UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

ESCUELA DE COMPUTACIÓN

TEMA:

ANALISIS, DISEÑO E IMPLEMENTACION DE PLAN CONTINGENCIAL PARA LA ADMINISTRACION DE RECURSOS DE RED, APLICADO A: "INSTITUCION GUBERNAMENTAL, DEDICADA A LA ADMINISTRACION Y FOMENTO DEL COOPERATIVISMO EN EL SALVADOR".

PARA OPTAR AL TITULO DE:

INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

PRESENTAN:

MAURICIO SAUL QUINTEROS DIAZ

RICARDO MANUEL PINEDA SANTILLAN

ASESOR:

MASTER ING CARLOS QUIÑONEZ

Ciudadela Don Bosco, febrero de 2007.

Soyapango, El Salvador.

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

ESCUELA DE COMPUTACIÓN

AUTORIDADES DE LA UNIVERSIDAD DON BOSCO

RECTOR:

ING. FEDERICO MIGUEL HUGUET

VICE-RECTOR ACADEMICO:

PADRE VICTOR MANUEL BERMUDEZ

SECRETARIO GENERAL:

LIC. MARIO OLMOS ARGUETA

DECANO DE LA FACULTAD DE INGENIERIA:

ING. GODOFREDO GIRON

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

ESCUELA DE COMPUTACIÓN

JURADO EVALUADOR

MASTER ING CARLOS QUIÑONEZ

Asesor.

ING. JORGE ABERTO CHAVEZ

Jurado

ING. DAX FERNANDO GARCIA

Jurado

ING. JOSE ALBERTO DAVILA

Jurado

AGRADECIMIENTOS

Agradecemos en primer lugar a Nuestro Señor Jesucristo, ya que ha sido por medio de El, que hemos podido llevar a la finalizacion nuestros estudios, esforzandonos por medio de las fuerzas que el ha derramado en nosotros.

A nuestros Padres, que nos han guiado dia con dia, con esfuerzo en nuestras vidas, mostrandonos el camino que debiamos seguir para poder alcanzar nuestra formacion academica; de igual manera a nuestra familia, quienes nos apoyaron en todo momento.

A nuestros Catedraticos, que en el transcurrir de los años nos enseñaron sobre las distintas materias, permitiendonos cada dia profesionalisarnos a traves de su experiencia y sabiduria.

A nuestro Asesor de trabajo de graduacion, quien con esfuerzo y corage nos enseño a realizar el documento, guiandonos en cada paso del mismo; enriquiciendo con esto el producto final.

INTRODUCCION

En la actualidad las empresas se han vuelto cada vez más dependientes de las computadoras y las redes para manejar sus actividades, esta dependencia hace que las mismas se especialicen poco a poco en la busqueda y uso de tecnologia de punta que les permita realizar sus actividades en el menor tiempo posible con eficiencia y eficacia. Por lo que se vuelve impresindible, contar con herramientas que le permitan reaccionar ante eventos que esten fuera de su control, en lo que se refiere a lo tecnologico. Con lo que se asegure, el brindar el servicio al cliente con calidad, en cualquier momento que este lo solicitase.

En el trabajo de graduacion que a continuacion se presenta, el cual ha sido diseñado en el caso especifico de una empresa gubernamental, se construyo una herramienta que brinda la seguridad a la empresa para poder reaccionar ante diferentes situaciones, permitiendole a la vez, asegurar la calidad en el servicio al cliente, en todo momento. Esta herramienta denominada Plan de Contingencia, esta compuesta por dos grandes areas, una de ellas es Plan Contingencial, el cual comprende algunos de los posibles desastres, que se podrian encontrar en la oficina de dicha empresa, detallando en cada uno de estos los pasos a seguir, antes y despues según sea el caso; la segunda herramienta que se detalla en este trabajo de graduacion es el Manual de Procedimiento y Politicas de Administracion de Red, el cual tiene como objetivo principal el completar las acciones para minizar riesgos en la empresa, ademas de reglamentar los procedimientos y politicas que se deben utilizar en la administracion de la red de datos.

INDICE

No. Pagina

AGRADECIMIENTOS……i

INTRODUCCION……ii

CAPITULO I ANTECEDENTES ¡ERROR! MARCADOR NO DEFINIDO.

1.1 ANTECEDENTES DE ESTRATEGIA DE SEGURIDAD PREVENTIVA 7

1.2 PLANTEAMIENTO DEL PROBLEMA 8

1.3 JUSTIFICACIÓN E IMPORTANCIA 9

1.4 OBJETIVOS 12

1.4.1 OBJETIVO GENERAL 12

1.4.2 OBJETIVOS ESPECIFICOS 12

1.5 ALCANCES Y LIMITACIONES 13

1.5.1 ALCANCES 13

1.5.2 LIMITACIONES 13

CAPITULO II. MARCO TEÓRICO 14

2.1 PLAN CONTINGENCIAL 16

2.1.1 PLAN DE RECUPERACIÓN DEL NEGOCIO EN CASO DE CONTINGENCIAS. 16

2.2 SEGURIDAD INFORMATICA 17

2.2.1 ANÁLISIS DEL OBJETIVO DE SEGURIDAD INFORMÁTICA 17

2.3 AMENAZAS 19

2.3.1 AMENAZAS NATURALES 20

2.3.1.1 PRESENTACIÓN 20

2.3.1.2 TERREMOTOS 21

2.3.1.3 INTENSIDAD Y MAGNITUD DE LOS TERREMOTOS 21

2.3.1.4 ERUPCIONES VOLCÁNICAS 24

2.3.1.5 CLASIFICACION DE LOS VOLCANES 25

2.3.1.6 CLASIFICACIÓN DE LAS ERUPCIONES 26

2.3.1.7 VIGILANCIA Y PREVISIÓN DE LAS ERUPCIONES 26

2.3.1.8 EFECTO DE LAS ERUPCIONES EN EL MEDIO NATURAL 27

2.3.1.9 INUNDACIONES 29

2.3.1.9.1 TIPOS DE DAÑOS CAUSADOS POR INUNDACIONES 31

2.3.1.10 INCENDIOS 32

2.3.1.10.1 INCENDIOS INDUSTRIALES 34

2.3.1.10.2 INCENDIOS URBANOS 35

.

2.4 ADMINISTRACION DE RECURSOS TECNOLOGICOS 35
2.4.1 ORGANIZACIÓN DE LOS RECURSOS TECNOLOGICOS..... 35
2.4.2 ELEMENTOS MATERIALES 37
2.4.3 ELEMENTOS PERSONALES 38
2.4.4 ELEMENTOS FUNCIONALES 38
2.5 ADMINISTRACION DE RIESGO 39
2.5.1 ESTRATEGIAS DE SEGURIDAD 41
2.5.1.1 DEFINICION DE ESTRATEGIAS 43
2.5.2 INDICADORES TECNOLOGICOS 44
2.6 DAÑO 47
2.6.1 HACKERS 48
2.6.2 CRACKERS 48
2.6.3 VIRUS 49
2.6.4 GUSANOS 49
2.6.5 TROYANOS 50
2.7 PROCESO DE TECNOLOGIA DE INFORMACION 50
2.7.1 UN RESULTADO DESEADO, SE ALCANZA CON MAS EFICIENCIA CUANDO SUS ACTIVIDADES Y RECURSOS RELACIONADOS, SON MANEJADOS COMO PROCESOS. 50
2.8 ARQUITECTURA DE SEGURIDAD PARA AREAS INFORMATICAS 52
2.8.1 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA..... 52
2.8.1.1 PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD 53
2.8.1.1.1 PRINCIPIO DE MENOR PRIVILEGIO 54
2.8.1.1.2 LA SEGURIDAD NO SE OBTIENE A TRAVÉS DE LA OSCURIDAD 54
2.8.1.1.3 PRINCIPIO DEL ESLABÓN MÁS DÉBIL 55
2.8.1.1.4 DEFENSA EN PROFUNDIDAD: 56
2.8.1.1.5 PUNTO DE CONTROL CENTRALIZADO 56
2.8.1.1.6 SEGURIDAD EN CASO DE FALLO 56
2.8.1.1.7 PARTICIPACIÓN UNIVERSAL 57
2.8.1.1.8 SIMPLICIDAD 57
2.8.2 NORMAS Y ESTRUCTURAS..... 58
2.8.3 PROCEDIMIENTOS Y SOPORTE 60
2.8.3.1 PROCEDIMIENTOS DE SEGURIDAD 60
2.8.3.1.1 ELABORACIÓN DE PROCEDIMIENTOS DE SEGURIDAD 60
2.8.3.2 SOPORTE DE SEGURIDAD 62
2.8.3.2.1 FUNCIONES DEL SOPORTE DE SEGURIDAD 62
2.9 LA TECNOLOGÍA DE INFORMACIÓN 63

2.9.1 INTRODUCCIÓN *63*
2.9.2 LA CREACIÓN DEL CONOCIMIENTO Y LA VENTAJA COMPETITIVA *64*
2.9.2.1 VENTAJA COMPETITIVA 65
2.9.3 CONCLUSIONES *66*
2.10 MANTENIMIENTO PREVENTIVO 67
2.10.1 VENTAJAS DEL MANTENIMIENTO PREVENTIVO *68*
2.10.2 FASES DEL MANTENIMIENTO PREVENTIVO *69*
2.11 VULNERABILIDAD 69
2.11.1 TIPOS DE VULNERABILIDAD *69*
2.11.1.1 VULNERABILIDAD FÍSICA 69
2.11.1.2 VULNERABILIDAD NATURAL 70
2.11.1.3 VULNERABILIDAD DEL HARDWARE Y DEL SOFTWARE 70
2.11.1.4 VULNERABILIDAD DE LOS MEDIOS O DISPOSITIVOS 70
2.11.1.5 VULNERABILIDAD POR EMANACIÓN 70
2.11.1.6 VULNERABILIDAD DE LAS COMUNICACIONES 71
2.11.1.7 VULNERABILIDAD HUMANA 71

CAPITULO III. 72

3.1 METODOLOGIA DE LA INVESTIGACION. 72
3.2 DELIMITACION DE LA INVESTIGACION. 75
3.2.1 DELIMITACIÓN GEOGRÁFICA. *76*
3.2.1.1 IMPACTO DE SUSPENSIÓN DE SERVICIOS 76
3.2.2 DELIMITACIÓN TEMPORAL *77*
3.3 DETERMINACION DE EL UNIVERSO Y LA MUESTRA. 77
3.4 PRESENTACION DE LA INFORMACION 78
3.4.1 ENCUESTA *79*
3.5 SITUACIÓN ACTUAL. 107

CAPITULO IV 110

PLAN CONTINGENCIAL 110
4.1.1 INTRODUCCION *111*
4.1.2 CRITERIOS *111*
4.1.3 OBJETIVOS *112*
4.1.3.1 GENERAL 112
4.1.3.2 ESPECIFICOS 112
4.1.4 COMITÉ DE CONTINGENCIA *113*
4.1.4.1 INTEGRACION 113

.

4.1.4.2 FUNCIONES Y RESPONSABILIDADES DEL COMITÉ.....113
4.1.4.3 FUNCIONES Y RESPONSABILIDADES DEL COORDINADOR 114
4.1.4.4 GRUPOS DE APOYO.....114
4.1.5 CENTROS DE OPERACIONES.....115
4.1.5.1 UBICACIONES 115
4.1.5.2 RECURSOS.....115
4.1.5.3 ADMINISTRACION Y LOGISTICA 116
4.1.6 PLAN DE MANTENIMIENTOS (EQUIPO INFORMATICO). 116
4.1.7 EVALUACION DE LA PROBLEMATICA.....117
4.1.7.1 PASO 1. 118
4.1.7.2 PASO 2. 118
4.1.7.3 PASO 3. 118
4.1.7.4 PASO 4. 119
4.1.7.5 PASO 5. 120
4.1.8 GUÍAS.....120
4.1.8.1 GENERAL.....120
4.1.8.1.1 GUÍA GENERAL PARA EJECUTIVOS Y JEFES DE DEPARTAMENTO. 121
4.1.8.1.2 CENTRO DE OPERACIONES. 121
4.1.8.1.3 COMUNICACIONES.....122
4.1.8.2 ESPECIFICAS 122
4.1.8.2.1 INCENDIOS 123
4.1.8.2.1.1 EN LOS ALREDEDORES DE LA UNIDAD.....123
4.1.8.2.1.2 EN LA UNIDAD 123
4.1.8.2.2 INUNDACIONES. 124
4.1.8.2.2.1 CON UNIDAD ABIERTA. 124
4.1.8.2.2.2 CON UNIDAD CERRADA. 125
4.1.8.2.3 TERREMOTOS.....125
4.1.8.2.3.1 CON UNIDAD ABIERTA. 125
4.1.8.2.3.2 CON UNIDAD CERRADA. 126
4.1.8.2.4. ERUPCIONES VOLCÁNICAS. 126
4.1.8.2.4.1. EN LOS ALREDEDORES DE LA UNIDAD.....126
4.1.8.2.4.2 EN LA UNIDAD 127
4.1.8.2.5 SUSPENSIÓN DE SERVICIOS.....128
4.1.8.2.5.1 ENERGÍA ELÉCTRICA. 128
4.1.8.2.5.2 COMUNICACIÓN DE DATOS. 128
4.1.8.2.6 DAÑO DE EQUIPO INFORMÁTICO.....129
4.1.8.2.7 VIOLACIÓN DE SEGURIDAD DE LA RED DE DATOS.....129

4.1.8.2.8 ASALTOS Y ROBOS DE EQUIPO INFORMÁTICO 130
4.1.9 PLANES DE CONTINGENCIA. 131
4.1.9.1 INCENDIOS 131
4.1.9.2 INUNDACIONES. 134
4.1.9.3 TERREMOTOS. 136
4.1.9.4 ERUPCIONES VOLCANICAS 139
4.1.9.5 SUSPENSIÓN DE SERVICIO 142
4.1.9.5.1 ENERGÍA ELÉCTRICA 142
4.1.9.5.2 COMUNICACIÓN DE DATOS 146
4.1.9.6 DAÑO DE EQUIPO INFORMATICO. 152
4.1.9.7 VIOLACION DE SEGURIDAD DE LA RED DE DATOS 156
4.1.9.8 ASALTOS Y ROBOS (EQUIPO INFORMÁTICO). 159
MANUAL DE PROCEDIMIENTO Y POLÍTICAS DE ADMINISTRACIÓN DE RED 162
4.2.1 INTRODUCCIÓN 163
4.2.2 OBJETIVOS 163
4.2.2.1 GENERAL 163
4.2.2.2 ESPECÍFICOS 164
4.2.3 ALCANCES 164
4.2.4 RESPONSABLES DE REVISIÓN DEL MANUAL 164
4.2.5 AREA ADMINISTRACIÓN DE RED 164
4.2.6 ALCANCES DE PROCEDIMIENTOS Y POLÍTICAS. 166
4.2.7 PROCEDIMIENTOS Y POLÍTICAS DE USUARIOS DEL DOMINIO. 166
4.2.7.1 PROCEDIMIENTO 167
4.2.7.1.1 SOLICITUD. 167
4.2.7.1.2 AUTORIZACIÓN. 167
4.2.7.1.3 CONFIGURACIÓN 167
4.2.7.2 POLÍTICAS CUENTAS DE USUARIO 168
4.2.7.3 POLÍTICAS CUENTAS DE CORREO ELECTRÓNICO 169
4.2.7.4 POLÍTICAS DEL PERSONAL DE INSTITUTO. 169
4.2.8 SERVICIOS 170
4.2.8.1 SERVICIO DE RED 171
4.2.8.2 SERVICIO DE SISTEMAS 171
4.2.8.3 SERVICIO DE CORREO ELECTRÓNICO 171
4.2.8.4 SERVICIO DE INTERNET 171
4.2.8.5 SERVICIO DE ANTIVIRUS 172
4.2.9 POLÍTICAS Y PROCEDIMIENTOS DE SERVICIOS TECNOLOGICOS 172
4.2.9.1 POLÍTICAS DE LOS SERVICIOS TECNOLOGICOS 172
4.2.9.1.1 SERVICIO DE RED 172

