de manera detallada a mediano y largo plazo.

Estos pasos conducen hacia la recolección y la presentación de todos los informes necesarios para una decisión bien fundada sobre los costos y beneficios de la estrategia de seguridad en computación.

Toda la información que se obtenga y las decisiones que se tomen se deben documentar de manera progresiva, lo que consolida el informe final ante la dirección.

Es conveniente convocar a una reunión de los directivos correspondientes para evaluar los hallazgos como las recomendaciones, a fin de que se obtenga una decisión y que se apruebe un plan de acción destinado a la investigación y a la aplicación más detallada. De esta forma esta práctica constituye un marco de trabajo para el método que se acepte a los niveles de costo en los cuales se incurra sin solicitudes redundantes a la dirección.

Hay que recordar la importancia de la dirección, ya que esta es la que toma la decisiones sobre el método que adopte y los niveles de gastos.

Para definir la política sobre seguridad, el primer problema consiste en determinar quien tiene las responsabilidades generales de la seguridad en computación.

- ◆ Asunto de riesgo técnico en las computadoras

Los asuntos técnicos son, de manera evidente, responsabilidad de un área de soporte. Este es un modo práctico de deslindar responsabilidades, pero se requiere cierta coordinación para garantizar un cambio productivo entre las funciones administrativas y técnicas.

El comité de seguridad para las computadoras se encarga entre otras cosas, de los siguientes aspectos:

- ◆ Definir la Asignación de responsabilidades

- ◆ Participar en la determinación de una política de seguridad.
- ◆ Hacer el seguimiento de los logros e incluir la asignación detallada de los medios correctores.
- ◆ Revisar y comprobar en forma periódica la suficiencia de la seguridad en computación.

Resulta útil contar con dicho comité desde el principio, cuando se revisa y define la política de seguridad en computación.

Organización y División de las Responsabilidades

La manera de organizar las actividades del área de informática incluye aspectos que afectan la seguridad en computación; estos son:

División de Responsabilidades:

Dentro de cualquier empresa, división de responsabilidades permite lograr la

revisión y los balances sobre calidad del trabajo.

Dentro del contexto del área de informática hay varios recursos que mejoran la calidad del control de la dirección y, con ello, la seguridad;

estos recursos –con sus restricciones correspondientes- son los siguientes:

Restricciones:

- ◆ El personal que prepara los datos no debe tener acceso a las Actividades de operación.
- ◆ Los analistas de sistemas y los programadores no deben tener acceso irrestricto a las funciones de protección de información o departamentos donde se localicen los archivos maestros.
- ◆ Los operadores no deben tener los controles únicos del procesamiento del trabajo y se les debe prohibir que inicien las correcciones de los errores.

El grado de división entre los diferentes funciones depende del nivel de seguridad que la instalación requiera. Los elementos claves de este criterio constituye funciones claramente definidas y autónomas.

En el contexto de las actividades de computación estas funciones claves son:

- ◆ Desarrollo de los sistemas
- ◆ Programación

- ◆ Mantenimiento de programas
- ◆ Preparación de los datos
- ◆ operaciones centrales y remotas
- ◆ Control
- ◆ Preservación de los archivos

Las divisiones del trabajo también se deben aplicar a los procedimientos del usuario.

Esto se realiza tradicionalmente en el nivel de la aplicación. Con frecuencia, dentro del departamento de computación o área de informática, se produce una fuerte resistencia contra el establecimiento –dentro de una aplicación- una división efectiva de las responsabilidades sobre la base de los procedimientos, pues se considera que inhiben y obstaculizan la eficiencia general.

Las medidas de seguridad reducirán la flexibilidad en el trabajo pero, mediante el diseño meticuloso, no se afectará la eficiencia. Muchas veces no se consulta con el personal afectado cuando se diseñan las divisiones del trabajo. En consecuencia, las personas no se comprometen con las medidas y se pueden propiciar que se sientan

muy desmotivadas. Esta situación genera un aumento de riesgo en la seguridad, lo que se puede evitar fácilmente mediante la reflexión previa.

Los dos elementos claves que sirven de base para las divisiones subsecuentes de responsabilidad son las funciones de **control** y de **archivo**. Resulta conveniente que estas funciones sean autónomas y se adscriban a la autoridad más alta que se pueda –de preferencia el director de la empresa-

Sistema De Control Interno

La división de responsabilidades y los sistemas de verificación interna se combinan para formar el sistema de control interno de una institución.

Los sistemas de verificación permiten las comprobaciones de evidencia que prueban que se realizan la recolección de datos de forma completa y precisa y que se trabaja de acuerdo con las divisiones de responsabilidades y de jerarquía.

La verificación documentada de evidencias requiere que:

1. Las modificaciones de los programa se autoricen y prueben de forma adecuada.
2. Se documenten de manera adecuada y progresiva los sistemas nuevos.
3. Los departamento de origen documenten y verifiquen los datos de los archivos, tanto registros nuevos como corregidos, contra impresos que sean editados en el área de informática.
4. Los datos de entrada se agrupen y revisen de acuerdo con datos aceptados para procesamiento .
5. Se documenten los errores y se autoricen y comparen las correcciones de los mismos.

Asignación de responsabilidades en cuanto a la seguridad

En la descripción de las labores es necesario que participen todos los departamentos. Pues resulta muy importante especificar sus responsabilidades. La seguridad es un área clave de resultado o de acción.

Un factor crítico para el éxito de la seguridad es la gente. La organización y división de responsabilidades también debe adoptarse en esta área.

La organización que se establezca en esta área se determinará por el tipo de persona que se encargará de las funciones de seguridad. Las funciones más importantes son las siguientes:

Supervisor de seguridad. Se encarga de evaluar los riesgos y preparar los planes de seguridad, así como supervisar los procesos de selección de los productos y los procedimientos de evaluación de las bitácoras de seguridad. También debe asistir en la definición de límites, para determinar una violación de seguridad, planes de seguridad para el sistema de red y establecer el programa de capacitación para su personal.

Oficial de Seguridad. Evalúa los riesgos de seguridad, dicta las acciones contra los intrusos, supervisa la seguridad en tiempo real, así como el sistema de administración de la red. Además, ayuda en la selección de instrumentos, en la evaluación de las bitácoras de vigilancia, en la elaboración de los planes de seguridad y en la administración de los pasaportes.

Auditor de Seguridad. Ayuda en la estimación de riesgos de seguridad, en el establecimiento de límites para determinar una violación a la seguridad, en la definición de la relación correcta de precauciones físicas y lógicas, además de evaluar las bitácoras de vigilancia, categorizar los riesgos de seguridad, auxiliar en la selección de instrumentos y escribir los reportes de avance de los planes de seguridad.

Analista de seguridad. Se encarga de definir las funciones de monitores y vigilancia, evaluar el impacto de las

técnicas de seguridad en el desempeño de la red y seleccionar los servicios del área de seguridad. También debe recomendar instrumentos durante el proceso de selección de los mismos, programar los instrumentos y establecer procedimientos para asegurar el sistema administración de la red.

Coordinador de seguridad de la red. Controla la configuración de la seguridad de la red, las autorizaciones de acceso a las aplicaciones, servicios gateways, routers, bridges y firewalls de la red; realiza el seguimiento del directorio de la red, administra los pasaportes locales y asiste en la toma de acciones contra los intrusos.