4.2.9.1.2 SERVICIO DE APLICACIONES Y/O SISTEMAS 173
4.2.9.1.3 SERVICIO DE CORREO ELECTRONICO 173
4.2.9.1.4 SERVICIOS DE NAVEGACIÓN INTERNET 175
4.2.9.1.5 SERVICIO DE ANTIVIRUS 176
4.2.9.1.6 PROCEDIMIENTO CONFIGURACIÓN DE SERVICIOS DE USUARIO 176
4.2.10 POLÍTICAS Y PROCEDIMIENTOS DE APLICACIONES (SOFTWARE) 176
4.2.10.1 POLÍTICAS DE APLICACIONES 177
4.2.10.2 PROCEDIMIENTO INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES 178
4.2.10.3 PROVEEDORES 178
4.2.10.3.1 POLÍTICAS 178
4.2.10.3.2 PROCESO ADQUISICIÓN DE SOFTWARE 179
4.2.11 POLÍTICAS Y PROCEDIMIENTOS DE HARDWARE 179
4.2.11.1 POLÍTICA GENERAL 179
4.2.11.2 POLÍTICAS 180
4.2.11.2.1 SERVIDOR BASE DE DATOS. 180
4.2.11.2.2 SERVIDOR DE WEB 180
4.2.11.2.3 SERVIDOR DE CORREO 181
4.2.12 POLÍTICAS Y PROCEDIMIENTOS DE MANTENIMIENTO 181
4.2.12.1 POLÍTICAS 181
4.2.12.2 PROCEDIMIENTOS 181
4.2.12.2.1 MANTENIMIENTO PREVENTIVO 181
4.2.12.2.2 MANTENIMIENTO CORRECTIVOS 182
4.2.13 POLÍTICAS Y PROCEDIMIENTOS DE COPIAS DE SEGURIDAD (BACKUPS) 182
4.2.13.1 POLITICAS 182
4.2.14 POLÍTICAS Y PROCEDIMIENTOS DE OFICINAS REGIONALES. 183
4.2.14.1 PROCEDIMIENTOS 184
4.2.14.2 POLITICAS 184
4.2.15 PROCESO DE DIVULGACION 185
RECOMENDACIONES. 186
CONCLUSIONES. 187
GLOSARIO 188
BIBLIOGRAFIA 192

.

CAPITULO I ANTECEDENTES

1.1 ANTECEDENTES DE ESTRATEGIA DE SEGURIDAD PREVENTIVA

La estrategia de la seguridad preventiva es una necesidad básica que fue reconocida desde los tiempos antiguos, teniendo como interés principal la prevención de la vida y las posesiones.

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). También la Biblia, Homero, Cicerón, Cesar han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno. Estos hechos nos hacen pensar en que la "Seguridad" dependía de las fortalezas que estos mostraran para enfrentar las diferentes circunstancias y a la ves para resolver los problemas que se ocasionaban al no estar preparados debidamente.

Las personas a través de la historia no solo han pensado en la seguridad principal, sino que además nos han mostrado que es importante estar preparados para cuando esta seguridad sea quebrantada por los diferentes invasores. Es así como se construían las diferentes edificaciones pensando en planes preventivos que permitieran tener estrategias de supervivencia, resolviendo con esto la ecuación de "luchar o huir". Los seres humanos aprendieron rápidamente que la mera existencia de medidas protectoras y de prevención, era frecuentemente suficiente para descorazonar a los adversarios con intenciones agresivas. Dolorosas experiencias enseñaron a los atacantes que buscaban penetrar las organizadas defensas que las pérdidas eran a menudo inaceptables y frecuentemente fueron disuadidos de nuevos ataques([1]).

Es así que con el tiempo la seguridad ha venido avanzando y evolucionando, permitiendo alcanzar objetivos específicos y a la vez constituyéndose en el punto central, en la búsqueda de la protección absoluta, entendiendo esto como la protección y prevención las propiedades y esencialmente de la vida.

.

AL definir el objetivo de la Seguridad Fayol dice: "…salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Es, generalmente hablando, todas las medidas para conferir la requerida paz y tranquilidad (Peace of Mind) al personal".

Las medidas de seguridad a las cuales se refería Fayol, solo se restringían a lo exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado.

Hoy, la seguridad y en especial la seguridad preventiva, desde el punto de vista legislativo, esta en manos de los políticos, es a estos a quienes les toca decidir sobre su importancia, los delitos en los que se pueden incurrir y los respectivos castigos, correspondientemente. También, hay otros factores importantes que mencionar como lo son la creación de la Instituciones que permitan crear las respectivas bases para la prevención, teniendo como objetivo fundamental estas el salvaguardar en primer lugar la vida humana y posteriormente lo material.

En cambio desde el punto de vista técnico, las estrategias de seguridad preventiva, están en manos de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientizacion respecto a la importancia de la información y el conocimiento en este nuevo mundo globalizado tecnológicamente.

1.2 PLANTEAMIENTO DEL PROBLEMA

EL desarrollo de un Plan de Contingencia, nace como resultado de las pláticas sostenidas con la empresa gubernamental dedicada al Fomento de Cooperativas, en las cuales se planteo la problemática que se encuentra en el área informática, específicamente en lo relacionado a la red de datos.

La empresa ha dedicado sus esfuerzos a poder mejorar el servicio hacia los clientes, tanto internos como externos, uno de estos servicios internos, es el poder brindar un funcionamiento constante en los recursos de la red de datos, solventando necesidades informáticas a dichos clientes. Es importante mencionar

.

que la Empresa se encuentra certificada ISO 9001:2000, por lo que se encuentra en la obligación de certificar los procesos y asegurar la calidad del servicio, lo que conlleva a la necesidad de desarrollar los Planes Contingenciales, donde se planteen cada uno de los procedimientos, que la empresa aplicaría a la hora de enfrentar las problemáticas dentro de la red de datos o también en el momento de estudiar la forma de cómo prevenir las posibles situaciones criticas.

En la empresa, existe una red de datos, por medio de la cual establecen relación con cada una de las Oficinas Regionales, las cuales están diseminadas en los departamentos de Santa Ana, San Vicente y San Miguel; entre las que intercambia diferentes tipos de información.

La empresa informa que ellos han tenido problema con la red de datos tanto en la parte de hardware como de software, y que dichos problemas se han resuelto después de haber dejado sin servicio a sus clientes internos por algún tiempo, afectando directamente a sus clientes externos a la hora de brindar los servicios. Además, se ha identificado que la red de datos de la empresa, ha sufrido ataques externos, violando en algunos casos la seguridad de la red de datos; dejando al descubierto información clave para la misma.

La falta de las políticas, procedimientos y procesos en el área de informática, en lo referente a la red de datos, permite que los usuarios puedan violar algunos niveles de seguridad necesarios para la prevención de futuras situaciones críticas, además de que deja al descubierto la documentación necesaria para brindar el servicio adecuado a los clientes externos.

1.3 JUSTIFICACIÓN E IMPORTANCIA

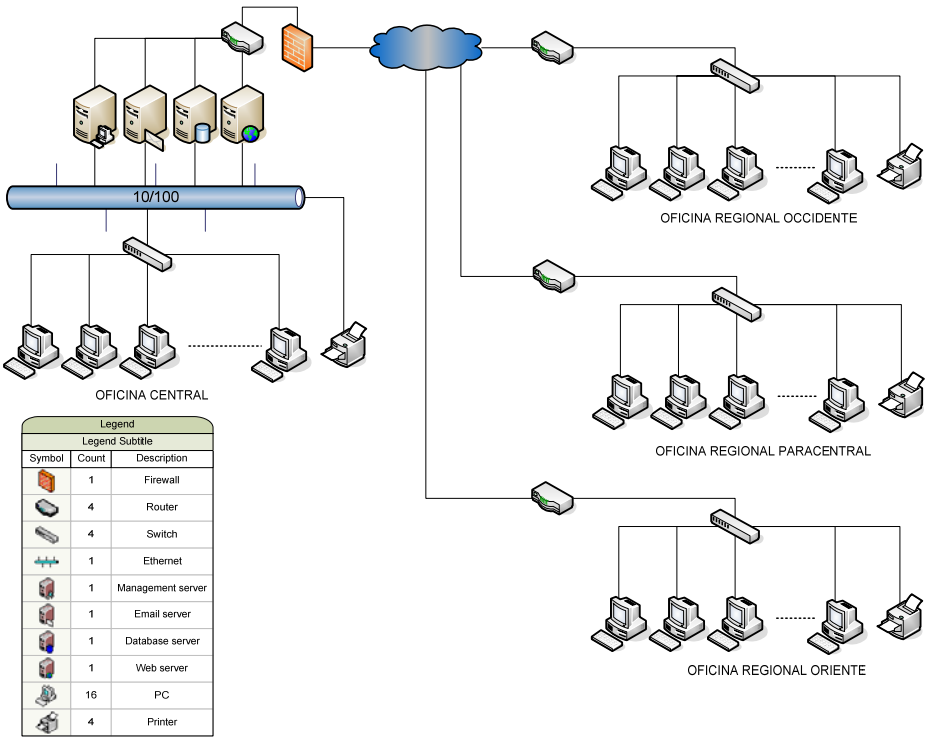
En cada una de las reuniones sostenidas entre el grupo de trabajo, el asesor y las personas responsables de la institución gubernamental en la parte de la Dirección Superior (Presidente y Vicepresidenta de la misma), como de la parte operativa (Administrador de la Red y Técnicos) se ha dejado claro, la necesidad de desarrollar un Plan Contingencial que permita a la Empresa asegurar la Red de Datos, contra el mal uso de los datos que viajan dentro de la misma, así como protegerla de personas externas a la misma, posibles errores de usuario o las fallas de los equipos. Además, el Presidente de dicha Institución, menciono que es un “requerimiento obligatorio”, que les exige la certificadora ISO 9001:2000, en

el momento de las auditorias de los procesos, para poder seguir manteniendo la certificación obtenida desde el año 2003.

También es importante resaltar que la empresa gubernamental se ha puesto en completa disposición para poder llevar a acabo el proyecto, ofreciendo de parte de la Dirección Superior como del personal técnico, el apoyo necesario en lo referente al tiempo y a otros factores que determinan la factibilidad del proyecto.

El beneficio que obtendrá la empresa no solo será el ordenamiento y desarrollo de una herramienta que les permita saber como actuar en diferentes problemáticas o a la ves prevenir con anticipación algunas de estas, sino que también se obtendrá un beneficio a nivel nacional, ya que esta, cuenta con las regionales diseminadas en tres zonas geográficas de nuestro país como los son la Zona Occidental, Paracentral y Oriental. Los beneficiarios se estiman que son a nivel nacional, según el último censo (con fecha, septiembre de 2005) realizado por la empresa, un total de 456,789 personas asociadas al Cooperativismo Salvadoreño.
El diagrama que a continuación se describe permite observar el entorno de la red de datos y el ámbito de acción de un Plan de seguridad.

Figura 01 -Descripción Gráfica de la Red



.

El diagrama anterior es una muestra grafica de la forma en que funciona la red institucional. La cantidad y los tipos de equipos son los siguientes:

a)	FIREWALL	1
b)	ROUTER	4
c)	SWICHT	4
d)	SERVIDOR	1
e)	CPU	39
f)	TECLADO	39
g)	MONITOR	39
h)	MOUSE	39
i)	UPS	39
j)	IMPRESOR	20
k)	PARLANTES	26
l)	LAPTOP	5
m)	ESCANNER	1
n)	CAÑON	2

Los programas que se encuentran instalados en las maquinas son los siguientes:

1. Sistemas Operativos
    a. Windows NT 4.0 (Servidor)
    b. Windows 98
    c. Windows 2000
    d. Windows XP
2. Manejadores de Texto
    a. Office 2000
    b. Office 2003
    c. Office XP
3. Antivirus
    a. Norton Antivirus 2000
    b. Norton Antivirus Administrable Ver. 10

.

Estos equipos reciben su mantenimiento preventivo y correctivo, según el siguiente cronograma, el cual es creado por la institución y entregado a la empresa externa que realiza dicha actividad, la cual es contratada anualmente por la institución.

Mantenimientos:

Oficina Occidental	Oficina Central	Oficina Paracentral	Oficina Oriental
Marzo	Marzo	Marzo	Marzo
Junio	Junio	Junio	Junio
Septiembre	Septiembre	Septiembre	Septiembre
Diciembre	Diciembre	Diciembre	Diciembre

Cada una de las fechas en las que se realizan las visitas a las Oficinas son coordinadas por el Departamento de Informática y la Empresa contratada, además de los Jefes de las oficinas regionales, según sea el caso.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

- Desarrollar una propuesta de un Plan Contingencial que permita el manejo de los recursos de red de una forma eficiente y eficaz, y que a la vez permita reestablecer los servicios de red implementados, por la Institución objeto del estudio, ante ciertos hechos o sucesos que interfieran con el desarrollo normal de los mismos, y poder continuar proporcionando a sus clientes los beneficios de dichos servicios.

1.4.2 OBJETIVOS ESPECIFICOS

- Presentar las diferentes áreas que conforman el Plan de Contingencia así como los servicios que ofrece cada una de las mismas, basados en los requerimientos de la Empresa y las Normas ISO 9001:2000.

.

- Elaborar un Plan Contingencial, en su contexto de plan de seguridad que contenga políticas de seguridad que permita a la empresa mejorar los servicios de la red de datos a sus clientes internos a nivel nacional, resolviendo y previniendo los problemas que se presenten.
- Elaborar un documento donde se presentara el Plan Contingencial, conteniendo las investigaciones realizadas en la Institución, con las áreas de Informática y Unidad de Calidad; además de aquellas en lo referente a los procedimientos y políticas creadas para la Institución

1.5 ALCANCES Y LIMITACIONES

1.5.1 ALCANCES

- Se analizara y diseñara un documento en el cual se desarrollara el Plan Contingencial para la empresa gubernamental, basado en los requerimientos y necesidades de la misma. Este Plan Contingencial estará conformado por un conjunto de políticas y/o medidas de seguridad, así como los procesos para el restablecimiento de los servicios claves que presta la institución.
- Dichas políticas se elaboraran en el desarrollo del proyecto de tesis y serán definidas en base a las Normas de Calidad ISO 9001:2000, presentándose posteriormente a departamento de Informática.
- El Plan Contingencial, contendrá el análisis de los servicios y áreas de la empresa, diseño de las políticas de seguridad y la propuesta de implementación del mismo.