Las funciones del área de seguridad se encuentran distribuidas de la siguiente manera:

FUNCIONES			ORGANIZACION		
	Supervisor Seguridad	Oficial Seguridad	Auditor Seguridad	Analista Seguridad	Coordinador Seguridad Red
Analista de riesgos.	X	X	X	X	X
Evaluación de los Servicios de Seguridad	X	X			
Evaluación de las soluciones del dominio de seguridad	X	X			
Alarmas, acciones y reportes			X	X	X
Protección de los Sistemas de Administración de la red.	X			X	

Los Seguros

Los seguros existen desde hace mucho tiempo, provistos de criterios y prácticas bien definidas. Sin embargo,

cualquier institución que busque asesoramiento y orientación sobre cobertura de riesgos de computación,

corre el riesgo de enfrentar dificultades considerables. Existen dos problemas principales:

- ♦ La existencia de un gran vacío en la comunicación: en general, los aseguradores saben mucho sobre riesgos comerciales pero muy poco acerca de computadoras, mientras que el personal de computo conoce poco acerca de seguros y mucho sobre computadoras.

- ♦ No hay un entendimiento cabal respecto a los riesgos y sus consecuencias, debido a que la profesión computacional es reciente y a que los antecedentes en relación con las reclamaciones sobre seguros son pocos.

El resultado de lo anterior es que muy pocos usuarios de computadoras gozan de una cobertura adecuada para todos los riesgos. La tendencia es cubrir una o dos áreas de riesgo evidente, como la reposición del equipo o contra los incendios. Otro costo como la recaptura o el límite de responsabilidad ante esta pérdida, casi siempre se pasan por alto.

Existen tres aspectos en particular:

- ♦ Las áreas de riesgo asegurable.
- ♦ Los servicios de seguros especializados
- ♦ El cambio del tipo de riesgo.

A. Área de riesgo asegurable.

- ♦ Ambiente
- ♦ Equipo
- ♦ Programas y datos
- ♦ Interrupción comercial y su recuperación
- ♦ Personal
- ♦ Responsabilidades a terceras personas

Estas áreas de riesgo fueron publicadas por el *National Computing Centre*(NCC).

B. Servicios de seguro especializado

En la actualidad, ciertas instituciones ofrecen servicios especializados, para usuarios de computadoras.

Estos servicios incluyen la adopción del personal altamente capacitado en el manejo de las computadoras y, en consecuencia de los riesgos inherentes.

Además varias compañías internacionales de seguros cuentan

con pólizas especializadas para usuarios de computadoras.

Normalmente una póliza de seguros de equipo de computo cubre:

1. Daños materiales al equipo.

Ampara cualquier pérdida o daño físico, súbito e imprevisto, que requiera de reparación o reemplazo.

Excluye:

- ◆ Pérdidas o daños causadas por terremoto, temblor, maremoto, erupción volcánica, ciclón, tifón o huracán.
- ◆ Perdidas o daños causadas por hurto o robo sin violencia.
- ◆ Perdida o daños causados por fallo e interrupción en el suministro de corriente eléctrica, de gas o de agua

Pérdida o daños que sean consecuencia del uso continuo o deterioro gradual debido a condiciones atmosféricas.

Sin embargo este tipo de exclusiones se pueden prever mediante la contratación expresa de otra póliza

1. Portadores externos de datos.

Cubre la indemnización sobre daños causados a dispositivos de almacenamiento de datos así como la operación n contenida en estos.

Excluye, cualquier gasto resultante de la incorrecta programación, perforación, clasificación, operación, anulación accidental de informaciones, perdida de información causadas por campos magnéticos y virus informáticos.

2. Incremento en el costo de operación.

Esta cobertura se aplica si un daño material indemnizable diera lugar a una interrupción parcial o total de la operación, lo que causará un desembolso adicional al usar un centro de computo ajeno y/o suplente.

Los seguros a los equipos de computo se aplican a los bienes que se estén operando o que se encuentren en reposo, desmontados para propósito de limpieza o reparación o durante su

traslado dentro del periodo establecido en la póliza.

Generalmente excluyen los daños causados por:

- ◆ Guerra, invasión, actividades de enemigos extranjeros, hostilidades (con o sin declaración de guerra, guerra civil, rebelión, revolución, insurrección, motín, tumulto, huelga, paro decretado por el patrón, conmoción civil, poder militar o usurpado, conspiración, etc).
- ◆ Reacciones nucleares, radiación nuclear o contaminación radiactiva.
- ◆ Acto internacional o negligencia manifiesta del seguro o de sus representantes.

Sin embargo existen algunas pólizas adicionales que pueden contratarse y que cubren lo siguiente:

- ◆ Huelga, alborotos populares y conmoción civil
- ◆ Gastos extraordinarios y fletes expresos
- ◆ Gastos por flete aéreo
- ◆ Daños por fallo de la instalación de climatización.
- ◆ Robo sin violencia (hurto)
- ◆ Equipos móviles y portátiles fuera de los predios señalados.
- ◆ Cláusula de huracán, ciclón, tifón.
- ◆ Daños mecánicos y eléctricos internos
- ◆ Equipo de climatización

Se deben revisar y evaluar las diferentes alternativas de seguro que ofrecen las compañías dedicadas a este rubro.

C. Seguimiento de los cambios en los riesgos

Los riesgos asegurables cambian en forma progresiva dentro de la institución como un todo y en el interior de sus actividades de computo.

Es importante garantizar que los nuevos riesgos se encuentran cubiertos y que las pólizas estén actualizadas.

Un método valioso es la formación de un comité de seguridad de cómputo.

Sus objetivos son:

- ◆ Identificar y cuantificar los riesgos directos y consecuentes de la instalación de computo en la institución.
- ◆ Garantizar que la cobertura se revise para tomar nota de los incrementos de los costos en los precios de producción.
- ◆ Garantizar la existencia de los planes de contingencia adecuada, en especial cuando no se puede obtener la cobertura del seguro
- ◆ Asegurar que la pérdida consecuente se excluya de las responsabilidades de la institución hacia terceras personas.

- ◆ Obtener asesoría y orientación especializada cuando se requiera.

- ◆ Obtener asesoría y orientación especializadas cuando se requiera

Además, el comité debe contar con representantes de las siguientes dependencias:

- ◆ La dirección de procedimientos de datos
- ◆ La compañía de seguros
- ◆ Los gestores de seguros
- ◆ El departamento de control secretarial o financiero
- ◆ La auditoria interna o la externa.

Por medio de las reuniones periódicas, cuatrimestrales o anuales según el tamaño de la institución, es posible asegurar que la cobertura de riesgos esté claramente identificada y actualizada.

3.8. ACCIONES PARA LA AUDITORIA

La Informática actualmente, está incluida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática.

La palabra auditoría viene del latín *auditorius* y de esta proviene auditor, que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

La auditoria aplicada a la seguridad informática ayuda entre otros a determinar la existencia y origen de:

- ♦ Daños
- ♦ Salvaguarda activos Destrucción
- ♦ Uso no autorizado
- ♦ Robo
- ♦ Integridad de Información
- ♦ Consumo recursos
- ♦ Eficiencia en el uso de los recursos informáticos

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el informe final reciben el nombre de recomendaciones.

Las funciones de análisis y revisión que el auditor informático realiza, puede chocar con la psicología del auditado, ya que es un informático y tiene la necesidad de realizar sus tareas con racionalidad y eficiencia. La reticencia del auditado es comprensible y, en ocasiones, fundada. El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los Sistemas, unidos a los plazos demasiado breves de los que suelen disponer para realizar su tarea. Además del chequeo de los Sistemas, el auditor somete al auditado a una serie de cuestionarios. Dichos cuestionarios, llamados Check List, son guardados celosamente por las empresas auditoras, ya que son activos importantes de su actividad. Las Check List tienen que ser comprendidas por el auditor al pie de la letra, ya que si son mal aplicadas y mal recitadas se pueden llegar a obtener resultados distintos a los esperados por la empresa auditora. La Check List puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren. El cuestionario debe estar subordinado a la regla, a la norma, al método. Sólo una

metodología precisa puede desentrañar las causas por las cuales se realizan actividades teóricamente inadecuadas o se omiten otras correctas.