1.5.2 LIMITACIONES

- La disponibilida de los recursos materiales y financieros, para trasladarse a las diferentes oficinas que conforman la oficina gubernamental, objeto del estudio.
- La disponibilidad de tiempo de las personas que están a cargo y que forman parte de dichas áreas, a la hora de hacer la investigación de campo.

.

- La falta de documentacion de los servicios y los procesos instalados, para los usuarios que seran parte de la propuesta final de solución.

CAPITULO II. MARCO TEÓRICO

Para comenzar a hablar un poco de lo que es el Plan Contingencial que se pretende desarrollar hay que hablar de lo que es seguridad, administración de los recursos tecnológicos, todo lo que sea relacionado a seguridad de información.

En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas. Esto puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Para hablar de seguridad informática hay que hablar de Seguridad que se puede definir como “calidad de seguro” y seguro está definido como “libre de riesgo”. Información: es “acción y efecto de informar”. Informar: es “dar noticia de una cosa”. Redes: es el conjunto sistemático de tuberías o de hilos conductores o de vías de comunicación o de agencias y servicios o recursos para determinado fin. Uniendo todas estas definiciones, podemos establecer qué se entiende por

.

Seguridad en redes. Seguridad en Redes: es mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin.

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Al tratar de implementar políticas de seguridad también se debe de hablar del impacto que esta generará en la organización, para ser más específicos en su funcionalidad.

En realidad, la implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativa.

Por ejemplo, la disminución de la funcionalidad o el decremento de la operatividad tal vez sea uno de los mayores problemas. Esto se puede aclarar de la siguiente manera: en un primer momento, el usuario, para acceder a tal recurso, debía realizar un solo usuario. Ahora, con la implementación del nuevo esquema de seguridad, debe realizar dos usuarios: uno para ingresar al sistema y otro para acceder al recurso. El usuario visualiza esto como un nuevo impedimento en su tarea, en lugar de verlo como una razón de seguridad para él, pues de esta manera, se puede controlar más el uso del recurso y, ante algún problema, será mucho más fácil establecer responsabilidades. Por otro lado, al poner en funcionamiento una nueva norma de seguridad, ésta traerá una nueva tarea para la parte técnica (por ejemplo, cambiar los derechos a algo de algunos usuarios) y administrativamente, se les deberá avisar por medio de una nota de los cambios realizados y en qué les afectará.

La implementación de medidas de seguridad, es un proceso técnico administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por los departamentos, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria. Hay que tener muy en cuenta la complejidad que suma a la operatoria de la organización la

.

implementación de estas medidas. Será necesario sopesar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

2.1 PLAN CONTINGENCIAL

2.1.1 PLAN DE RECUPERACIÓN DEL NEGOCIO EN CASO DE CONTINGENCIAS.

A medida que las empresas se han vuelto cada vez más dependientes de las redes de datos, para manejar sus actividades, la disponibilidad de estos se ha vuelto crucial.

En caso de un desastre, la interrupción prolongada de los servicios puede llevar a pérdidas de clientes en gran medida, sobre todo si está implicada la responsabilidad del responsable de la red de datos o de los usuarios de los distintos departamentos.

Si bien es importante el establecer los respetivos seguros de cada uno de los activos de la Empresa, esto no ayudara a la empresa a conservar los clientes y podría derivar, en el peor de los casos, en el fracaso total de la empresa.

Por lo tanto, la capacidad para recuperarse exitosamente de los efectos de un desastre dentro de un periodo predeterminado debe ser un elemento crucial en un plan estratégico de seguridad para una organización.

Trate de pensar una situación que interrumpa las operaciones de la red de datos durante una semana o un mes; imaginémonos la pérdida de todos los datos de la empresa, todas las unidades de respaldo y la destrucción de equipos vitales para el funcionamiento de la red; la pregunta que nos haríamos, seria en ese momento ¿Cómo se manejaría semejante desastre?.

Para ello se necesita también conocer en profundidad lo que es un desastre. Se puede considerar como un desastre la interrupción prolongada de los recursos de red de la organización, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para

.

su recuperación. Ejemplos obvios son los grandes incendios, las inundaciones, los terremotos, las explosiones, los actos de sabotaje, etcétera.

La recuperación de las actividades ante un desastre puede ser una de las situaciones más difíciles con las que una organización deba enfrentarse. Tras un desastre, es probable que no haya posibilidades de regresar al lugar de trabajo o que no se disponga de ninguna de los recursos acostumbrados. Incluso, es posible que no se pueda contar con todo el personal. La preparación es la clave del éxito para enfrentar los problemas. No existe ninguna manera costeable para protegerse completamente contra todo tipo de riesgos, particularmente amenazas naturales a gran escala que pueden arrasar zonas extensas.

Un plan de contingencia es el proceso de determinar qué hacer si una catástrofe se abate sobre la empresa y es necesario recuperar la red de datos.

2.2 SEGURIDAD INFORMATICA

2.2.1 ANÁLISIS DEL OBJETIVO DE SEGURIDAD INFORMÁTICA

En principio, es importante desarrollar el analisis de la Seguridad Informatica, conociendo a la ves las caracteristicas de lo que se pretende proteger: “La Informacion”. Es asi como podemos definir “Dato”, como la unidad minima con la que se compone sierta informacion.

La Informacion se define como una agregacion de datos que tiene un significado especifico mas alla de cada uno de estos[2], y tendrán un sentido particular según como y quien la procese.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

.

“EL objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad, Control y autenticidad de la información manejada por computadora”.

Contrario a todo este concepto no es nuevo, y nace con los grandes centros de cómputo. Con el pasar de los años, y como se sabe, las redes de datos pasaron de ser algo exclusivo, a una necesidad dentro de cada una de las empresas a nivel mundial así como también dentro de los hogares. Con esto de dio inicio a una de las guerra interminables, la cual es entre la seguridad de las redes versus los intrusos o fallas de la misma.

Por lo que también cabe la pregunta ¿Qué es un intruso?; Intruso se le llama a la persona que accede o intenta acceder sin autorización a una red de datos, ya sea que lo haga de forma intencional o por accidente.

Luego, de que la seguridad falla, tendremos como resultado el daño, resultado de la no-acción o la acción defectuosa del establecimiento de políticas y procedimientos. Este se da también cuando no se ha identificado adecuadamente las posibles amenazas, derivándose las responsabilidades para los encargados de cada una de las partes. Por lo que es importante detectar cada una de las vulnerabilidades de la red de datos que pueden ser explotadas y empleada por las distintas amenazas.

Con lo anterior se podría definir las características mas importantes que una red de datos deberá tener como lo son Integridad, Operatividad, Privacidad, Control y Autenticidad.

1. La **Integridad** es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles.
2. La **disponibilidad u Operatividad** es la capacidad de estar siempre disponible para ser usada por las personas autorizadas.
3. La **Privacidad** es la necesidad de que la misma red de datos solo sea conocida y utilizada por personas con la autorización requerida.

.

4. EL **Control** permite asegurar que solo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la red de datos.
5. La **Autenticidad** permite definir lo que es valido y utilizable en tiempo, forma y distribución. Esta propiedad permite asegurar el origen de la información, validando al emisor de la misma, para evitar cualquier amenaza.

Comprender cada uno de estos conceptos ayudara a llevar acabo el análisis respectivo de la seguridad informática, además de permitir concluir en las ventajas y desventajas de la situación, a decidir medidas técnicas y metodologías, físicas e informáticas, en base de las necesidades de seguridad.

Finalmente, es importante remarcar que la premisa esencial que hay que considerar es que no existe el 100% de seguridad esperado o deseable en estas circunstancias.

2.3 AMENAZAS

Es necesario empezar definiendo los tipos de amenzas que podemos encontrar en el dia a dia de la empresa. Estas las podriamos clasificar en:

- Amenzas Humanas. Son aquellas a las cuales la red esta expuesta por parte de los usuarios de la misma, estos podrian ser errores u omisiones y actos intencionales.
- Desastres Naturales. Estos son los incendios, terremotos, inundaciones, seguias, granizo y erupciones.

Es por esto que generalmente los encargados de las redes de datos buscan en primer lugar cuales son las medidas defensivas, ya que de estas dependera totalmente las soluciones que se puedan proporcionar, y especialmente el tiempo en el cual se respondera.

.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo. Estos mecanismos conformaran políticas que garantizaran la seguridad de nuestra red de datos.

- La prevención (antes): mecanismos que aumentan la seguridad (o fiabilidad) de una red de datos durante su funcionamiento normal.
- La detección (durante): mecanismos o procedimientos orientados a revelar violaciones a la seguridad.
- La recuperación (después): mecanismos que se aplican, cuando la violación de la red de datos se ha detectado, para retornar a esta a su funcionamiento normal.

2.3.1 AMENAZAS NATURALES

2.3.1.1 PRESENTACIÓN

Es importante que cada red de datos es unica y por lo tanto la politica de seguridad a implementar no sera unica. Este concepto vale tambien, para el edificio en el que se encuentra la organización. Este tipo de seguridad esta enfocado en cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio fisico en que se encuentra ubicada la organización.

Cada una de estas amenazas no pueden ser prevenidas en tiempo por el hombre, por lo que el punto central son las medidas de seguridad que se puedan tomar antes de los eventos, estableciendo procedimientos por medio de los cuales se pueda tener claro el como actuar de la organización y de los empleados de la misma.

A continuacion se analizan los peligros mas importantes que se corren al tener fisicamente una red de datos; con el objetivo de identificar las acciones a seguir en forma eficaz y oportuna para la prevencion, recuccion, recuperacion y correccion de los diferentes tipos de riesgos.

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catastrofes sismicas similares. Las condiciones atmosfericas severas se

.

asician a ciertas partes del mundo y la probabilidad de que ocurran esta documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir el lugar fisico donde se encuentre la organización. La comprobacion de los informes climatologicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la iluminacion.

2.3.1.2 TERREMOTOS

Estos fenomenos sismicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o por el contrario ta intensos que causen la destruccion de edificios y hasta la perdida de vidas humanas. El problema es que en la actualidad estos fenomenos estan ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

La preparacion para este tipo de fenomenos dentro de la red de datos es similar a la preparacion que se hace con las llamadas rutas de evacuacion de cada una de las instalaciones de los edificios; ya que de la misma forma es importante diseñar el camino que se seguira en el caso que ocurriese una terremoto de pequeña escala, o uno que pueda causar el daño total de todas las instalaciones de la red de datos como de la organización misma.

2.3.1.3 INTENSIDAD Y MAGNITUD DE LOS TERREMOTOS

Los terremotos pode mos clasificarlos de acuerdo a su origen, en naturale y artificiales.

Los naturales son los que en general liberan mas su energia, por lo que sus efectos en la superficie son mayores. Estos a su ves pueden clasificarse en:

.

1. **Tectonicos**: Producidos por la interaccion de dos placas tectonicas; se definen en dos clases, los de interplaca, ocasionados por una frccion en las zonas de contacto entre placas. Un tipo particular de estos terremotos son los llamados locales, que son producto de deformaciones de los materiales terrestres devido a la concentracion de fuerzas en una region limitada. Y los intraplaca, que se presentan lejos de los limites de placas conocidas, son mucho menos frecuentes que los interplaca y generalmente de menor magnitud.
2. **Volcanicos:** Acompañan a las erupciones volcanicas, son generados principalmente por la ruptura de rocas debido al movimiento de magma, generalmente no llegan a ser tan grandes como los anteriores.
3. **De Colapso:** Producidos por derrumbamiento del techo de las cavernas y minas; por lo genral ocurren cerca de la superficie y se perciben en areas reducidas.

Los Terremotos artificiales son los producidos por el hombre por medio de explosiones convencionales o nucleares, con dines de exploracion, investigacion o explotacion de bancos materiales para su industria.

Los efectos de los terremotos se podrian dividir de la siguiente forma:

1. **Humanos:** Perdida de vidas o lesiones, causadas por derrumbes de constrcciones, incendios y explosiones entre otros.
2. **Materiales:** La cimentacion de edificios se desestabiliza, las estructuras sufren fuerzas de corte u de tension que causan agrietamientos o derrumbes de la construccion. Ademas del daño que puede ocurrir a los diferentes componentes que conforman el equipo de la organización.
3. **Sociales**: Afectan los servicios publicos de agua potable, energia electrica, transporte y comunicación.

Las acciones que se desarrollen seran en razon de la intensidad y la magnitud con que se presente el desastre. Debiendose entender por magnitud, la medida de la fuerza o potencia de una calamidad con base en la energia liberada. En el caso de los terremotos, esa energia generalmente se mide por la escala de Richter. Por intensidad deberan entenderse, el grado de energia de un agente

.

natural o mecanico. La escala mas comun para medir la intensidad de un terremoto es la de Mercalli Modificada (MM).

Es importante mencionar que en cualquiera de todos lo casos anteriores lo principal sera la comunicación que exista entre los diferentes departamentos de la organización, ademas de mantener la informados adecuadamente a cada uno de los que componen la misma, ya sea para salvaguardar la vida o para los procedimientos que se seguiran antes, durante y despues, con la red de datos de la organización.

Figura 02 – Descripción de la Escala de Mercalli

Figura 03 - Descripción de Magnitud en la Escala de Ritcher

MAGNITUD	EFECTOS
Menos de 3.5	Generalmente no se siente, pero es registrado.
De 3.5 A 5.4	A menudo se siente, pero solo causa daños menores.
De 5.5 A 6.0	Ocasiona daños ligeros a edificios.

.

De 6.1 A 6.9	Puede ocasionar daños severos en areas donde vive mucha gente.
De 7.0 A 7.9	Terremoto mayor. Causa Graves daños.
De 8.0 A mayor	Gran terremoto. Destruccion total a comunidades cercanas.

2.3.1.4 ERUPCIONES VOLCÁNICAS

Las erupciones volcanicas o vulcanismo es un conjunto de fenomenos y procesos relacionados con la emision de magma a traves de los volcanes. Un volcan es la abertura en la litosfera por la cual el magma alcanza la superficie.

Los materiales rocosos emitidos por un volcan pueden ser fragmentos de rocas “viejitas” o “nuevas” que conforman la corteza o estructura del mismo; las rocas nuevas pueden ser arrojadas por el volcan e estado solido o fundidas; la fusion de la roca preexistente forma, en las profundidades de la tierra, una mas fundida de composicion principalmente silicia con abundantes elementos metalicos a la cual se le da el nombre de magma. Este puede cristalizarse en el interior del volcan o bien aflorar a la superficie a traves de la actividad volcanica; cuando esto sucede se le denomina lava; y recien emitidas alcanzan temperaturas entre los 700 grados y 1200 grados centigrados, dependiendo de s composicion quimica. El magma, antes de emerger en una erupcion se acumula bajo el volcan en una camara maganetica.

A la emision de material rocoso y gases a altas temperaturas, es a lo que se denomina erupcion volcanica, estas puden resultar tambien, como efecto de calentamiento de cuerpos de agua por magma o gases magmaticos, Cuando el cuerpo de agua es subterraneo, la erupcion se denomina freatica, y generalmente expulsa fragmentos de roca solida “vieja”, producidas por las explosiones de vapor. Cuando la erupcion emite ademas productos magmaticos mezclados con los de erupcion de vapor, se denimina fratomagmatica. Comunmente despues de una gran erupcion de esta naturaleza comienza a depositarse una lava muy viscosa en el fondo del crater por la chimenea volcanica formando una cupula a la que se llama domo, el cual puede crecer hasta cubrir por completo al crater.

.

Los fragmentos rocosos de forma solida o liquida causados por una erupcion se denominan piroclasticos o tefra los cuales al depositarse en el suelo pueden cementarse por diversos procesos, tales como solidificacion por enfriamiento si venian fundidos, o por efectos del agua. Los piroclasticos cementados forman las rocas piroclasticas, a los fragmentos tefra de menor tamaño se les llama ceniza y a los demas grandes lapill, el tamaño de los fragmentos depende del tipo de materal expulsado, fuerza e identidad de la erupcion explosiva.

Estas erupciones pueden producir densas columnas de tefra que ocasionalmente penetran la estratosfera y alcanza alturas superiores a los 20 Kms., estas columnas se les denominan columnas eruptivas.

2.3.1.5 CLASIFICACION DE LOS VOLCANES

Los volcanes han sido clasificados atendiendo su actividad o a su estructura o composicion de su edificio. En base a la actividad registrada se clasifican en extintos y activos; los volcanes extintos, son los que no han tenido erupciones conocidas (hasta 50,000 años atrás); y los activos, son los que demuestran una o varias etapas de actividad, y se les denominan monogeneticos (una actividad) y poligeneticos (varias actividades).

Por su estructura y composicion de su edificio, los volcanes se clasidican en estratovolcanes, conos cinerticos y volcanes en escudo. Los Estratovolcanes, son los formados por capas de material fragmentario y corrientes de lavas intercaladasm surgidas en espocas de actividad explosivas, seguidas de otras donde arrojaron corrietes de lava fluida; los conos cinerticos (de cenizas) se forman por el acumulamiento de cenizas durante las erupciones basalticas, en las que predominan los materiales calientes solidificados en el aire, y que caen en las proximidades del centro de emision. Sus paredes son de pendientes no muy altas (entre 30 y 40 grados), son de forma conica, base circular, y exceden los 300 metros de altura, y los Volcanes de escudo, son aquellos cuyo diametro es mucho mayor que su altura, se foma por la acumulacion sucesiva de corrientes de lava

.

muy fluida; por lo que son de poca altura y pendiente ligera; su topografí a es suave y su cima forma una planicie ligeramente encorvada.

2.3.1.6 CLASIFICACIÓN DE LAS ERUPCIONES

Las erupciones han sido catalogadas de acuerdo a sus características; una de las más tradicionales es la que utiliza los nombres de los volcanes que en su actividad manifestaron particularidades que le permiten distinguirla de otras; así se clasifican en Hawaiana, Estromboliana, Vulcaniana, Paleeana, Pliniana, Ultrapliniana, Flujos Riolíticos.

Por los estilos de erupción, pueden clasificarse en tres grupos, erupciones efusivas, si consiste esencialmente en la emisión sin violencia de lava y gases, erupciones explosivas, cuando los materiales son arrojados violentamente, y erupciones mixtas, son las que presentan características de las dos anteriores.

2.3.1.7 VIGILANCIA Y PREVISIÓN DE LAS ERUPCIONES

En la actualidad los Gobiernos de todo el mundo han destinado recursos importante para la prevencion de este tipo de desastres, lo cual incluye a muchos entes educativos y otros que buscan los mismos objetivos de prenvencion. En este sentido se hace posible la vigilancia de todos los volcanes, en especial aquellos que se denominan como activos.

Es por ello, que cada una de estas instituciones esta creando planes de contigencia para poder salvaguardar en especial la vida humana, ademas de recuros materiales como naturales (la fauna y flora).

Si bien estos factores son de naturaleza imprevistos, las tecnologias actuales nos dan ana pequeña ventaja a la hora de la prevencion, podiendo evaluar las distintas posibilidades de fechas, horas y lugares en los cuales afectara la erupcion, ademas de poder medir los efectos secundarios y los materiales por los cuales estaria formada la erupcion.

.

2.3.1.8 EFECTO DE LAS ERUPCIONES EN EL MEDIO NATURAL

Las erupciones volcánicas pueden traer como consecuencia otras calamidades, como:

a) Flujos de lava. Lenguas o coladas de lava que pueden ser emitidas desde el cráter superior, algún cráter secundario, desde una fisura en el suelo o sobre los flancos de un volcán, impulsados por la gravedad; estos flujos se distribuyen sobre la superficie, según la topografía del terreno, a una velocidad que varían comúnmente entre los 5 a 1000 M/H, alcanzando excepcionalmente, velocidades de 30 hasta 60 Km/H.

   El riesgo asociado a las manifestaciones de lava, esta directamente ligado a la temperatura y composición de la lava, a las pendientes del terreno y a la distribución de la población. El efecto destructivo en los edificios se debe principalmente al peso de los materiales piro clásticos (arena, ceniza, lapilli, etc.), y a la presión dinámica que pueda ejercer lateralmente sobre el mismo.

b) Flujos Piro clásticos.- Flujo compuesto por fragmentos magmáticos y gases. Una mezcla de partículas sólidas o fundidas y gases a alta temperatura puede comportarse como líquido de gran movilidad y poder destructivo, alcanzando en ocasiones hasta 600 Kms/H a temperaturas que oscilan entre los 150 y 300 grados centígrados. A ciertos tipos de flujo piro clásticos se les denomina nuees ardentes (nubes ardientes).

   Comúnmente se clasifican de acuerdo a la naturaleza de su origen y a las características de los depósitos que se forman cuando el material volcánico flotante en los gases calientes se precipitan al suelo, así pues son flujos piro clásticos activos los que se producen durante una erupción, y flujos, sin calificativos, es el depósito.

   El poder destructivo de los flujos piro clásticos depende fundamentalmente de sus volúmenes y de sus alcances; el primer factor esta determinado por

.

el tipo de erupción que los produce y el segundo por la topografía del terreno. En base al tipo de erupción se distinguen tres clases de flujos, los flujos relacionados con domos o con el desbordamiento de los frentes de lava; flujos producidos directamente en cráteres de cumbre y flujos descargados desde fisuras.

c) Lahares o flujos de lodos. Son flujos que generalmente acompañan a una erupción volcánica; contienen fragmentos de roca volcánica, producto de la erosión de las pendientes de un volcán. Estos se mueven pendiente abajo y pueden incorporar suficiente agua, de tal manera que forman un flujo de lodo.

   La velocidad y alcance de estos flujos depende de la topografía del lugar y sus velocidades están determinadas por las pendientes, por la forma de los causes, por la relación sólidos agua y por el volumen de las mismas. Las velocidades más altas son la que se alcanzan sobre las pendientes de los volcanes, registrándose en sus flancos una velocidad mayor a los 165 Km/H (volcán Monte Santa Elena, 18 de mayo de 1980).

d) Materiales aéreos y Ceniza de caída libre.- La ceniza volcánica, que se deposita al caer lentamente desde las alturas considerables, consistente de fragmentos piro clásticos muy pequeños de material juvenil; esto es, el producto de la fragmentación extrema de lava fresca. Se denomina de caída libre, y generalmente tiene un diámetro entre 1/16 mm. La ceniza fina es aquella que tiene un diámetro menor de 1/16 mm. En ocasiones, cuando el magma contiene numerosos cristales, los sólidos se separan del líquido para formar ceniza cristalizada.

   Durante una erupción los fragmentos más grandes y densos de la columna eruptiva quedan en la parte baja, la parte superior de la columna es arrastrada por el viento depositando, en su trayectoria, su contenido de ceniza, la que posee cierto grado de peligrosidad por los daños que causa al acumularse en techos, vías de comunicación, servicios públicos, campos de cultivo y ganaderos afectando a la ecología.

.

e) Avalancha de detritos.- Los detritos son los materiales rocosos que se forman al fracturarse parte del edificio volcánico, provocando avalanchas de rocas. El riesgo que estos representan es semejante al de flujos piroclastos aunque su alcance puede ser menor.

f) Incendios.-Son ocasionados por la lluvia de cenizas y las oleadas de piroclastos, cuando las temperaturas de los materiales emitidos son lo suficientemente altas y se acumulan en áreas de bosques, pastizales, vegetación o construcciones flamables.

g) Gases y lluvias ácidas.- Los magmas contienen gases en solución que son liberados durante y entre erupciones, estos se forman por vapores de agua y varios compuestos de cloro, flúor, hidrógeno y nitrógeno.

   Así también, monóxido de carbono, venenoso e inodoro; bióxido de carbono, no venenoso pero diluye el oxígeno provoca asfixia, es más pesado que el aire y puede fluir pendiente abajo, concentrándose en depresiones, es inodoro; bióxido y trióxido de azufre, gases tóxicos detectables por su olor irritante.

h) Otros fenómenos.- como efectos secundarios asociados a una actividad volcánica se encuentran los terremotos, las deformaciones del terreno, las ondas de choque y la ocurrencia de daños.

La magnitud o efecto general de las erupciones dependera directamente de la clase de volcan que sea y el tipo de erupcion, ademas hay que tomar en cuenta cada uno de los factores geologicos de los suelos.

2.3.1.9 INUNDACIONES

En primer lugar hay que tocar el tema de las lluvias, en especial aquellas a las que podemos llamar intensas, las cuales son fenómenos atmosféricos producidos

.

por la condensación de las nubes. Consiste en la precipitación de gotas de agua líquida o sobré enfriada, cuyo diámetro es mayor a los 0.5 milímetros.

Las lluvias intensas producen un alto riesgo de inundación pluvial, y si existen montañas, la lluvia puede alcanzar valores extremos. Las fuertes precipitaciones pluviales que están asociadas a los huracanes, dependen de la prontitud con que este viaja, de su radio de acción y del área formada por nubes convectivas cumulonimbus.

La medición y registro de la precipitación pluvial y de la intensidad de la lluvia se efectúa con pluviómetros (recipiente graduado en milímetros en el que se mide la lluvia acumulada en un día) o pluviógrafos (dotado de un reloj que hace girar un cilindro con una hoja de papel en la que de manera continua se registra la altura de lluvia que se está acumulando. Determina la intensidad de lluvia en milímetros por hora).

Debido a la diversidad de los factores geográficos que afectan el territorio salvadoreño, este recibe varios tipos de lluvias y de cantidad variable, lo que hace necesario se implemente una estrategia de acciones de coordinación, que permitan suplir las deficiencias naturales, materiales y humanas, así como prever la magnitud de sus efectos, y responder oportuna y eficientemente, ante la presencia de contingencias de esta naturaleza.

Las inundaciones entonces, son el efecto generado por el flujo de una corriente, cuando sobrepasa las condiciones que le son normales y alcanza niveles extraordinarios que no pueden ser controlados en los vasos naturales o artificiales que la contienen, lo cual deriva, ordinariamente en daños que el agua desbordada ocasiona en zonas urbanas, tierras productivas y, en general en valles y sitios bajos.

Atendiendo a los lugares donde se producen, las inundaciones pueden ser: costeras, fluviales, lacustres y pluviales, según se registren en las costas marítimas, en las zonas aledañas a los márgenes de los ríos y lagos, en los

.

terrenos de topografía plana, a causa de la lluvia excesiva y a la inexistencia o defecto del sistema de drenaje, respectivamente.

Las inundaciones han sido clasificadas por su origen en; Pluviales, son aquellas que se deben a la acumulación de la precipitación (lluvia y granizo), que se concentra en terrenos de topografía plana o en zonas urbanas con insuficiencia o carencia de drenajes; Fluviales, se originan cuando los escurrimientos superficiales son mayores a la capacidad de conducción de los cauces; y Lacustres, se originan en los lagos y lagunas por el incremento de sus niveles y son peligrosos por el riesgo que representa para los asentamientos humanos cercanos a las áreas de embalse.

Las causas generalmente de las inundaciones son consecuencia directa de los fenómenos Hidrometeoro lógicos al combinarse los mecanismos productores de la precipitación; en ocasiones las inundaciones son inducidas con fines técnicos y de beneficio económico-social; como ejemplo podemos señalar las inundaciones inducidas en área no productivas para evitar o disminuir los daños en centros de alto desarrollo urbano, industrial o agropecuario.

Podemos citar como causas generadoras de inundaciones, las lluvias intensas, los ciclones tropicales, las trombas o tornados, granizo o presas.

2.3.1.9.1 TIPOS DE DAÑOS CAUSADOS POR INUNDACIONES

Por la forma en que inciden en los sistemas afectables, se clasifican en directos, cuando causan un menoscabo físico de las propiedades y de la producción, las actividades y bienes que en mayor medida pueden ser afectados por este tipo de daños son la agricultura, la ganadería, la industria, el comercio, las obras públicas y las construcciones; indirectos, son las pérdidas económicas de los productos y servicios de una región derivadas de la interrupción temporal de las actividades agropecuarias, forestales, industriales y de comercio, así como el gasto que se destina a ayudar a los damnificados; e intangibles, en este reglón se cuadra a los damnificados, heridos y las pérdidas de vidas humanas.

.

La afectabilidad de los fenómenos naturales que periódicamente azotan nuestro País, frecuentemente los Hidrometeoro lógicos son los que más daños causan, al originar inundaciones de diversas magnitudes y duración, aún en áreas donde no parecería factible, a ello se suman efectos orográficos y fenómenos meteorológicos convectivos (ascenso de humedad debido a diferencia de temperatura), que favorecen la ocurrencia de lluvias, esta diversidad de fenómenos produce la precipitación, con una secuela de avenidas que pueden generar desbordamiento de cauces e inundación de terrenos.

En razón de que las inundaciones no solamente dañan propiedades y ponen en peligro vidas humanas y de animales, sino que pueden producir escurrimientos rápidos que originen otros fenómenos como la erosión del suelo y el depósito de sedimentos, es indispensable emprender acciones coordinadas de protección, atendiendo a la intensidad con la que se presente y el riesgo que esta represente.

Ademas de las causas naturales de inundaciones, puede existir la posibilidad de una inundacion provocada por la necesidad de apagar un incendio en cualquier lugar fisico dentro de la organización.

Para evitar estos inconvenientes, una de las medidas que se puede tomar es la siguiente: construir la red en sitios altos dentro de la organización.

2.3.1.10 INCENDIOS

Por su magnitud y destructividad los incendios se pueden clasificar en:

a) Conato.- inicio de un incendio que se puede apagar utilizando extintores comunes.
b) Incendio.- Fuego no controlado de grandes proporciones, que pude presentarse en forma súbita, gradual o instantánea y requiere para su eliminación o control, de hidrantes, mangueras y extintores de carros. Sus efectos destructivos alcanzan hasta un 25% del sistema afectable.
c) Conflagración.- Incendio que destruye significativa o totalmente un inmueble (del 26 al 100%).

.