El auditor sólo puede emitir un juicio global o parcial basado en hechos y situaciones incontrovertibles, careciendo de poder para modificar la situación analizada por él mismo. En cuanto a empresas se refiere, solamente las más grandes pueden poseer una Auditoría propia y permanente, mientras que el resto acuden a las auditorías externas. Puede ser que algún profesional informático sea trasladado desde su puesto de trabajo a la Auditoría Interna de la empresa cuando ésta existe.

Objetivos Generales de realizar procedimientos de Auditoría en la seguridad:

- ♦ Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados diseñados e implantados por el procesamiento automatizado de datos (PAD)
- ♦ Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

recomendación de seguridades y controles.

Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático

- ♦ Minimizar existencias de riesgos en el uso de Tecnología de información, decisiones de inversión y gastos innecesarios
- ♦ Capacitación y educación sobre controles en los Sistemas de Información

Razones para efectuar una auditoria de seguridad

Aumento considerable e injustificado del presupuesto del PAD (Procesamiento automatizado de datos)

- ♦ Desconocimiento en el nivel directivo de la situación informática de la empresa
- ♦ Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- ♦ Descubrimiento de fraudes efectuados con la computadora.
- ♦ Falta de una planificación informática

♦ Seguridad de personal, datos, hardware, software e instalaciones

♦ Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del Recurso Humano

♦ Falta de documentación o documentación incompleta de sistemas que revela la dificultad de efectuar el mantenimiento de los sistemas en producción

♦ No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables.

Actividades Propiamente Dichas De La Auditoria

Auditoria por temas generales o por áreas específicas:

La auditoria Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

cuando la auditoria se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

obtiene más rápidamente y con menor calidad.

Metodología De Una Auditoria De Sistemas

La metodología de Auditoría de Sistema depende de lo que se pretenda revisar o analizar, pero como estándar existen cuatro fases básicas de un proceso de revisión:

1. Estudio preliminar
2. Revisión y evaluación de controles y seguridades
3. Examen detallado de áreas críticas
4. Comunicación de resultados

Estudio preliminar.- Incluye definir el grupo de trabajo, el programa de auditoria, efectuar visitas a la unidad informática para conocer detalles de la misma, elaborar un cuestionario para la obtención de información para evaluar preliminarmente el control interno, solicitud de plan de actividades, Manuales de políticas, reglamentos, Entrevistas con los principales funcionarios del PAD.

Revisión y evaluación de controles y seguridades.- Consiste de la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de aplicaciones de las áreas críticas, revisión de procesos históricos (backups), revisión de documentación y archivos, entre otras actividades.

Examen detallado de áreas críticas. Con las fases anteriores el auditor descubre las áreas críticas y sobre ellas hace un estudio y análisis profundo en los que definirá concretamente su grupo de trabajo y la distribución de carga del mismo, establecerá los motivos, objetivos, alcance recursos que usará, definirá la metodología de trabajo, la duración de la auditoría, presentará el plan de trabajo y analizará detalladamente cada problema encontrado con todo lo anteriormente analizado en este manual.

Comunicación de resultados.- Se elaborará el borrador del informe a ser discutido con los ejecutivos de la empresa hasta llegar al informe definitivo, el cual presentará esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados los efectos y las recomendaciones de la Auditoria.

El informe debe contener lo siguiente:

- ◆ Motivos de la Auditoria
- ◆ Objetivos
- ◆ Alcance
- ◆ Estructura Orgánico-Funcional del área Informática
- ◆ Configuración del Hardware y Software instalado
- ◆ Control Interno
- ◆ Resultados de la Auditoría

Para Realizar Una Auditoria En Seguridad El Auditor Debe Conocer :

Organización, para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto en auditor deberá fijarse en:

1) Organigrama:

El organigrama expresa la estructura oficial de la organización a auditar. Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

2) Departamentos:

Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

3) Relaciones Jerárquicas y funcionales entre órganos de la Organización:

El equipo auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes. Las de Jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.

4) Flujos de Información:

Además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales. Los flujos de información entre los grupos de una organización

son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama. En ocasiones, las organizaciones crean espontáneamente canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa.

Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización.

5) Número de Puestos de trabajo

El equipo auditor comprobará que los nombres de los puestos de trabajo, de la organización corresponden a las funciones reales distintas. Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes. Esta situación pone de manifiesto deficiencias estructurales; los auditores darán a conocer tal circunstancia y expresarán el número de puestos de trabajo verdaderamente diferentes.

6) Número de personas por puesto de trabajo

Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

7) Entorno Operacional

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse. Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

a) Situación geográfica de los sistemas: se determinará la ubicación geográfica de los distintos centros de proceso de datos en la empresa. A continuación, se verificará la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.

b) Arquitectura y configuración de Hardware y Software:

Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad lógica de las compañías. Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

c) **Inventario de Hardware y Software:** El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remotas, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

d) Comunicación y Redes de Comunicación:

En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones. Igualmente, poseerán información de las redes locales de la empresa.

e) Aplicaciones, bases de datos y ficheros

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

- ◆ Volumen, antigüedad y complejidad de las Aplicaciones
- ◆ Metodología del Diseño

Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizado varias a lo largo del tiempo se pondrá de manifiesto.

- ◆ Documentación

La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes. La documentación de programas disminuye gravemente el mantenimiento de los mismos.

- Cantidad y complejidad de bases de datos y ficheros.

El auditor recabará información de tamaño y características de las bases de datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.

Revisión De Controles De La Gestión Informática

Uno de los principales objetivos de la auditoría es la verificación de la observancia de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la institución. Para ello, habrán de revisarse sucesivamente y en este orden:

1. Las Normas Generales de la Instalación Informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta Normativa General Informática no está en contradicción con alguna Norma General no informática de la institución.

2. Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de Explotación. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.

3. Los Procedimientos Específicos Informáticos. Igualmente, se revisará su existencia en las áreas fundamentales. Así, explotación no debería explotar una aplicación sin haber exigido a desarrollo la pertinente documentación. Del mismo modo, deberá

comprobarse que los procedimientos específicos no se opongan a los procedimientos generales.

En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la normativa y los procedimientos generales de la propia institución, a los que la Informática debe estar sometida.

Participación De Auditoria En El Desarrollo De Proyectos O Aplicaciones:

La función de desarrollo es una evolución del llamado análisis y programación de sistemas y aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la institución. Muy escuetamente, una aplicación recorre las siguientes fases:

Prerequisitos del usuario (único o plural) y del entorno

- ◆ Análisis funcional
- ◆ Diseño
- ◆ Análisis orgánico (Preprogramación y Programación)
- ◆ Pruebas Entrega a Explotación y alta para el proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros. Una auditoría de Aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

1. Revisión de las metodologías utilizadas: Se analizarán éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
2. Control interno de las aplicaciones: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo:

- ◆ Estudio de Vialidad de la Aplicación. (importante para Aplicaciones largas, complejas y caras)
- ◆ Definición Lógica de la Aplicación. (se analizará que se han observado los postulados lógicos de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto)
- ◆ Desarrollo Técnico de la Aplicación. (Se verificará que éste es ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles)
- ◆ Diseño de Programas. (deberán poseer la máxima sencillez, modularidad y economía de recursos)
- ◆ Métodos de pruebas. (Se realizarán de acuerdo a las normas de la instalación. Se utilizarán juegos de ensayo de datos, sin que sea permisible el uso de datos reales)
- ◆ Documentación. (cumplirá la normativa establecida en la instalación, tanto la de desarrollo como la de entrega de aplicaciones a explotación)
- ◆ Equipo de Programación. (Deben fijarse las tareas de análisis puro, de programación y las intermedias. En aplicaciones complejas se producirían variaciones en la composición del grupo, pero estos deberán estar previstos)

3. Satisfacción de usuarios: Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

4. Control de Procesos y Ejecuciones de Programas Críticos: El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de desarrollo de

aplicaciones. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación.