Se han establecido cuatro clases de fuego según las propiedades de combustión de los materiales, la forma en que se desarrolla el fuego y las técnicas de combate que se emplean.

a) Fuego tipo “A”.- Fuego que se produce en materiales sólidos tales como madera, estopa, papel, cartón, telas, basura, etc., se caracteriza porque al arder forma brazas y cenizas y se propaga de afuera hacia adentro. Para apagarlo se emplea de preferencia el enfriamiento con agua.
b) Fuego tipo “B”.- Se produce en combustible líquido, derivados del petróleo y flamables como: gasolina, diesel, alcohol, tiner, lubricantes y grasa; de estos líquidos lo que arde son vapores, por lo que para apagar el fuego se emplean métodos de eliminación de oxígeno por medio de productos químicos o espumas sufocantes. El empleo de agua en forma de chorro no extingue el fuego, más bien alienta su propagación; en cambio la aplicación de agua a presión en forma de rocío, ayuda para extinguirlo.
c) Fuego tipo “C”.- Se produce en equipo y maquinaria que funciona por medio de electricidad como motores, alternadores, generadores, sub-estaciones, maquinaria de soldar, etc., para extinguirlos es necesario cortar la corriente eléctrica y utilizar extintores de polvo químico (universal), de bióxido de carbono.
d) Fuego tipo “D”.- Se produce en cierto tipo de materiales combustibles como: magnesio, titanio, sodio, litio, potasio, aluminio, o zinc en polvo, entre otros. No se recomienda usar extintores comunes pues existe el peligro de aumentar el fuego por reacciones químicas entre el agente extintor y el metal ardiente.

Los metales más peligrosos son el magnesio, el sodio y el potasio ya que generan su propio oxígeno y al contacto con el agua producen reacciones violentas y hasta explosivas. Estos incendios deben combatirse con extintores de polvo químico.

Con esta información queda claro que deben incrementarse las medidas de prevención y seguridad en las plantas e industrias que emplean agentes químicos. La forma más práctica de hacerlo es evaluando meticulosamente los riesgos químicos inherentes a la actividad que se desarrolla, enseguida

.

estableciendo medidas de prevención que oponen a la remoción y control de dichos riesgos y en todos los casos, planificando la mitigación de efectos.

Así pues, las acciones de prevención deben concentrarse en evitar que ocurran los accidentes donde se involucren sustancias peligrosas, ya que sus características corrosivas, tóxicas, reactivas, explosivas, inflamables, infecciosas o irritantes, pueden traer daños inmediatos y crónicos, cuyos efectos pueden extenderse en tiempo y espacio, más allá de las capacidades del hombre.

Los incendios que se podrían dar serian los siguientes:

2.3.1.10.1 INCENDIOS INDUSTRIALES

Como su nombre lo indica, son aquellos incendios no controlados de grandes proporciones, que pueden presentarse en forma súbita, gradual o instantánea en plantas e industrias que emplean agentes químicos, en el tránsito de vehículos con tanques líquidos inflamables y/o tóxicos, la generada por cableado eléctrico de alta tensión, en bodegas de material combustibles o por combustión espontánea (como consecuencia de la degradación y/o descomposición orgánica de algunos compuestos químicos, cuyo resultado es una reacción exotérmica o un sobrecalentamiento gradual, que provoca fuego) y que requieren para su eliminación o control de métodos acordes al tipo de agente que lo origina.

Los incendios industriales que se dan en zonas de alta densidad poblacional implican mayores riesgos, por ello la preparación y colaboración ciudadana adquiere mayor importancia y valor. Dado que el desarrollo urbano y su convivencia con zonas industriales implica incongruencia, por la mezcla de establecimientos industriales peligrosos con mercados, escuelas y zonas habitacionales. Cuando un riesgo no se puede eliminar, en primera instancia se debe buscar el método de protección más eficaz y eficiente, que permita la prevención de desastres y la reducción de lesiones y daños a la población y entorno.

Una forma de prevenir o mitigar los efectos de este tipo de fenómenos es la de evaluar meticulosamente los riesgos inherentes a las actividades industriales,

.

además de planificar la actuación interinstitucional coordinada que permita prestar el auxilio oportuno y eficaz en caso de este tipo de contingencia, por lo que atendiendo al tamaño o extensión física, al tipo de fuego y agente que lo origina será la magnitud del posible daño.

2.3.1.10.2 INCENDIOS URBANOS

Siniestro en el cual ocurre la destrucción total o parcial de instalaciones, casas o edificios, en los cuales existe alta concentración de asentamientos humanos, ya sea dentro de ellos o en sus alrededores.

Los incendios urbanos se dividen en domésticos, comerciales e industriales, y representan el 93% del total de incendios ocurridos en el país; 85% suceden principalmente en casas habitación; los comerciales implican un 5%, y los Industriales alrededor de 3%; esto según la delegación centro de los bomberos salvadoreños, específicamente el Jefe de la Delegación, dichos datos pertenecen al año 2005.

El menosprecio a la probabilidad de riesgo de incendios en oficinas, condominios y casas-habitación, ha provocado que estos se agraven por apatía e incuria, por lo que es de tomarse en cuenta que la causa principal que provoca más muertes durante siniestros de este tipo es la asfixia por inhalación de humo, lo que indica que el problema en la mayoría de las veces es el control de la ventilación; lo cual radica específicamente en el diseño de las edificaciones, donde poco se piensa en la seguridad integral de los inmuebles y mucho en su apariencia estética, muchas veces a expensas de la seguridad.

2.4 ADMINISTRACION DE RECURSOS TECNOLOGICOS

2.4.1 ORGANIZACIÓN DE LOS RECURSOS TECNOLOGICOS

El crecimiento de las empresas depende de los recursos tecnológicos que éste utilice. A mayores necesidades mayores recursos de gestión informática necesitará la organización para poner en marcha sus proyectos. El uso

.

inadecuado de éstos puede generar una difícil administración, contratación de personal altamente calificado para atender las necesidades de cada herramienta, así como la pérdida de control y gestión sobre los recursos informáticos.

Administrar una infraestructura significa atender diversos problemas y necesidades. Por lo que es necesario que el área de Tecnologías de Información adquiera diferentes soluciones para hacerlos frente de un modo adecuado, ya que el punto crucial es cuando se necesita que las diversas soluciones se comuniquen entre sí, intercambien información y provean de un único punto de referencia a los usuarios. A este proceso se le denomina: Integración. En esta etapa, el beneficio más notorio es la reducción de costos, porque solo se gestiona aquello que es absolutamente necesario. En segunda instancia se logra mejorar notablemente el grado de satisfacción del cliente.

Efectuar cambios tecnológicos no sólo quiere decir renovar equipos sino también mejorar toda la plataforma informática de una organización. Actualmente existen en el mercado productos de gestión que ayudan a mejorar los niveles de servicio y atención a los recursos y usuarios de la empresa. Con la aplicación de estas soluciones, se logra entre otras cosas reducir la complejidad de administración de los recursos tecnológicos, aumentar la satisfacción y productividad de los usuarios.

Para afrontar estos cambios y tendencias de mercado, las organizaciones deben tomar conciencia de la importancia de la gestión de los recursos de TI. Hacer un análisis y evaluación de los problemas que tienen al momento de dar soporte a la plataforma informática con la que cuentan, para finalmente diseñar e implementar una solución que se ajuste a las necesidades actuales y futuras.

Todo proceso de mejora tecnológica debe ir acompañado de un plan de sistemas que ayude a definir los objetivos y, alcanzar las metas propuestas por la organización, a fin de que éstas mejoren la productividad y reduzcan el mal uso que los usuarios dan a los recursos tecnológicos, uno de los factores que más afecta a la organización.

.

2.4.2 ELEMENTOS MATERIALES

En la organización de los recursos tecnológicos se pueden distinguir tres tipos de elementos materiales:

1- La infraestructura física. Dentro de la infraestructura física consideramos:

- El espacio físico disponible para el uso y el almacenamiento de los recursos.
- Las instalaciones: iluminación, enchufes, ventilación, aislamiento, sistemas de seguridad.
- Los materiales complementarios: mesas, armarios, sillas, archivadores, etc.

2- Los recursos tecnológicos. Son los recursos necesarios para poder proveer los servicios necesarios a las personas que realizan cierto tipo de funciones que requieren del soporte tecnológico. Por ejemplo:

- Computadoras, servidores, telefonía, redes de comunicación, impresoras, conexiones telemáticas y otros recursos informáticos.
- TV, TV por cable, TV por satélite, equipos de radio, celulares.
- Retroproyectores, proyectores de diapositivas, cámaras fotográficas, micros.

3- Materiales de Apoyo. Son los materiales que permitirán a cada uno de las personas que proveen los servicios dentro de la organización el aprendizaje de cada unos de los recursos tecnológicos. Estos materiales son mas que nada de apoyo para facilitar el uso de los diferentes equipos informáticos. Dentro de estos materiales podemos destacar:

- Programas informáticos.
- Programas de vídeo.
- Diapositivas, transparencias.
- Casetes, discos compactos.

.

2.4.3 ELEMENTOS PERSONALES

Los elementos personales de la organización comprenden todo el personal (profesional, administrativo, técnico, y de apoyo) que toma parte en cualquiera de las actividades de la organización, elementos personales de la organización constituyen quizás su más valioso elemento. Esto es especialmente así cuando las personas que desempeñan las labores más importantes en la organización son altamente capacitadas.

La administración de los elementos personales de la organización es la responsable de asegurar que se satisfagan las necesidades de las personas. Esta no es una función meramente altruista: el personal satisfecho con sus condiciones laborales y estimulados por el ambiente suele ser el más productivo. La administración de los elementos personales es la responsable de la planificación; contratación; desarrollo de recursos humanos; evaluaciones y recompensas; y de mantener relaciones efectivas en los elementos personales.

2.4.4 ELEMENTOS FUNCIONALES

Los elementos funcionales son aquellos sobre los cuales actúa la logística operativa, son considerados como: la agrupación de actividades logísticas, técnicas con una función básica en común.

Las políticas de uso de equipo dentro de la organización será uno de los elementos fundamentales para poder asegurar la red de datos, tanto en la información que se maneja dentro de la misma, como la que pueda entrar o salir a la Internet. El conocimiento de estas Políticas por parte de los integrantes de la organización garantizara el buen funcionamiento de la red de datos, realizando cada una de estas políticas en los momentos adecuados.

.

2.5 ADMINISTRACION DE RIESGO

Al margen de la seguridad que se pueda tener, nos parece que el mayor riesgo, aún teniendo un entorno muy seguro, es que la Informática y la Tecnología de la Información en general no cubran las necesidades de la entidad; o que no estén alineadas con las finalidades de la organización.

Limitándonos a la seguridad propiamente dicha, los riesgos pueden ser múltiples. El primer paso es conocerlos y el segundo es tomar decisiones al respecto; conocerlos y no tomar decisiones no tiene sentido y debiera crearnos una situación de desasosiego.

Dado que las medidas tienen un costo, a veces, los funcionarios se preguntan cuál es el riesgo máximo que podría soportar su organización. La respuesta no es fácil porque depende de la criticidad del sector y de la entidad misma, de su dependencia respecto de la información, y del impacto que su no disponibilidad pudiera tener en la entidad. Si nos basamos en el impacto nunca debería aceptarse un riesgo que pudiera llegar a poner en peligro la propia continuidad de la entidad, pero este listón es demasiado alto.

Por debajo de ello hay daños de menores consecuencias, siendo los errores y omisiones la causa más frecuente - normalmente de poco impacto pero frecuencia muy alta - y otros, como por ejemplo:

- El acceso indebido a los datos (a veces a través de redes),
- La cesión no autorizada de soportes magnéticos con información crítica (Algunos dicen "sensible"),
- Los daños por fuego, por agua (del exterior como puede ser una inundación, o por una tubería interior),
- La variación no autorizada de programas, su copia indebida, y tantos otros, persiguiendo el propio beneficio o causar un daño, a veces por venganza.

.

Otra figura es la del “hacker”, que intenta acceder a los sistemas sobre todo para demostrar (a veces, para demostrarse a sí mismo/a) qué es capaz de hacer, al superar las barreras de protección que se hayan establecido.

Alguien podría preguntarse por qué no se citan los virus, cuando han tenido tanta incidencia. Afortunadamente, este riesgo es menor en la actualidad comparando con años atrás. Existe, de todas maneras, un riesgo constante porque de forma continua aparecen nuevas modalidades, que no son detectadas por los programas antivirus hasta que las nuevas versiones los contemplan. Un riesgo adicional es que los virus pueden llegar a afectar a los grandes sistemas, sobre todo a través de las redes, pero esto es realmente difícil - no nos atrevemos a decir que imposible- por las características y la complejidad de los grandes equipos y debido a las características de diseño de sus sistemas operativos.

En definitiva, las amenazas hechas realidad pueden llegar a afectar los datos, en las personas, en los programas, en los equipos, en la red y algunas veces, simultáneamente en varios de ellos, como puede ser un incendio.

Podríamos hacernos una pregunta realmente difícil: ¿qué es lo más crítico que debería protegerse? La respuesta de la mayoría, probablemente, sería que las personas resultan el punto más crítico y el valor de una vida humana no se puede comparar con las computadoras, las aplicaciones o los datos de cualquier entidad. Ahora bien, por otra parte, podemos determinar que los datos son aún más críticos si nos centramos en la continuidad de la entidad.

Como consecuencia de cualquier incidencia, se pueden producir unas pérdidas que pueden ser no sólo directas (comúnmente que son cubiertas por los seguros) más fácilmente, sino también indirectas, como la no recuperación de deudas al perder los datos, o no poder tomar las decisiones adecuadas en el momento oportuno por carecer de información.

Sabemos que se producen casos similares en gran parte de entidades, pero en general no conocemos a cuáles han afectado (o lo sabemos pero no podemos difundirlo), porque por imagen estos no se hacen públicos y el hecho de que se

.

conozcan muchos más referidos a Estados Unidos y a otros puntos lejanos que respecto de nuestros países no significa que estemos a salvo, sino que nuestro pudor es mayor y los ocultamos siempre que podemos.

2.5.1 ESTRATEGIAS DE SEGURIDAD

El analisis de riesgos supone mas que el hecho de calcular la posibilidad de que ocurran cosas negativas.

- Se debe poder obtemer una evaluacion economica del impacto de estos sucesos. Este valor se podra utilizar para contrastar el costo de la proteccion de la informacion en analisis, versus el costo de volverla a producir (reproducir).
- Se debe tener en cuenta la probabilidad que sucedan cada uno de los problemas posibles. DE esta forma se pueden priorizar los problemas y su costo potencial desarrollando un plan de accion adecuado.
- Se debe conocer que se quiere proteger, donde y como, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se debera identificar los recursos (hardware, software, informacion, personal, accesorios, etc.) con que se cuenta y las amenazas a las que se esta expuesto.

La evaluacion de riesgos y presentacion de respuestas debe prepararse de forma personalizada para cada organización; pero se puede presuponer algunas preguntas que ayudan en la identificacion de lo anteriormente expuesto:

- “¿Qué puede ir mal?”
- “¿Con que frecuencia puede ocurrir?”
- “¿Cuáles serian sus concecuencias?”
- “¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?”
- “¿Se esta preparado para abrir las puertas del negocio sin tener una red de datos, por un dia, una semana, cuanto tiempo?”
- “¿Cuál es el costo de una hora sin la red, un dia, una semana…?”

.

- “¿Cuánto, tiempo se puede estar off-line sin que los clientes se vayan a la competencia?”
- “¿Se tiene forma de detectar a un empleado deshonesto dentro de la red de datos?”
- “¿Se tiene control sobre las operaciones de los distintos puntos de la red de datos?”
- “¿Cuántas personas dentro de la organización, (sin considerar su honestidad), estan en condiciones de inhibir la seguridad de la red de datos?”
- “¿A que se le llama dentro de la red informacion confidencial y/o sensitiva?”
- “¿La informacion confidencial y sensitiva permanece asi dentro del manejo o uso de la red?”
- “¿La seguridad actual cubre los tipos de ataques existentes y esta preparada para adecuarse a los avances tecnologicos esperados?”
- “¿A quien se le permite el uso de este recurso?”
- “¿Quién es el propietario del recurso? y ¿Quién es el propietario con mayores privilegios sobre los recursos?”
- “¿Cuáles seran los privilegios y responsabilidades del Administrador vrs la del usuario?”
- “¿Cómo se actuara si la seguridad es violada?”

Una vez obtenida la lista de cada uno de los riesgos, se podria efectuar un resumen del tipo de estos, como por ejemplo:

Figura 04 -Descripción de Tipos de Riesgo

Tipo de Riesgo	Factor
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

.

2.5.1.1 DEFINICION DE ESTRATEGIAS

Una vez conocidos los riesgos, los recursos que se deben proteger y como su daño o falta pueden influir en la organización es necesario identificar cada una de las amenazas y vulnerabilidades que pueden causar estas bajas en los recursos.

Existe por ende, una relacion directa entre amenaza y vulnerabilidad a tal punto que si una no existe la otra tampoco.

Se suelen dividir las amenazas existentes según su ambito de accion:

- Desastres del entorno (Seguridad Fisica).
- Amenazas del Sistema (Seguridad Logica).
- Amenazas en la red (Comunicaciones).
- Amenazas de personas (Dentro y fuera de la Institucion).

Por lo que una de las estratefias principales que se tiene que elaborar es una lista de amenazas (actualizadas) para ayudar a el administrador de la red de datos, a identificar los distintos metodos, herramientas y tecnicas de ataque que se pueden utilizar. Es importante que los administradores actualican constantemente sus conocimientos en esta area, ya que los nuevos metodos, herramientas y tecnicas para sortear las medidas de seguridad evolucionan de forma continua.

Cada una de las estrategias que se defina tendra que tener puntualmente la forma en la cual se podra resolver la amenza. Dicho procedimiento tendria que considerar la posibilidades de la amenaza antes, durante y despues de esta.

Por lo anterior es necesario que para definir una estrategia es conveniente pensar en las politicas de prevencion en los distintos niveles que esta debe abarcar y que son los Fisicos, Logicos Humanos y la interaccion que existe entre los factores. Dichas estrategias las podemos dividirlas en Proactiva y Reactiva.

.

La Estrategia Proactiva, (proteger y proceder) o de prevision de amenzas es un conjunto de pasos que ayuda a reducir al minumo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar los planes de contingencia. La determinacion del daño que una amenaza ca a provocar en una red de datos y las debilidades y puntos vlnerables explotados durante esta amenza ayudara a desarrollar esta estrategia.

La Estrategia Reactiva (perseguir y procesar) o estrategia posterior a la amenaza, ayuda al personal de la red de datos o administradores a evaluar el daño que ha causado la amenaza o ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia Proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos:

- Lo que no se permite expresamente esta prohibido: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa esta prohibida.
- Los que no se prohibe expresamente esta permitido: significa que, a menos que se indique expresamente que cierto servicio no esta disponible, todos los demas si lo estaran.

Estas posturas constituyen la base de todas las demas politicas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir que acciones se toleran y cuales no.

Actualmente, y “gracias” a las, cada dia mas repetitivas y eficaces, acciones que atenta contra las redes de datos, se inclinan para recomendar la primera politica mencionada.

2.5.2 INDICADORES TECNOLOGICOS

.

En la actualidad se observa una creciente preocupación por el papel de la tecnología en el comercio y en el desarrollo de los países. La rapidez de los cambios tecnológicos ha renovado el interés por las cuestiones de tecnología. Esto ha desembocado en la tarea de elaborar indicadores que permitan evaluar la capacidad científica y tecnológica de los países, y el seguimiento y estimación de los correspondientes progresos realizados y resultados obtenidos.

Debido a esto, desde hace años organismos gubernamentales y no gubernamentales vienen esforzándose continuamente por elaborar nuevos indicadores y mejorar los ya existentes. Entre las organizaciones que se encargan de la recolección de información se pueden nombrar la UNESCO, la OMPI, la ONUDI, el FMI, la OCDE y el Banco Mundial.

Un inconveniente presente en el desarrollo de estos indicadores está determinado por la brecha que existe entre los países del primer mundo y los países en vías de desarrollo. Las características de industrialización, así como sus políticas y la escasez de información influyen sobre la utilidad de los indicadores existentes.

Para realizar un mejor análisis de los indicadores se decidió agrupar los mismos analizando el carácter del cambio tecnológico como proceso.

La clasificación que se utiliza es la siguiente:

a) Indicadores de insumos de la tecnología: miden los recursos dedicados a la producción de conocimientos científicos y tecnológicos. Los recursos que se destinan a la producción de conocimientos científicos y tecnológicos forman parte del sistema de ciencia y tecnología relativa a los insumos.
   También se debe incluir las actividades de investigación y desarrollo, la tecnología transferida y el esfuerzo interno en forma de desarrollo de los recursos humanos o inversiones en maquinaria y equipo. Se dividen en dos grupos:
   - Tecnología transferida: proviene de fuentes externas al país. Al hablar de transferencia de tecnología, no solo se refiere al equipo físico y el soporte lógico, sino a los conocimientos técnicos necesarios para

.

dominar la tecnología importada. La transferencia de tecnología se puede lograr a través de corrientes comerciales y corrientes no comerciales.

En el caso de las corrientes comerciales, la transferencia se realiza mediante la importación de bienes de capital con “tecnología incorporada”, las inversiones extranjeras directas, concesión de patentes, acuerdos para la transferencia de conocimientos técnicos, la prestación de servicios técnicos y de asesoramiento, la migración de mano de obra calificada, entre otras.

La transferencia de tecnología por canales no comerciales se centra en la cooperación técnica financiada por organismos gubernamentales oficiales y por no gubernamentales y clientes, así como la información proveniente de publicaciones especializadas.

El principal inconveniente en el funcionamiento de estos indicadores es la falta de datos de los países en vías de desarrollo. Otro inconveniente lo plantea la transferencia de tecnología dentro de las empresas multinacionales, que por lo general no se registra.

- Innovación o esfuerzo interno: es resultado del esfuerzo del país. El esfuerzo tecnológico interno, el desarrollo de recursos humanos e inversiones en activos fijos, son fundamentales para el crecimiento tecnológico de un país. Este esfuerzo se ve influido por una gran gama de factores (infraestructura física e institucional, sistemas de financiación, características del mercado, políticas nacionales, entre otras). La insuficiencia de datos no permite tener indicadores que admitan tener en cuenta en forma simultánea, el desarrollo de recursos humanos y las inversiones en activos fijos. Por este motivo estos parámetros se deben estudiar por medio de indicadores separados.

b) Indicadores de resultados de la tecnología: miden el producto de las actividades científicas y económicas. No existe todavía una forma directa

.

de medir los “resultados” de la tecnología. Los únicos indicadores que se utilizan se basan en datos reunidos con otros fines. Los más utilizados en los países se basan en actividades en materia de patentes y en las publicaciones científicas o bibliometría.

2.6 DAÑO

Al hablar de daño dentro de nuestra red de datos tenemos que hablar de los que son los hackers y virus y de los perjuicios que estos producen dentro de nuestra res de datos.

Desde el momento que nos conectamos a Internet, nuestro equipo se encuentra vulnerable a diversos tipos de ataques, desde virus, hasta intrusiones.

La cuestión es, que acciones tenemos en caso de sufrir un daño, destrucción de archivos en nuestro sistema informático. Generalmente se produce por la utilización de "virus informáticos" que pueden entrar a través de la red, en igual medida sirven para destruir archivos en las bases de datos.
El "delito de daño" se produce sobre las cosas por ejemplo el hardware, en el caso del software son "impulsos electrónicos magnéticos o lumínicos susceptibles de apropiación y de ser decodificados y convertidos en accesibles a la lectura humana" por analogía "energía".

Se trata de una acción dolosa o culposa que penalmente en la medida en que se destruyen o inutilizan archivos, siendo de aplicación las normas civiles sobre responsabilidad por los delitos.

Aunque parezca una tontería, nuestro primer error es dar por sentado que al no tener enemigos aparentes, nadie nos va a hacer nada. En la mayoría de los casos, tanto la infección, como la vulnerabilidad de nuestro sistema, son debido a la dejadez o a ciertos actos involuntarios difíciles de controlar, como navegar por una página web infectada.

.

Dentro de la red de datos hay muchos peligros que nos acechan, en casi todos los casos, el modo de infección o transmisión se reduce a dos vías: la navegación y el correo electrónico. Ambos caminos son utilizados por "piratas informáticos" (hackers y crackers) para cometer sus delitos.

2.6.1 HACKERS

Hacker (del inglés hack, recortar) es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc.

Su entendimiento es más sofisticado y profundo respecto a los sistemas informáticos, ya sea de tipo hardware o software. Se suele llamar hackeo y hackear a las obras propias de un hacker.

El término "Hacker" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. No implica trabajar solo ni con otros necesariamente. Es posible en cualquier proyecto. No implica tampoco hacerlo con computadoras. Es posible ser un hacker de las bicicletas.

2.6.2 CRACKERS

Los llamados crackers (que significa rompedores) o "Black hat" (sombreros negros) usan su conocimiento con fines maliciosos, antimorales o incluso bélicos, como intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información, distribuir material ilegal o moralmente inaceptable, fabricación de virus, herramientas de Crackeo y elementos de posible terrorismo como la distribución de manuales para fabricar elementos explosivos caseros o la clásica

.

tortura china. El Cracker se distingue del Hacker por sus valores morales, sociales y políticos.

2.6.3 VIRUS

Es un pequeño programa capaz de reproducirse a sí mismo, infectando cualquier tipo de archivo ejecutable, sin conocimiento del usuario. El virus tiene la misión que le ha encomendado su programador, ésta puede ser desde un simple mensaje, hasta la destrucción total de los datos almacenados en el ordenador.

Lo único que tienen en común todos es que han de pasar desapercibidos el mayor tiempo posible para poder cumplir su trabajo. Una vez infectado una computadora, el virus no tiene por que cumplir su misión al momento, algunos esperan una fecha, evento o acción del sistema para llevar a fin su objetivo.

Se llaman de esta forma, por su analogía con los virus biológicos del ser humano. Al igual que estos, los informáticos tienen un ciclo de vida, que va desde que "nacen", hasta que "mueren". Creación, gestación, reproducción, activación, descubrimiento, asimilación, y eliminación. Además, existen varias técnicas que permiten a un virus ocultarse en el sistema y no ser detectado por el antivirus: ocultación, protección antivirus, camuflaje y evasión.

2.6.4 GUSANOS

Es un código maligno cuya principal misión es reenviarse a sí mismo. Son códigos víricos que, en principio, no afectan a la información de los sitios que contagian, aunque consumen amplios recursos de los sistemas, y los usan para infectar a otros equipos.

A diferencia de la mayoría de virus, los gusanos se propagan por sí mismos, sin modificar u ocultarse bajo otros programas. No destruyen información de forma directa, pero algunos pueden contener dentro de sí, propiedades características de los virus.

.

El mayor efecto de los gusanos es su capacidad para saturar, e incluso bloquear por exceso de tráfico los sitios web, aunque estos se encuentren protegidos por un antivirus actualizado.

2.6.5 TROYANOS

Es un programa potencialmente peligroso que se oculta dentro de otro para evitar ser detectado, e instalarse de forma permanente en nuestro sistema. Este tipo de software no suele realizar acciones destructivas por sí mismo, pero entre muchas otras funciones, tienen la capacidad de capturar datos, generalmente contraseñas e información privada, enviándolos a otro sitio.

Otra de sus funciones es dejar indefenso nuestro sistema, abriendo brechas en la seguridad, de esta forma se puede tomar el control total de forma remota, como si realmente se estuviera trabajando delante de nuestra pantalla.

2.7 PROCESO DE TECNOLOGIA DE INFORMACION

2.7.1 UN RESULTADO DESEADO, SE ALCANZA CON MAS EFICIENCIA CUANDO SUS ACTIVIDADES Y RECURSOS RELACIONADOS, SON MANEJADOS COMO PROCESOS.

Las organizaciones son tan eficientes como lo son sus procesos. La mayoría de las empresas han tomado conciencia de esto y se plantean como mejorarlos y evitar algunos males habituales como: bajo rendimiento, poco enfoque al cliente, barreras departamentales, subprocesos inútiles debido a la falta de visión global del proceso, etc.

Un proceso puede ser definido como un conjunto de actividades interrelacionadas entre sí que, a partir de una o varias entradas de materiales o información, dan lugar a una o varias salidas también de materiales o información con valor añadido.

.

En otras palabras, los procesos es la manera en la que se hacen las cosas en la empresa. Ejemplos de procesos son el de producción y entrega de bienes y/o servicios, el de gestión comercial, el de desarrollo de la visión estrategia, el de desarrollo de producto, estos procesos deben estar correctamente gestionados empleando distintas herramientas de la gestión de procesos.

La incorporación de las Tecnologías de la Información permite redefinir los procesos alcanzando grados de eficacia y eficiencia inimaginables hace unos años. Las organizaciones que sean capaces de descubrir estas posibilidades e implantarlas correctamente, conseguirán ventajas competitivas debido a la disminución de costes y el aumento de flexibilidad frente a los requerimientos de los clientes.

Los procesos de negocio deben estar correctamente gestionados empleando los sistemas de información para la gestión (ERP Enterprise Resource Planning en ingles). Un sistema de información para la gestión se puede definir como una aplicación de gestión empresarial que integra el flujo de información, consiguiendo así mejorar los procesos en distintas áreas (financiera, de producción, logística, comercial y de recursos humanos).

Los objetivos principales de los sistemas ERP son:

1. Optimización de los procesos empresariales.
2. Acceso a información confiable, precisa y oportuna.
3. La posibilidad de compartir información entre todos los componentes de la organización.
4. Eliminación de datos y operaciones innecesarias.
5. Reducción de tiempos y de los costes de los procesos.

En cuanto a los procesos que tienen oportunidades de mejora, en cualquier proceso en el que existan intercambios de información, el impacto de las Tecnologías de Información será muy importante, tanto que redefinirá totalmente el proceso. Es debido a que toda la información podrá ser "digitalizable" y por tanto gestionada automáticamente empleando los sistemas de Información y pudiendo ser comunicada a coste cero empleando las redes (Intranet, Extranet e Internet).

.

Claramente, todos los procesos que se basen fundamentalmente en intercambios de bienes físicos, tendrán muchísimas menos oportunidades.

2.8 ARQUITECTURA DE SEGURIDAD PARA AREAS INFORMATICAS

2.8.1 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la organización para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de

.

la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

2.8.1.1 PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la organización, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.

.

- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

2.8.1.1.1 PRINCIPIO DE MENOR PRIVILEGIO

Este 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, etc.) debe tener tan solo los privilegios de uso necesarios 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, programa, etc., 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 llevar a cabo estas acciones.

2.8.1.1.2 LA SEGURIDAD NO SE OBTIENE A TRAVÉS DE LA OSCURIDAD

Una red de datos no es más seguro porque escondamos sus posibles defectos o vulnerabilidades, sino porque los conozcamos y corrijamos 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 corrija.

No es una buena medida basar la seguridad en el hecho de que un posible atacante no conozca las vulnerabilidades de nuestra red de datos. Los atacantes

.

siempre disponen de los medios necesarios para descubrir las debilidades más insospechadas de nuestra red de datos.

No se consigue proteger una red de datos 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 ordenes que pueden utilizarse para entrar a la red de datos. Educar a los usuarios o diseñadores sobre el funcionamiento de la red de datos 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 nuestra red de datos 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.

2.8.1.1.3 PRINCIPIO DEL ESLABÓN MÁS DÉBIL

En toda red 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 una red de seguridad el atacante siempre acaba encontrando y aprovechando los puntos débiles o vulnerabilidades.

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

Por ejemplo, si se establece una política de asignación de passwords muy segura, en la que estos se asignan automáticamente, son aleatorios y se cambian cada semana. Si en nuestra red de datos utilizamos la red ethernet para conectar nuestras máquinas, y no protegemos la conexión, no nos servirá de nada la política de passwords establecidas. Por defecto, por ethernet, los passwords circulan descifrados. Si cualquiera puede acceder a nuestra red de datos y "escuchar" todos los paquetes que circulan por la misma, es trivial que pueda

conocer nuestros passwords. En esta red de datos el punto débil es la red. Por mucho que hayamos reforzado la seguridad en otros puntos, la red de datos sigue siendo altamente vulnerable.

2.8.1.1.4 DEFENSA EN PROFUNDIDAD:

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

Por ejemplo en una red de datos podemos establecer un mecanismo de passwords 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.

2.8.1.1.5 PUNTO DE CONTROL CENTRALIZADO

Se trata de establecer un único punto de acceso a nuestra red de datos, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él. No se trata de utilizar un sólo mecanismo de seguridad, sino de "alinearlos" todos de modo que el usuario tenga que pasar por ellos para acceder a la red de datos.

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

2.8.1.1.6 SEGURIDAD EN CASO DE FALLO

.

Este principio afirma que en caso de que cualquier mecanismo de seguridad falle, nuestra red de datos debe quedar en un estado seguro. Por ejemplo, si nuestros mecanismos de control de acceso a la red de datos fallan, es mejor que como resultado no dejen pasar a ningún usuario que dejen pasar a cualquiera aunque no esté autorizado.

Quizás algunos ejemplos de la vida real ayuden a aclarar este concepto. Normalmente 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.

2.8.1.1.7 PARTICIPACIÓN UNIVERSAL

Para que cualquier red de seguridad funcione es necesaria la participación universal, o al menos no la oposición activa, de los usuarios de la red de datos. 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 una red de datos 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 la red de datos siempre tenderá a mejorar.

2.8.1.1.8 SIMPLICIDAD

La simplicidad es un principio de seguridad por dos razones. En primer lugar, mantener las cosas lo más simples posibles, 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.

.

Por eso al hacer el diseño de las políticas de seguridad es mejor hacer un previo estudio de las tareas o servicios que realizan cada una de las áreas para poder hacer que dichas políticas sean desarrolladas con la mayor simplicidad posible para que las personas afectadas por las mismas las entiendan y les sea fácil aplicarlas en su trabajo.

2.8.2 NORMAS Y ESTRUCTURAS

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. Estas políticas son de tres tipos:

- Laborales.
- Hardware.
- Software.

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.

Los propios directivos deben acoplarse a estas políticas de seguridad, con el objetivo de que se mantengan estándares dentro de la organización. Es importante resaltar que la creación de políticas conlleva a la creación de reglamentos de seguridad.

El compromiso de la Dirección con Seguridad Informática debe tomar la forma de una política de seguridad de los Sistemas de Seguridad Informática formalmente acordada y documentada. Dicha política tiene que ser consistente con las prácticas de seguridad de otros departamentos, puesto que muchas amenazas (incendio, inundación) son comunes a otras actividades de la organización.

.

Algunas reglas básicas a la hora de establecer una política de seguridad.

- Toda política de seguridad debe ser estratégica, es decir, debe cubrir todos los aspectos relacionados con la red de datos.
- Debe proteger el sistema en todos los niveles: físico, humano, lógico y logístico.
- Debe tener en cuenta no sólo 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 de la red de datos, esto es, el tipo de compañía o entidad con que tratamos (comercial, bancaria, educativa, etc.). De esta consideración surge la segunda regla básica.
- La política de seguridad debe adecuarse a nuestras necesidades y recursos, el valor que se le da a los recursos y a la información, el uso que se hace de la red de datos en todos los departamentos.
- Deben evaluarse los riesgos, el valor de la red de datos y el coste de atacarlo. Las medidas de seguridad tomadas deben ser proporcionales a estos valores.
- Toda política de seguridad debe basarse fundamentalmente en el sentido común. Es necesario:

    A. Un conocimiento de la red de datos a proteger y de su entorno.
    B. Un conocimiento y experiencia en la evaluación de riesgos y el establecimiento de medidas de seguridad.
    C. Un conocimiento de la naturaleza humana, de los usuarios y de sus posibles motivaciones.

A la hora de establecer una política de seguridad debemos responder a las siguientes tres preguntas:

1. ¿Qué necesitamos proteger?
2. ¿De qué necesitamos protegerlo?
3. ¿Cómo vamos a protegerlo?

Lo que nos lleva a los siguientes pasos básicos:

.

1. Determinar los recursos a proteger y su valor.
2. Analizar las vulnerabilidades y amenazas de nuestra red de datos, su probabilidad y su costo.
3. Definir las medidas a establecer para proteger la red de datos.

Estas medidas deben ser proporcionales a lo definido en los pasos 1 y 2.

Las medidas deben establecerse a todos los niveles: físico, lógico, humano y logístico.

Además debe definirse una estrategia a seguir en caso de fallo.

Monitorizar el cumplimiento de la política y revisarla y mejorarla cada vez que se detecte un problema, esto se logra por medio de una auditoria externa que tiene como propósito disparar estas alarmas generadas por problemas.

Los pasos 1 y 2 se denominan Análisis de riesgos, mientras los pasos 3 y 4 se denominan Gestión de riesgos. La política de seguridad es el conjunto de medidas establecidas en el paso 3.

2.8.3 PROCEDIMIENTOS Y SOPORTE

2.8.3.1 PROCEDIMIENTOS DE SEGURIDAD

Un procedimiento de seguridad es una serie de procedimientos de trabajo (pasos o actividades separadas) que establece qué riesgos de accidentes físicos se pueden encarar en la consecución del objetivo establecido. Los procedimientos de seguridad deben utilizarse como herramientas para capacitar al trabajador en su trabajo/tarea de manera segura. En los casos en que sea factible deberán utilizarse los procedimientos de operación en lugar de los procedimientos de seguridad; sin embargo, estos procedimientos deberán ser tan detallados como un procedimiento de seguridad en los casos en que esté involucrado algún peligro.

2.8.3.1.1 ELABORACIÓN DE PROCEDIMIENTOS DE SEGURIDAD

.

Básicamente, un procedimiento de seguridad implica cuatro pasos fundamentales. Es necesario que se cumplan los pasos que a continuación se listan para elaborar satisfactoriamente un procedimiento de seguridad:

a) Disgregar el trabajo en pasos
b) Seleccionar el trabajo que será analizado
c) Identificar el peligro potencial involucrado en cada paso
d) Desarrollar soluciones para controlar dichos peligros

La decisión de desarrollar un procedimiento de seguridad para un trabajo determinado dependerá de los siguientes factores: índice de accidentes, repetición o frecuencia del trabajo, si es un trabajo nuevo, si es un trabajo crítico, si ha habido quejas, o bien, dependerá de la evaluación de riesgos. Las prioridades dependerán de la razón por la cual se requiere elaborar el procedimiento de seguridad.

En cada trabajo se puede analizar la secuencia de pasos ya sea mediante la observación del mismo y su discusión con los empleados, realizando una discusión de grupo, o bien, una combinación de ambos métodos. El trabajo deberá disgregarse en pasos generales de acción. Hay que evitar establecer tanto pasos muy amplios como pasos demasiado específicos.

Posteriormente, es necesario identificar todos los peligros posibles que puede involucrar cada paso. No pase por alto los peligros triviales ya que generalmente son reales y pueden resultar en peligros más serios. No pase por alto información que puede utilizarse para investigar accidentes. Liste todas las posibilidades de cada paso.

Finalmente, desarrolle métodos seguros para controlar cada peligro. Aquí se pueden tomar en cuenta cuatro enfoques:

a) Soluciones radicales (una nueva forma de hacer las cosas, equipo nuevo, materiales nuevos, métodos nuevos, etc.).

.

b) Revisiones de ingeniería (reubicación de equipo, proporcionar escaleras, etc.).
c) Requisitos que debe cubrir el personal (habilidad física del empleado, aptitudes, etc.).
d) Proporcionar capacitación o instrucciones

2.8.3.2 SOPORTE DE SEGURIDAD

Tiene por objetivos mantener la operatividad y funcionalidad de los mecanismos de seguridad tanto física como a nivel lógico de la infraestructura tecnológica y de los servicios de Información que dan soporte a la gestión administrativa de la Institución. Realizar soporte en segundo nivel a los usuarios y red de datos en lo que a seguridad se refiere. Debe desarrollar e implementar políticas de seguridad para la infraestructura tecnológica y servicios de información. Evaluar en forma continua el cumplimiento y funcionamiento de todas las políticas de seguridad implementadas.

2.8.3.2.1 FUNCIONES DEL SOPORTE DE SEGURIDAD

Las funciones específicas son:

- Establecer mecanismos de muestreo (monitoreo) sobre la funcionalidad de los mecanismos de seguridad existentes.
- Asegurar la integridad de la Información mediante la aplicación de mecanismos de seguridad.
- Debe desarrollar e implementar políticas de seguridad para la infraestructura tecnológica y servicios de información.
- Atender los requerimientos de soporte y servicio de la unidad de Soporte al Usuario.
- Realizar la instalación y puesta en producción de mecanismos de seguridad que sean adquiridos o desarrollados por la unidad de Informática.

.

- Impartir adiestramiento a la Unidad de Atención al Usuario sobre las políticas de seguridad establecidas.
- Llevar diversas estadísticas sobre la funcionabilidad de los sistemas de seguridad implantados.
- Realizar pruebas periódicas de la seguridad.
- Reportar a la unidad de Informática sobre posibles fallas y vulnerabilidades de las redes de seguridad implantados.

2.9 LA TECNOLOGÍA DE INFORMACIÓN

2.9.1 INTRODUCCIÓN

En el mundo electrónico en el que vivimos nos encontramos rodeados de fuentes de información: televisión, radio, revistas, periódicos, revistas y más recientemente el Internet. Todas las noches vemos un noticiero, por las mañanas leemos el diario y durante el día hojeamos una revista, el Internet o vemos algún programa informativo por la televisión.

Y este gran cúmulo de información que absorbemos día con día pasa muchas veces desapercibido ante nosotros; estamos tan acostumbrados a éste tipo de información que no nos percatamos de la gran importancia que tiene esta información para nuestra vida personal.

Esta información se utiliza de maneras muy diversas, desde la persona que toma un paraguas antes de irse a trabajar, porque vio el estado del tiempo, hasta el inversionista que compra o vende acciones gracias a la información de la Bolsa. El punto importante es que todos buscamos la manera de mantenernos siempre "bien informados", además de buscar la manera de utilizar esa información para nuestro beneficio.

Ahora si viviéramos en un mundo aislado, sin ningún tipo de información más que la que se transmite de forma oral, de padres a hijos, de jefe a empleado. Solo por un momento, piense que en los albores del siglo XXI, no existieran los noticiarios, los periódicos, las revistas, las gacetas, ni ningún otro tipo de medio de

información, no, tampoco el Internet. Seguramente usted estará pensando: ¿Primitivo? ¿Imposible? ¿Inimaginable? Pues esto es precisamente lo que puede estar sucediendo en su empresa o negocio, si usted no cuenta con los suficientes -y adecuados- canales de información, tanto en el interior como hacia el exterior de la misma.

La información nos permite hacer eficientes todos los procesos internos de nuestra organización, nos permite también conocer mejor a nuestra competencia así como el mercado por el que se compite. En general podemos conocer mejor el medio tanto interno como externo de nuestro negocio, para así detectar nuestras debilidades y potencialidades, atacarlas, y lograr una ventaja competitiva con respecto a las demás organizaciones del ramo.

2.9.2 LA CREACIÓN DEL CONOCIMIENTO Y LA VENTAJA COMPETITIVA

La revolución de las Tecnologías de Información ha tenido un profundo efecto en la administración de las organizaciones, mejorando la habilidad de los administradores para coordinar y controlar las actividades de la organización y ayudándolos a tomar decisiones mucho más efectivas. Hoy en día el uso de las Tecnologías de Información se ha convertido en un componente central de toda empresa o negocio que busque un crecimiento sostenido.

El uso de Tecnologías de Información ya no lo es solo para procesos de producción o conversión, sino que deberá estar implícito en todos los ámbitos del negocio, incluyendo en el área administrativa, por ser esta la que controla toda la empresa. Como resultado del uso de estas tecnologías podemos decir que la empresa puede reducir el tamaño de su estructura jerárquica e incrementar el flujo de información horizontal, esto es, a través de todos los departamentos de la empresa, además de proveer de una ventaja competitiva a la empresa.

Reducción del tamaño de la estructura jerárquica. Esto se logra al proveer a los administradores y ejecutivos información de alta calidad, oportuna y completa, lo

.

cual reduce la necesidad de varios niveles de burocracia y jerarquía administrativa. Los sistemas de información al reducir éstos niveles jerárquicos, actúan como dispositivos de control en las actividades de la empresa o negocio. Cabe señalar que los sistemas de información también reducen la necesidad de los administradores de coordinar e integrar las actividades de las sub-unidades de la empresa, además de que las Tecnologías de Información actualmente pueden coordinar completamente el flujo de producción de una empresa.

Incremento del flujo de información horizontal. Facilitado por el crecimiento de los sistemas Cliente - Servidor del tipo three-tier (que permiten la conexión de computadoras personales a potentes servidores o mini-computadoras y éstos a su vez conectados a un mainframe) en los últimos años se ha visto una rápida expansión de los sistemas de red global en las empresas. Actualmente las redes de computadoras son usadas como el canal primario de información interna de una organización. Los sistemas de e-mail así como el desarrollo de software de Intranet para compartir documentos electrónicos, como Lotus Notes, han acelerado ésta tendencia tecnológica.