Si los programas fuente y los programa módulo no coincidieran puede provocar, desde errores de bulto que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las librerías de programas; aquellos programas fuente que hayan sido dados por bueno por desarrollo, son entregados a explotación con el fin de que éste:

- ◆ Copie el programa fuente en la librería de fuentes de explotación, a la que nadie más tiene acceso
- ◆ Compile y monte ese programa, depositándolo en la librería de módulos de explotación, a la que nadie más tiene acceso.
- ◆ Copie los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique.
- ◆ Cualquier cambio exigirá pasar nuevamente por el primer punto .

Auditoría Comunicaciones Y Redes

Para el informático y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios).

El auditor de Comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá

proveerse de la topología de la red de comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los puestos de trabajo correspondientes (pantallas, servidores de redes locales, computadoras con tarjetas de comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y de ser posible, dependientes de una sola organización.

La decisión de abordar una auditoria informática de seguridad global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada <<Amenaza-Impacto>>, en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

Ejemplo:

1- Improbable 2- Probable 3- Certeza

Impacto	Amenaza
Error	1
Incendio	1
Sabotaje	2
Destrucción de Hardware	1
Borrado de Información	3

El cuadro muestra que si por error codificamos un parámetro que ordene el borrado de un fichero, éste se borrará con certeza.

Herramientas Y Técnicas Para La Auditoria Informática:

Cuestionarios:

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias. Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma. Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otros medios la información que aquellos preimpresos hubieran proporcionado.

Entrevistas:

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado, siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

Checklist:

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados.

Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente. El conjunto de estas preguntas recibe el nombre de Checklist. Salvo

excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer. Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética. El auditor deberá aplicar el Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. Checklist de rango; contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

Ejemplo de Checklist de rango:

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al centro de cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tiene los siguientes significados:

1 : Muy deficiente.

2 : Deficiente.

3 : Mejorable.

4 : Aceptable.

5 : Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. La cumplimentación del Checklist no debe realizarse en presencia del auditado. Los Checklists de rango son adecuados si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en los checklist binarios. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Los Checklists Binarios siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

Trazas y/o Huellas:

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo. Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por técnica de sistemas a cada uno de los parámetros variables de las librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

No obstante la utilidad de las trazas, ha de repetirse lo expuesto en la descripción de la auditoria informática de sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio sistema: Así, los ficheros de <Accounting> o de <contabilidad>, en donde se encuentra la producción completa de aquél, y los <Log*> de dicho sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general. Del mismo modo, el sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos, etc.

Técnicas de Trabajo:

- ◆ Análisis de la información recabada del auditado.
- ◆ Análisis de la información propia.
- ◆ Cruzamiento de las informaciones anteriores.
- ◆ Entrevistas.
- ◆ Simulación.
- ◆ Muestreos.

Otras Herramientas:

- ◆ Estándares.
- ◆ Monitores.
- ◆ Simuladores (Generadores de datos).
- ◆ Paquetes de auditoria (Generadores de Programas).
- ◆ Matrices de riesgo.

3.9. PLAN DE CONTINGENCIA

La planeación formal implica diseñar un futuro deseado e identificar las formas para lograrlo. Su esencia consiste en la identificación sistemática de las oportunidades y peligros que puedan surgir en el futuro, los cuales – combinados con otros datos importantes- proporcionan la base para lograr que una empresa tome mejores decisiones en el presente para explorar

esas mismas oportunidades y evitar los peligros.

Un plan de contingencia es una “presentación para tomar acciones específicas cuando surja un evento o condición que no esté considerado en el proceso de planeación formal”. Es decir, se trata de un conjunto de procedimientos de recuperación para casos de desastre; es un plan formal que describe pasos apropiados que se deben

seguir en caso de un desastre o emergencia.

Consiste en un amplio estado de acciones consistentes para ser tomadas;

- ♦ **Antes**, como un plan de respaldo
- ♦ **Durante**, como un plan de emergencia y

Después, como un plan de recuperación tras un desastre.

Un adecuado plan de contingencia ayuda a la instalación de cómputo y a la organización en general a minimizar sus pérdidas en caso de desastre, y reanudar las operaciones normales de una manera rápida, eficiente y oportuna.

“El término desastre en este contexto significa la interrupción en la capacidad de acceso a la información y el procesamiento de la misma a través de las computadoras, necesarias para la operación normal del negocio”.

El Plan de contingencia constituye en cierta forma un control netamente preventivo, ya que se configura como un instrumento que permite prevenir la eventualidad de un desastre, así como mantener el nivel de operación del

ambiente informático, esto forma un control correctivo en la cual se materializa un riesgo, ya que se pretende reducir el impacto de éste.

Se recomienda establecer un modelo a partir de aquellas organizaciones que se han preocupado por su desarrollo y crecimiento, han establecido dentro de la estructura orgánica de la empresa una función definida para la administración de riesgos y que han obtenido estupendos resultados, como una disminución considerable del impacto físico y económico de los riesgos dentro de la misma organización.

Este tipo de plan implica invertir tiempo, dinero y esfuerzo, y su verdadero valor sólo se podrá medir en el caso en que se presente alguna contingencia.

El contenido del plan de contingencia se recomienda manejarlo conforme a los procedimientos siguientes:

- ♦ Objetivo
- ♦ Características
- ♦ Consideraciones
- ♦ Aspectos base

◆ Elementos del plan de contingencia

OBJETIVO

El propósito principal de un plan de contingencia es “mantener a la compañía y sus actividades operando aún en una situación de desastre”, es decir, habilitar a la organización para responder y sobrevivir a problemas críticos o catastróficos, de forma que permita una pronta recuperación de la operación normal del centro de cómputo.

Este plan dependerá de la naturaleza de la organización, ya que inevitablemente incurrirá en costos altos. Sin embargo, es importante tener en mente que su importancia no depende de la probabilidad de un desastre, sino del efecto que éste pueda tener.

Se debe considerar que la pérdida parcial o total de las facilidades del procesamiento de datos puede causar entre otras cosas:

- ◆ Pérdidas financieras directas
- ◆ Pérdidas de la producción
- ◆ Pérdidas financieras indirectas
- ◆ Pérdidas de clientes
- ◆ Costos extras para apoyo
Costos de compensación
- ◆ Pérdidas de control
- ◆ Información errónea o incompleta
- ◆ Bases pobres para la toma de decisiones.

CARACTERÍSTICAS

En una organización, el plan de contingencia ha de contemplar dos aspectos: operacional y administrativo.

En el nivel operacional, cada usuario debe saber qué hacer cuando aparezca el problema. Asimismo debe saber la

respuesta a la pregunta ¿A quién hay que llamar?

Es muy importante que el plan de contingencia determine quién debe tomar las decisiones durante la recuperación del desastre y establezca la disponibilidad y entrenamiento del personal debidamente experimentado.

En el nivel administrativo, el plan contempla aspectos como:

- ◆ Definición de riesgos y porcentajes de factibilidad a que está expuesta la organización.
- ◆ Identificación de las aplicaciones críticas para la empresa.

Procedimiento de recuperación para la reproducción de información.

- ◆ Especificación de las alternativas de respaldo.
- ◆ Localización de los medios de respaldo
- ◆ Responsables de los medios de respaldo
- ◆ Archivos o bases de datos prioritarios que deben ser reconstruidos primero

- ◆ La configuración del equipo de cómputo similar y su localización (centro de cómputo alternativo o espejo).
- ◆ Localización del software de reemplazo
- ◆ Localización de otro equipo de apoyo, tal como generadores y aire acondicionado
- ◆ La ayuda que se puede esperar del proveedor del equipo
- ◆ La acción a ser tomada en cada año parcial inesperado.
- ◆ Procedimiento para la imposición de controles extraordinarios durante el desastre y hasta que regresen los sistemas a la normalidad.

En este punto también debe considerarse que para el desarrollo y mantenimiento de una buena recuperación se debe tomar en cuenta:

- A. Respaldo de configuración del equipo de cómputo y de la programación del software.
- B. Documentación y almacenamiento seguro de los procedimientos de recuperación. Un aspecto importante

de la documentación es el entrenamiento de los individuos que se encargan de las operaciones de recuperación.

C. Respaldo y almacenamiento seguro de los programas de forma que se pueda disponer de ellos cuando se requieran.

Respaldo y almacenamiento seguro de los archivos de datos que sean esenciales para la operación continua de la organización.

Al identificar un plan de contingencia como un proceso dentro de la función administrativa de riesgos, es necesario hacer consciente a todos el personal de que está involucrado en el mismo; indicar que su implantación es al mismo tiempo un dispositivo de control, el cual entra en acción en el momento en que otros controles –ya sean preventivos o detectores- fallan.

De esta manera se debe enfatizar el seguimiento de los siguientes puntos clave:

- ◆ Dar a los controles detectores las bases necesarias para el

entendimiento de los esfuerzos totales que se requieren para desarrollar y mantener un efectivo plan de recuperación.

- ◆ Obtener el consentimiento de los directivos apropiados para apoyar y participar en los esfuerzos.
- ◆ Definir los requerimientos de recuperación desde la perspectiva que establece la misión de la empresa.
- ◆ Converger apropiadamente en la prevención de desastres y reducción del impacto.
- ◆ Integrar el plan de contingencia dentro de los planes generales de la organización y los procesos de desarrollo de los sistemas de forma que el plan se mantenga factible todo el tiempo.

El plan de recuperación debe cumplir con las siguientes características:

1. Actual
2. Entendible
3. Factible
4. Probado
5. Documentado

CONSIDERACIONES

Dentro de las actividades que se deben realizar para que el desarrollo e implantación de un plan de contingencia sea el adecuado son recomendables las siguientes acciones:

- ♦ Designar al grupo encargado de elaborar el plan de contingencia

Dar a la organización propuesta prioridad sobre la organización tradicional para ejecutar las acciones

especificadas dentro del plan de contingencia.

- ♦ Considerar a los niveles de contingencia como una aplicación vital del negocio y como registros vitales los documentos que generen.

Tomar en cuenta los factores externos que puedan afectar la operación de la organización al elaborar el plan de contingencia.

ORGANIZACIÓN DIRECTIVA

Es la autoridad máxima de la organización en materia de

administración y operación del plan de contingencia.

ATRIBUCIONES

- ♦ Actuar como unidad administrativa para realizar la coordinación de planeación, organización, integración, dirección, ejecución y

control, en materia de planes de contingencia.

- ♦ Ejerce el nivel de autoridad máximo en caso de contingencias

-
-
1. Director General ◆ Decidir la puesta en operación de la organización encargada de la aplicación del plan de contingencia. ◆ Coordinar las acciones y aprobar las decisiones de la organización directiva. 1.1 Coordinador general ◆ Establecer, coordinar y administrar el plan de contingencia para el control de las operaciones ◆ Obtener, interpretar y analizar los informes de cada uno de los grupos de coordinación específica. ◆ Establecer los enlaces de comunicación eficientes entre la	dirección general y la estructura operativa. ◆ Establecer y emitir la comunicación con el exterior. ◆ Coordinar las pruebas para asegurar la operabilidad del plan. 1.1.1 Coordinador del grupo ◆ Actuar y decidir en el ámbito de su competencia. ◆ Informar de los avances y resultados de sus funciones asignadas.

ORGANIZACIÓN OPERATIVA

Es el área encargada de ejecutar las acciones necesarias para el cumplimiento del plan de contingencia.

ATRIBUCIONES

Realizar las actividades establecidas por el coordinador respectivo. 1.1.1. Grupo administrativo A. Recursos Humanos 1. Servicios médicos	2. Localización de personal 3. Transportación B. Recursos Materiales 1. Servicios de oficina 2. Contratación de servicios
-
-

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

-
-
3. Adquisición de equipos C. Recursos Financieros 1. Gastos de emergencia 2. Contabilidad en el pago de la nómina 3. Seguros 4. Indemnizaciones 5. Financiamientos para garantizar la continuidad de la operación y la recuperación. D. Apoyo Legal 1. Asesoría jurídica y formulación de opciones en las consultas de tipo legal. 2. Responsabilidad legal 3. Contratos y convenios 4. Suspensión de pagos E. Relaciones Públicas Mantener el control con: 1. Servicios de emergencia 2. Organización operativa 1.1.2. Grupo de Bienes Inmuebles 1. Tener disponibles en el tiempo requerido las instalaciones y servicios para la operación.	2. Coordinar con los otros grupos de operación la selección y diseño de instalaciones. 3. Supervisar la instalación física de equipos, servicios y mobiliario 1.1.3 Grupo de Servicios Técnicos 1. Restablecer la infraestructura de cómputo 2. Realizar una evaluación de daño 3. Proporcionar opciones de evaluación. 4. Asegurar que el procesamiento normal pueda llevarse a cabo tan pronto como los datos, equipos y comunicaciones requeridos estén disponibles. 5. Coordinar que los grupos de hardware, software, y comunicaciones,
-
-

-
-
restablezcan al ambiente de cómputo. 6. Realizar pruebas de equipos para determinar las consideraciones de operabilidad. 1.1.4. Grupo de Sistemas o Aplicaciones Vitales 1. Restablecer la operación de los sistemas en el menor tiempo posible, con base en el programa de registros vitales. 2. Establecer los procedimientos de recuperación y respaldo 3. Asegurar que cualquier aplicación crítica sea	procesada dentro del tiempo requerido. 4. Control de documentación 5. Un plan más amplio también incluye áreas de operación fuera del proceso de datos principal. Debe tener un alcance extenso si se desea contemplar efectivamente los muchos escenarios de desastre que pueden afectar la organización.

ASPECTOS BASE

Los aspectos base de un plan de contingencia pueden dirigirse sobre algunas de las siguientes áreas:

1. **Facilidad de destrucción.**

El equipo de planeación debe considerar la total destrucción de la operación

principal y/o la instalación de procesamiento. El plan debe incluir revisiones que podrían ser necesarias en caso de que las instalaciones primarias fueran sólo parcialmente destruidas.

2. **Disponibilidad de personal**

El organigrama para el plan de contingencia en caso de desastre debe ser un subgrupo que incluya personal de toda la organización, con las posiciones clave identificadas como necesarias para ejecutar el plan.

3. Determinar los tiempos del desastre

Las consideraciones deben ser dadas para los diversos momentos en que un desastre puede ocurrir, para tratar de identificar los tiempos en que podrá haber los más devastadores efectos sobre la organización.

Algunas organizaciones dependen totalmente del procesamiento nocturno, mientras otras pueden creer que la falta de disponibilidad de sistemas en la línea durante las horas pico de servicio a la clientela, pueden ser el más devastador período de tiempo. Otras consideraciones pueden incluir el efecto sobre la organización en fin de mes, fin de cuatrimestre o fin de año, si estos procesos fueran demorados a causa de un desastre.

4. Instalaciones de almacenamiento fuera del centro de cómputo

Muchas organizaciones suponen que estas instalaciones sobrevivirán al desastre; esto puede ser un falso supuesto si la instalación está cerca al desastre. Ciertamente, los medios magnéticos protegidos, el aprovisionamiento crítico y otros registros proveerán los medios para recuperar la normalidad de operación.

Otros aspectos que el equipo de planeación debe considerar incluyen:

- ◆ Desastres que afecten únicamente a departamentos usuarios específicos
- ◆ Trabajos sin procesar y trabajos en proceso
- ◆ Destrucción de microcomputadoras
- ◆ Redes inoperables de telecomunicaciones.

El plan de contingencia debe ser documento con vida, es decir, debe ser dinámico, por lo que se deberá estar modificando cada vez que cambien algunos de los siguientes factores:

1. Cambio de personal
2. Cambio de equipo de instalación

3. Cambio de teléfonos
4. Cambio de sistemas
5. Cambio de contratos de mantenimientos
6. Cambio en las pólizas de seguros
7. Ruptura de privacidad en el plan de contingencia y recuperación
- Cambio en las instalaciones de respaldo y alternas.

ELEMENTOS DEL PLAN DE CONTINGENCIA

El Plan de contingencia contempla tres tipos de acciones, las cuales son:

1. ACCIONES DE EMERGENCIA

Deben contener el daño en el momento, así como limitarlo tanto como sea posible, contemplando todos los desastres naturales y eventos no considerados.

2. ACCIONES DE RECUPERACIÓN

Abarcan el mantenimiento de partes críticas entre la pérdida del servicio y los recursos, así como su recuperación o restauración.

3. ACCIONES DE RESPALDO

Conjunto de acciones a realizar una vez que se ha presentado cualquier contingencia que afecte la continuidad operativa, ya sea en forma parcial o total, del centro de procesamiento de datos, a las instalaciones auxiliares, recursos, información procesada, en tránsito y almacenada, con la finalidad de estar preparados para hacer frente a cualquier contingencia. De esta forma se reducirá su impacto, permitiendo restablecer a la brevedad posible los diferentes servicios interrumpidos.

PLAN DE RECUPERACIÓN EN CASO DE DESASTRE

“La importancia que se le da a la seguridad, es directamente proporcional al grado de percepción del riesgo que se tenga”

Las acciones del plan de recuperación en caso de desastre, se implementan como medidas previsoras, pero entran en función una vez que se constata el daño.

Su objetivo es establecer la metodología y los recursos necesarios con la finalidad de restablecer los servicios de cómputo en forma oportuna, al presentarse cualquier contingencia.

Responsabilidades del Plan de Respaldo

Los responsables de la ejecución, el plan de respaldo y las responsabilidades que competen a cada uno de ellos.

El área de sistemas que diseña una aplicación es responsable de:

- ◆ Definir estrategias de respaldo, y conjuntamente con el usuario, verificar su validez y eficacia.
- ◆ Elaborar los programas y procesamiento de cómputo necesarios para obtener y validar el contenido de los respaldos y la vigencia de su contenido.
- ◆ Definir, conjuntamente con el usuario, los mecanismos de respaldo que permitan continuar con la operación normal ante la presencia de una contingencia grave o

desastrosa en el centro o en los centros de cómputo.

- ◆ Elaborar los programas y procedimientos que permitan la generación de los mecanismos de respaldo necesarios para cubrir las contingencias graves en los sistemas y equipos de cómputo.

DESCRIPCIÓN DEL PROGRAMA

La planeación del plan de recuperación es un proceso que requiere de la redirección y evaluación técnica del personal y recursos del procesamiento de información de una forma apropiada.

El proyecto para el desarrollo e implementación del plan de

recuperación de desastres y el plan de reanudación del negocio debe ser parte del plan de actividades normales de la organización.

Metodología del Trabajo

Fase 1. Actividad de pre-planeación (proyecto inicial)

La fase uno se utiliza para obtener y entender la existencia y los ambientes de proyectos de computación de la organización. Esto permite que el equipo del proyecto pueda referirse al alcance del proyecto y la asociación del programa de trabajo, desarrollar proyectos de programación e identificar y direccionar cualquier problema que pueda tener un impacto en la entrega y el éxito del proyecto.

Durante esta fase, un comité de dirección debe estar establecido el cual debe tener cubierta toda la

responsabilidad para informar a la dirección y guiar al equipo de trabajo. El comité también debe ser hacer todas las decisiones relacionadas con los esfuerzos del plan de recuperación. El director del proyecto debe trabajar con el comité de dirección para definir con detalle el trabajo y desarrollar programas de entrevistas para conducir la seguridad y el análisis de los impactos en el negocio.

Otras dos claves para esta fase son el desarrollo de una política y un programa de conciencia.

Fase 2 Evaluación de Vulnerabilidad y Definición General de Requerimientos

Esta fase direcciona medidas para reducir la posibilidad de ocurrencia.

Incluye las siguientes tareas clave:

Una seguridad absolutamente completa en la evaluación del equipo de cómputo y en el ambiente de las comunicaciones incluyendo prácticas personal; seguridad física; procesos operativos; planes de contingencia y respaldos; desarrollo de sistemas y mantenimiento; seguridad en base de datos; seguridad en las comunicaciones de voz y datos; software de seguridad para sistemas y controles de acceso; seguros; administración y planes de seguridad; control de aplicaciones y computadoras personales.

- ◆ La evaluación de la seguridad permite que el equipo del proyecto mejore cualquier plan de emergencia y medidas para la prevención de desastres y para implementar los requerimientos en el plan de emergencias y medidas de

prevención de desastres donde no los exista.

- ◆ Definir el alcance en la planeación del esfuerzo.
- ◆ Analizar, recomendar y comparar planes de recuperación y requerimientos en el mantenimiento del software para apoyar el desarrollo de los planes y para mantener actualizados los planes y/o para la siguiente implementación.
- ◆ Desarrollar del marco del plan de trabajo.
- ◆ Reunir el equipo del proyecto y conducir sesiones de trabajo.

Fase 3 Análisis del Impacto en los Negocios

Permite al equipo del proyecto identificar sistemas críticos y desastres que resultan de los accesos denegados a servicios del sistema y otros servicios y facilidades. De esta forma se puede fijar el “umbral del dolor”, es decir, definir la medida de las unidades de tiempo que la organización puede sobrevivir sin el

acceso a los sistemas, los servicios y las facilidades.

El reporte debe de presentarse al “comité de dirección”. Este reporte por lo tanto debe de utilizarse como algo básico para identificar sistemas y requerimientos de recursos para apoyar los servicios críticos que proporcionan procesamiento de información y otros servicios y facilidades.

Fase 4 Definición detallada de Requerimientos

Es para ser utilizado como una base para analizar las estrategias alternativas para la recuperación. Está desarrollado para identificar recursos que se requieran para apoyar las funciones críticas identificadas en la fase 3. Además se debe incluir hardware de mainframe, comunicaciones, comunicaciones de voz y datos, computadoras personales, software (proveedores, vendedores, desarrolladores en casa, etc.), documentación (de usuarios y procedimientos), soporte externo (redes públicas, servicios, etc.) y personal para

cada unidad del negocio. Las estrategias de recuperación estarán basadas en un período a corto, mediano y largo plazo en general.

Otra llave de liberación de esta fase es la identificación de un plan de alcance de objetivos y suposiciones.

Fase 5 Plan de Desarrollo

Los componentes del plan de recuperación están definidos y los planes están documentados. También incluye la implementación de cambios para utilizar los procedimientos, las actualizaciones de procedimientos de datos existentes, operación de procedimientos requeridos para apoyar las estrategias de recuperación y alternativas seleccionadas, negociaciones con contactos de vendedores (quienes ofrecen los servicios de recuperación, sus roles y responsabilidades. Los estándares de recuperación también pueden ser desarrollados durante esta fase.

Fase 6 Programa de Pruebas

El objetivo de las pruebas y ejercicios está establecido y las alternativas para la estrategia de pruebas son evaluadas. Las estrategias de pruebas para el ambiente deben ser seleccionadas y el programa de pruebas continuas debe establecerse.

Fase 7 Programa de Mantenimiento

El programa debe reflejar los cambios para el ambiente que están apoyados por el plan. Esto es vital, ya que existen cambios para el manejo de procesos los cuales son revisados para tomarlos en cuenta. En áreas donde el manejo de los cambio no existe, un procedimiento para manejo de cambios y la implementación es recomendable. Varios productos de software para recuperación toman en cuenta este requerimiento.

Fase 8 Plan Inicial de Pruebas e Implementación

Una vez que los planes son desarrollados, las pruebas iniciales del plan son conducidas siguiendo la secuencia e incluso, si fuera necesario,

realizando alguna modificación basada en un análisis del test de resultados.

Las actividades específicas son:

1. Definición de metas y objetivos del test
2. Identificación de quipos para el test
3. Estructurar el test
4. Conducir el test
5. Analizar resultados del test
6. Realizar las modificaciones apropiadas sobre el plan

El objetivo es someter a prueba el plan seleccionado para encontrar errores que deben ser corregidos.

Una vez que las estrategias de recuperación son definidas, los procedimientos específicos de pruebas deben ser desarrollados para asegurar que los planes escritos sean comprensibles y actuales.

Planeación del alcance y objetivos del plan

El objetivo primordial de la planificación de recuperación es permitir que una organización sobreviva ante un desastre y continúe las operaciones del negocio normalmente. Para sobrevivir, la organización debe asegurarse que las operaciones críticas puedan continuar su procesamiento normal a través del esfuerzo de recuperación; el plan establece claramente las líneas de autoridad y prioridades en los esfuerzos del trabajo. Los problemas clave para el plan de contingencia deben ser:

- ◆ Proporcionar seguridad y entrenamiento al personal que entrará en acción al momento de ocurrir un desastre.
- ◆ Continuar con las operaciones críticas del negocio.
- ◆ Reducir la operación de un disturbio serio en las operaciones y resultados (ambos, información de los procesos y otros recursos).
- ◆ Reducir inmediatamente el daño y las pérdidas.

- ◆ Establecer sucesores de la dirección y fuerzas de emergencia.
- ◆ Facilitar la efectiva coordinación de tareas de recuperación.
- ◆ Reducir la complejidad de los esfuerzos de la recuperación.
- ◆ Identificar líneas críticas de los negocios y funciones de soporte.

La administración puede asignar roles y responsabilidades para la planeación de la recuperación a un empleado dedicado a este servicio.

La dirección debe tomar una decisión para controlar un proyecto que satisfaga los siguientes objetivos:

- ◆ Determinar vulnerabilidad para servicios importantes en caso de interrupciones en el centro de datos y negocios, así como brindar facilidades y definir medidas preventivas que puedan tomarse para reducir la probabilidad e impactos de interrupciones.
- ◆ Identificar y analizar la economía, servicios, imagen publicitaria y otras implicaciones en el servicio de

interrupciones externas en el centro de datos y otras facilidades en el negocio.

- ◆ Determinar inmediatamente las necesidades de recuperación en períodos cortos y largos, así como las fuentes de requerimientos.
- ◆ Identificar las alternativas y seleccionar el acercamiento más efectivo para realizar operaciones de

respaldo en las operaciones y servicios de restauración.

Desarrollar e implementar planes de contingencia que cubran ambos sentidos: necesidades a corto y largo plazo, para el centro de datos y otras facilidades del negocio.

Organización del proyecto y del personal

La organización del equipo encargado del proyecto está diseñada para aumentar la flexibilidad de las necesidades para tratar con la implementación del plan de la manera más eficientemente posible.

Una clave de éxito es el desarrollo e implementación de un programa para la recuperación en las organizaciones que estén dedicadas de tiempo completo y que cuenten con los recursos para la recuperación de los negocios y la planeación de la continuidad.

Debe asegurarse que el personal con responsabilidades específicas para l

recuperación esté preparado para ejecutar el plan.

Debe asegurarse que el personal con responsabilidades específicas para la recuperación esté preparado para ejecutar el plan.

Esto no se puede lograr con recursos de tiempo completo con responsabilidades como el mantenimiento de los planes; la coordinación de componentes y planes de pruebas completos, la capacitación de personal con responsabilidades para recuperación, y la actualización de los planes para reflejar los cambios de la

información procesada y el ambiente del negocio.

Comité de la dirección

Debe incluir representación de áreas claves de la organización, como las siguientes:

1. Sistemas de información
2. Soporte tecnológico
3. Desarrollo de sistemas

4. Servicio de operaciones y redes
5. Comunicaciones
6. Unidades clave en el negocio

Equipo del proyecto

La composición del equipo del proyecto puede variar dependiendo de los ambientes y del negocio para los cuales el plan se desarrolle.

El personal de las unidades responsables de la recuperación y continuidad de la planeación debe realizar el papel de coordinador de las actividades de prueba, revisiones de planes y mantenimiento del plan maestro.

El equipo del proyecto correspondiente es automáticamente parte de otros

equipos de proyectos. La auditoría interna debe ser invitada para formar parte de todos ellos. Los directores representativos de varios proyectos pueden seleccionarse para recomendar otros individuos en su área para representarlos o para juntar grupos específicos donde su experiencia será requerida para el desarrollo de sus planes.

Sugerencias para la composición de un equipo básico

◆ Dirección del proyecto	◆ Soporte de sistemas
◆ Operaciones de redes y cómputo	◆ Voz, redes y comunicaciones

Sugerencias para sistemas de información y soporte a la tecnología

◆ Redes y comunicaciones	◆ Sistemas de seguridad informática
◆ Facilidades de dirección	◆ Operaciones
◆ Desarrollo y soporte de redes	◆ Soporte de redes
Administración de base de datos	◆ Implementación de redes

Control de proyecto

El control de manejo de este proyecto debe estar aprobado por el proyecto de manejo de software. El software debe

utilizarse para tareas específicas e identificación para liberaciones y sus fuentes.

Fuentes de requerimientos

En algunas organizaciones que han tratado de desarrollar planes para la continuación de sus labores cuando se presentan desastres pierden tiempo y dinero desarrollando planes de recuperación, pues fracasan en el al tanto durante el ciclo del desarrollo y que un recurso esté dedicado al diario mantenimiento del programa.

Las fuentes de requerimientos están divididos dentro de tres categorías:

- ◆ Personal

mantenimiento de sus recuperaciones comparadas con la competencia.

Es, por lo tanto, esencial que el manejo esté comprometido para el desarrollo, implementación y mantenimiento de su programa. Requiere de fuentes que estén

- ◆ Costo de capital
- ◆ Costo diario

GLOSARIO DE TÉRMINOS

Acceso: Momento que precede a la utilización de un sistema de información o de una red. Puede efectuarse a través de cables, terminales y dispositivos (acceso físico) o a través de programas (acceso lógico).

Administrador: Responsable de los intereses de la seguridad de la información y del cumplimiento de las disposiciones legales e internas de la institución, referente a la planificación, instalación, funcionamiento y control de sistemas de información.

Análisis de riesgos: Determinación de capacidad que es necesario emplear en materia de medidas de defensa, relacionadas con el peligro existente, a fin de alcanzar un equilibrio adecuado entre costo y beneficio.

Archivo: Conjunto de datos relacionados con características comunes compuesto por registros.

Auditoria: Seguimiento de las actividades de los usuarios, mediante el registro de determinados tipos de sucesos en el registro de seguridad de un servidor o estación de trabajo.

Backup: Proceso por el cual se obtiene una copia funcional de la información de un sistema, la cual puede ser empleada cuando se presenten fallos.

Base de datos: recopilación de información almacenada en una computadora que permite el rápido acceso a los datos.

Búfer: Área para el almacenamiento temporal de información.

CD-ROM: Soporte de almacenamiento de información para computadoras que

permite su lectura y escritura por medios ópticos.

CPU: Unidad Central de Procesamiento.

Es responsable de controlar el flujo de datos y la ejecución de las instrucciones de los programas sobre los datos; puede sumar, restar, multiplicar, dividir y comparar números y caracteres.

CLUF Contrato de licencia de usuario final.

Cableado: Función de procesamiento integrada a los circuitos electrónicos de la computadora en lugar de que le proporcionen instrucciones de un programa.

Centros de Cómputo: Un sistema o conjunto de sistemas, para obtener información oportuna y adecuada. Oficina que presta servicios de computación, como el manejo de un computador y su equipo periférico, la

escritura de programas de aplicación e informes de computación, así como otros servicios diversos a una amplia variedad de personas.

Contraseña: Cadena de caracteres exclusiva que debe introducirse antes de que se autorice el inicio de una sesión o el acceso a un sistema.

Computadora: es un dispositivo electrónico de uso general que realiza operaciones aritmético-lógicas a gran velocidad, de acuerdo con instrucciones internas, que se ejecutan sin intervención humana.

Correo electrónico: servicio en Internet que permite el envío de correspondencia entre usuarios, incluyendo textos, imágenes, videos, audio, programas, entre otros.

Cuenta de usuario: Consta de toda la información que define a un usuario.

Esto incluye aspectos tales como: nombre del usuario y la contraseña necesaria para iniciar una sesión, los grupos a los que pertenece la cuenta de usuario y los derechos y permisos de que dispone el usuario para la utilización del sistema y para el acceso a los recursos del mismo.

Clasificación: Establecimiento del grado de necesidad de protección de los documentos.

Cracker: es una persona que intenta acceder a un sistema informático sin autorización.

Criptografía: Procedimiento que permite a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, tras haberlo descifrado.

Encriptación; Proceso para ocultar información, alterar un texto para que no muestre información coherente.

Datos: Información real, como texto, números, sonidos e imágenes, en una forma que una computadora pueda procesar.

Delitos informáticos: el delito en computadora es la comisión de actos fuera de la ley usando la tecnología de la computación o la informática.

Derechos: Autoriza a un usuario a realizar ciertas acciones en el sistema.

Derechos de acceso: Autorizaciones fijadas o por definir en los sistemas operativos para el acceso a datos y a medios de explotación.

Discos Duros: es el medio de almacenamiento que puede almacenar más datos y se puede recuperar más

rápidamente que en los flexibles o disquetes.

Disco ópticos (CD ROM): es otra forma nueva de almacenamiento secundario, que almacena datos ópticamente, con la misma tecnología de las grabaciones musicales en CD.

Ergonomía: Es la disciplina tecnocientífica que interviene en la adaptación del trabajo y las condiciones de trabajo para la comodidad y sanidad del trabajador.

Falsificación de software es la duplicación ilegal y venta de software con derechos de autor, frecuentemente en una forma diseñada para que el producto parezca legítimo.

FIREWALLS: (paredes de fuego), es un sistema o grupo de sistemas que deciden qué servicios pueden ser accesados desde el exterior de una red.

Gateway: (pasarela) Hoy se utiliza el término router (direccionador, encaminador, enrutador) en lugar de la definición original. Pasarela es un programa o un dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero implantaciones diferentes.

Hacker: (pirata) una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores.

Hardware: Todos los componentes electrónicos, eléctricos y mecánicos que componen una computadora.

Identificación del usuario: sucesión de caracteres que identifican a un usuario frente al sistema.

Internet: Soporte de comunicación entre computadoras.

Licencia para uso de software: acuerdo legal incluidos en los programas comerciales, que especifica los derechos y las obligaciones que adquiere el comprador del programa y fija la responsabilidad del editor del software.

Login: proceso de presentación para acceder a un sistema en diálogo directo o a sistemas alejados a través de una red.

Manual: es un cuerpo sistemático que indica las actividades a ser cumplidas por los miembros de una organización y la forma en que las mismas deben ser realizadas.

Mantenimiento correctivo: consiste en actuar o sustituir algo que ya se dañó.

Mantenimiento preventivo: es el procedimiento mediante el cual se contribuye a través de la limpieza de equipos que trabajen adecuadamente previniendo antes que suceda cualquier situación de daño.

Procedimientos estándar de operación: son reglas definidas con precisión para realizar tareas desarrolladas para enfrenar situaciones esperadas.

Password: (clave) Sucesión de caracteres que un usuario tiene que comunicar a un sistema como prueba de su identificación.

Piratería: modo irregular de adquisición de un ejemplar de software de sistema o de otros programas, así como de datos y documentos.

Políticas: Bases establecidas para definir el nivel de seguridad de una red.

Procedimiento: descripción detallada de los pasos a seguir para solucionar un problema.

Programa: conjunto de instrucciones o sentencia, con un orden lógico, que le dicen al computador qué hacer y cuánto hacerlo, escrito en un lenguaje de programación.

Programa antivirus: programa para la localización de virus informáticos.

Protocolo: Es un conjunto de reglas que gobiernan comunicación entre entidades de una misma capa-

Red: conjunto formado por todas las estaciones y por los sistemas de comunicación utilizados para el enlace de las mismas.

Root: usuario principal en un sistema Unix.

Router: Dispositivo que distribuye tráfico entre redes.

Seguridad: Protección del hardware y del software contra el acceso, la utilización, la modificación, la destrucción o la divulgación ya sean accidentales o delictivos. La seguridad atañe también al personal, los datos, las comunicaciones y la protección física y lógica de las instalaciones informáticas.

Seguridad de la información: conjunto de prevenciones y medidas destinadas a la protección de informaciones frente a la pérdida de confidencialidad

Servidor: Es una computadora que proporciona recursos compartidos a los usuarios de la red.

Sistemas de nivel operativo: Son los que hacen el seguimiento de las actividades y las transacciones elementales de la organización.

Tecnología: Herramienta de la que dispone el administrador para enfrentar el cambio de hoy en día.

Usuario: Toda persona que utiliza sistemas, programas, procesos, entre otros, de información, independientemente del nivel de conocimiento requerido o de los privilegios especiales de que pueden disfrutar.

Virus: Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas.

Zip: (comprimir) Acción de empaquetar en un solo fichero uno o más ficheros que habitualmente son también comprimidos, con objeto de que ocupen menos espacio en disco y se precise menos tiempo para enviarlos a la red.

BIBLIOGRAFÍA DEL MANUAL

- colpos.mx/cominf/mmsegurid.htm
- w.monografias.com
- w.mipagina.cantv.net/arte_ernesto/auditoria_y_seguridad_informatic.htm
- w.culmx/apuntes/afi
- w.cpcipc.org/razonestado/seguridad.htm
- w.geocities.com/athens/olympus/7428/virus1.html
- w.members.nbci.com/segutot/el.htm
- OLGUIN, Romo Heriberto. **Organización y Administración de Centros de Cómputo.** Primera Edición. México D.F. 1997
- SUAREZ, Domínguez Federico. **Seguridad en Centros de Cómputo.** Edición S.I. México D.F. 1991
- FINE, Leonard H. **Seguridad en los Centros de Cómputo: Políticas y Procedimientos.** Edición Trillas México, D.F. 1998.

BIBLIOGRAFIA

- “Centro de Enseñanza de Computación”, **Folleto del CETEC**
- Código Procesal Penal de El Salvador
- Echenique, José Antonio, **Auditoria en Informática**, McGraw Hill LR 90.
- Gómez Ceja, Guillermo, **Sistemas Administrativos**, McGraw Hill.
- Kenneth C. Laudon, Jane P. Laudon, **Administración de los Sistemas de Información**. México DF. 3ª Edición, 1996. p 884 Prentice Hall
- Menschel Richard F., **Management by System** McGraw Hill, p.10.
- Normativa General Para la **Modernización del Órgano Ejecutivo, Jul 23-1999**
- Place, Irene, **Business Report Administrative Analysis**, Michigan, p28.
- Senn A., **Análisis y Diseño de Sistemas de Información**. México DF., 2ª. Edición 1994. p884.
- Stephen Cobb, **Manual de Seguridad para PC's y Redes Locales**. 2ª. Edición. McGraw Hill