2.9.2.1 VENTAJA COMPETITIVA

Como se ha visto, el implementar apropiadas Tecnologías de Información puede significar un incremento en el potencial competitivo de la empresa o negocio. Actualmente, en la búsqueda de competitividad, se han vuelto los ojos hacia el uso de Tecnologías de Información, por ejemplo, al reducir la necesidad de muchas jerarquías, los sistemas de información ayudan a reducir los gastos burocráticos, ya que los administradores se basan en las Tecnologías de Información para coordinar y controlar las actividades de la empresa.

Además de que gracias a los canales de comunicación que proveen las Tecnologías de Información, podemos tener información clara y oportuna de todos los movimientos del entorno industrial, como lo son precios, clientes, impuestos, tipos de cambio, regulaciones, estándares y movimientos de la competencia, lo cuál ayuda a los ejecutivos al momento de diseñar estrategias competitivas. Aun

.

cuando a esto los grandes corporativos pueden mantener un flujo de información constante en todas sus Unidades de Negocios sin importar la distancia física a la que se encuentren distribuidos estos.

Por último, las Tecnologías de Información pueden ser usadas para mejorar la respuesta de una empresa o negocio hacia los requerimientos de los clientes, lo cual es una fuente muy importante de competitividad. La esencia de su argumento es que las Tecnologías de Información permiten a las compañías crear "productos virtuales", productos que pueden ser personalizados de acuerdo con las necesidades específicas de algún cliente en particular, sin cargos adicionales.

2.9.3 CONCLUSIONES

En la actualidad se puede obtener la información de un gran número de fuentes diversas, sin embargo, muchas empresas todavía no han adoptado las Tecnologías de Información como una herramienta básica para su desarrollo y competencia. Las Tecnologías de Información pueden ayudar a mejorar la productividad de todas las funciones de la empresa, y además de mejorar el flujo de información dentro y entre las Unidades del Negocio. Una organización que pretenda ser efectiva deberá de explotar y administrar todas éstas tecnologías para dar un valor agregado a toda la organización.

A través de la historia, las estructuras jerárquicas de muchos niveles han sido el modus operandi de la mayoría de las grandes empresas, sin embargo, el uso de Tecnologías de Información puede ayudar a la descentralización de la toma de decisiones, ya que la información puede fluir horizontal y verticalmente de una forma fácil y rápida. Los sistemas de Tecnologías de Información pueden ayudar de esa forma a disminuir los niveles jerárquicos desde los altos ejecutivos hasta el personal operativo. Las Tecnologías de Información permiten a una organización mejorar el manejo e integración de todos los datos y documentos que necesiten todas las unidades funcionales de ésta. Las Tecnologías de Información incrementan la flexibilidad organizacional y la coordinación de todas sus funciones. Adicionalmente a esto, las Tecnologías de Información nos dan una ventaja competitiva, al reducir nuestros costos de operación, flexibilidad

organizacional, rapidez en la toma de decisiones, respuesta hacia los requerimientos del cliente, información del mercado, competencia y entorno en general, además de manejar a las diferentes Unidades de Negocios como un todo, no importando su localidad física.

Por todo esto, debemos voltear la vista hacia las Tecnologías de Información como una parte medular del negocio, implementarla en todas las etapas de la empresa (entrada, conversión y salida), ya que esto nos permitirá evolucionar hacia el siguiente nivel: Las empresas en la Era de la Información. Debemos de enfocar el rumbo hacia las Tecnologías de Información ya que esta transición ya es inminente y si no se realiza a tiempo, mas tarde será mucho más costosa y dolorosa, y eventualmente podemos llegar a desaparecer como empresa si hacemos caso omiso del cambio tecnológico que en la actualidad se está viviendo en nuestro entorno.

2.10 MANTENIMIENTO PREVENTIVO

Este tipo de mantenimiento surge de la necesidad de rebajar el correctivo y todo lo que representa. Pretende reducir la reparación mediante una rutina de inspecciones periódicas y la renovación de los elementos dañados, si la segunda y tercera no se realizan, la tercera es inevitable.

Durante la segunda guerra mundial, el mantenimiento tiene un desarrollo importante debido a las aplicaciones militares, en esta evolución el mantenimiento preventivo consiste en la inspección de los aviones antes de cada vuelo y en el cambio de algunos componentes en función del número de horas de funcionamiento.

Características: Básicamente consiste en programar revisiones de los equipos, apoyándose en el conocimiento de la máquina en base a la experiencia y los históricos obtenidos de las mismas. Se confecciona un plan de mantenimiento para cada máquina, donde se realizaran las acciones necesarias, engrasan, cambian correas, desmontaje, limpieza, etc.

.

2.10.1 VENTAJAS DEL MANTENIMIENTO PREVENTIVO

Se hace correctamente, exige un conocimiento de las máquinas y un tratamiento de los históricos que ayudará en gran medida a controlar la maquinaria e instalaciones.

El cuidado periódico conlleva un estudio óptimo de conservación con la que es indispensable una aplicación eficaz para contribuir a un correcto sistema de calidad y a la mejora de los continuos.

Reducción del correctivo representará una reducción de costos de producción y un aumento de la disponibilidad, esto posibilita una planificación de los trabajos del departamento de mantenimiento, así como una previsión de los recambios o medios necesarios.

Se concreta de mutuo acuerdo entre las áreas donde se realizar el mantenimiento y las debidas personas que realizaran el mismo para ver cual será el mejor momento para realizar el paro de las instalaciones con producción para hacer las labores de mantenimiento.

Confiabilidad, los equipos operan en mejores condiciones de seguridad, ya que se conoce su estado y sus condiciones de funcionamiento.

Disminución de tiempo muerto, tiempo de parada de equipos/máquinas.

Mayor duración de los equipos e instalaciones.

Disminución de existencias en Almacén y, por lo tanto sus costos, puesto que se ajustan los repuestos de mayor y menor consumo.

Uniformidad en la carga de trabajo para el personal de Mantenimiento debido a una programación de actividades.

Menor costo de las reparaciones.

.

2.10.2 FASES DEL MANTENIMIENTO PREVENTIVO

1. Inventario técnico, con manuales, planos, características de cada equipo.
2. Procedimientos técnicos, listados de trabajos a efectuar periódicamente,
3. Control de frecuencias, indicación exacta de la fecha a efectuar el trabajo.
4. Registro de reparaciones, repuestos y costos que ayuden a planificar.

2.11 VULNERABILIDAD

Punto o aspecto de la red de datos que es susceptible de ser atacado o de dañar la seguridad de la misma. Representan las debilidades o aspectos falibles o atacables en la red de datos informática.

2.11.1 TIPOS DE VULNERABILIDAD

Realmente la seguridad es la facultad de estar a cubierto de algún riesgo o amenaza. Desde este punto de vista la seguridad total es muy difícil de logra, puesto que implicaría describir todos los riesgos y amenazas a que puede verse sometido la red de datos. Lo que se manifiesta en las redes de datos no es la seguridad, sino más bien la inseguridad o vulnerabilidad. No se puede hablar de una red informática totalmente segura, sino más bien de uno en el que no se conocen tipos de ataques que puedan vulnerarlo, debido a que se han establecido medidas contra ellos.

2.11.1.1 VULNERABILIDAD FÍSICA

Se encuentra en el nivel del edificio o entorno físico de la red de datos. Se relaciona con la posibilidad de entrar o acceder físicamente a la red de datos para robar, modificar o destruir la misma.

.

2.11.1.2 VULNERABILIDAD NATURAL

Se refiere al grado en que la red de datos puede verse afectada por desastres naturales o ambientales que pueden dañar completamente la red de datos, tales como el fuego, inundaciones, rayos, terremotos, o quizás más comúnmente, fallos eléctricos o picos de potencia. También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.

2.11.1.3 VULNERABILIDAD DEL HARDWARE Y DEL SOFTWARE

Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, ciertos sistemas requieren la posesión de algún tipo de herramienta o tarjeta para poder acceder a los mismos.

Ciertos fallos o debilidades del software de la red de datos hacen más fácil acceder al mismo y lo hacen menos fiable. En este apartado se incluyen todos los bugs en los sistemas operativos, u otros tipos de aplicaciones que permiten atacarlos.

2.11.1.4 VULNERABILIDAD DE LOS MEDIOS O DISPOSITIVOS

Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, etc. Cualquier tipo de medio en el cual se pueda almacenar o guardar información importante relacionada con la organización.

2.11.1.5 VULNERABILIDAD POR EMANACIÓN

Todos los dispositivos eléctricos y electrónicos emiten radiaciones electromagnéticas. Existen dispositivos y medios de interceptar estas emanaciones y descifrar o reconstruir la información almacenada o transmitida.

.

2.11.1.6 VULNERABILIDAD DE LAS COMUNICACIONES

La conexión de los ordenadores a redes supone sin duda un enorme incremento de la vulnerabilidad de la red de datos. Aumenta enormemente la escala del riesgo a que está sometido, al aumentar la cantidad de gente que puede tener acceso al mismo o intentar tenerlo. También se añade el riesgo de intercepción de las comunicaciones:

- Se puede penetrar a la red de datos a través de la intranet o Internet.
- Interceptar información que es transmitida desde o hacia la red de datos.

2.11.1.7 VULNERABILIDAD HUMANA

La gente que administra y utiliza la red de datos representa la mayor vulnerabilidad de la misma. Toda la seguridad de la red de datos descansa sobre el administrador de la misma que tiene acceso al máximo nivel y sin restricciones a la misma.

Los usuarios de la red de datos también suponen un gran riesgo al mismo. Ellos son los que pueden acceder a la misma, tanto físicamente como mediante conexión. Existen estudios que demuestran que más del 50% de los problemas de seguridad detectados son debidos a los usuarios de los mismos.

Por todo ello hay una clara diferenciación en los niveles de los distintos tipos de vulnerabilidad y en las medidas a adoptar para protegerse de ellos.

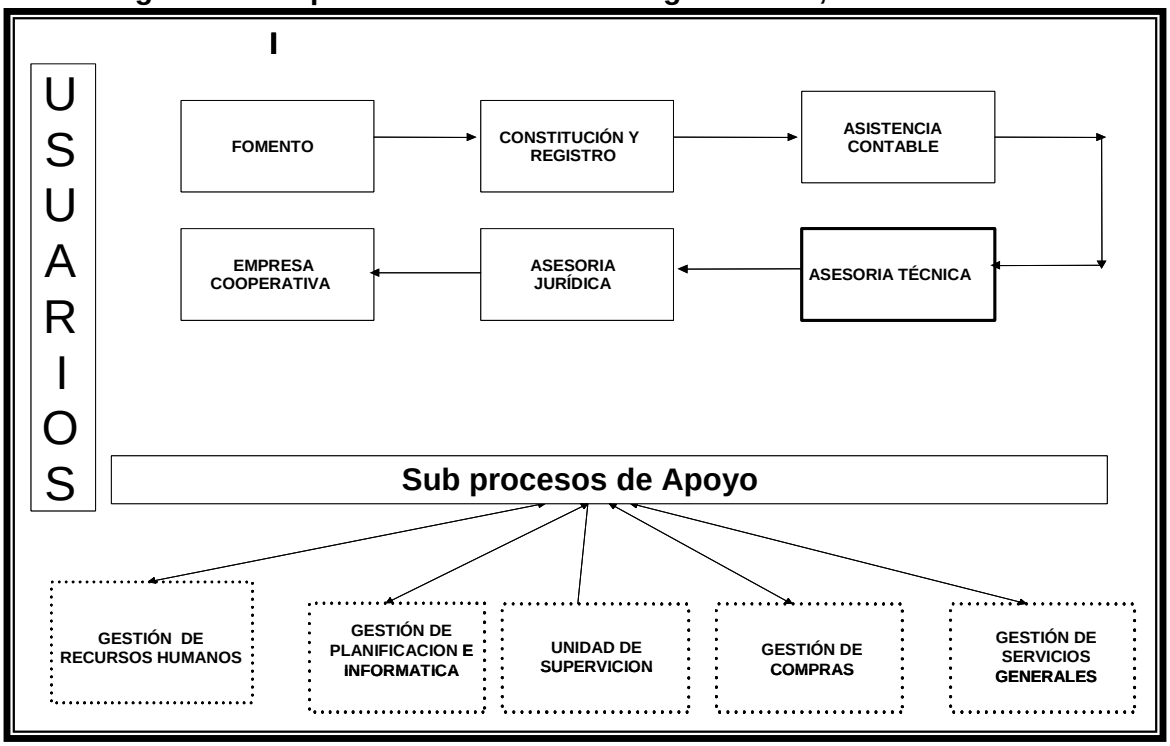
.

CAPITULO III.

3.1 METODOLOGIA DE LA INVESTIGACION.

La metodología de la investigación se construirá a partir de la técnica de la encuesta, en la cual se tomara como instrumento el cuestionario. Los encuestados serán los jefes de los departamentos que brindan los servicios a los clientes de la Institución, basados en el mapa de procesos del Sistema de Calidad ISO 9000:2000, el cual se muestra en la siguiente figura:

Figura 05 - Mapa de Procesos de La Organización, ISO 9000:2000



Al analizar el mapa de procesos, podemos observar que los departamentos que tienen una relación directa con el cliente externo son Fomento y Asistencia Técnica, Vigilancia y Fiscalización, Registro Cooperativo y Jurídico; Siendo los departamentos de Recursos Humanos, Planificación e Informática, Supervisión, unidad de Compras y Servicios Generales, apoyo para la realización de todos los servicios.

Los servicios certificados por la organización son los siguientes:

Listado de Servicios Certificados

1. Control documental
2. Control de los Registros
3. Competencia y formación
4. Mantenimiento preventivo y correctivo de equipo informático.
5. Control administrativo del equipo informático
6. Mantenimiento preventivo y correctivo de infraestructura.
7. Constitución e Inscripción de una Cooperativa
8. Asistencia Técnica, Administrativa y Legal
9. Investigación previa a asamblea General
10. Asistencia a Asambleas Generales
11. Diagnostico
12. Asesoria comité de Educación
13. Proceso de revisión de acuerdos
14. Proceso de reactivación
15. Proceso de reforma de estatutos
16. Artículo 72. Privilegios
17. Opinión Jurídica a Cooperativas
18. Diligenciar actos de denuncias
19. Convocatoria a asambleas
20. Revisión de Reglamentos
21. Revalúo
22. Extensión de documentos legales en caso de liquidación
23. Autorización de documentos para la operación de una Cooperativa.
24. Proyecto de estatutos
25. Nombramientos de delegados y elaboración de nota de asamblea.
26. Inscripción de estatutos
27. Revisión e Inspección de reforma de estatutos
28. Credenciales
29. Certificaciones
30. Requisitos para la legalización del sistema contable y libros de actas de una Asoc. Coop.
31. Aperturas y reaperturas contables.
32. Inspecciones parciales o totales de Estados Financieros.
33. Inspecciones Administrativas
34. Asistencia a Asambleas Generales.
35. Liquidaciones
36. Investigación de devolución de haberes
37. Investigación de exclusión de asociados en las asociaciones cooperativas.
38. Investigación beneficio Artículo 72.
39. Interventoría en las Asociaciones Cooperativas
40. Procedimiento para realizar revalúo de Inmuebles
41. Investigación previa a Asambleas Generales
42. Revisión de viáticos y recibos de transporte
43. Compras
44. Levantamiento de base de datos de cooperativas
45. Autorización de uso de vehículos en la Institución
46. Autorización de salida de equipo de la Institución
47. Preservación del producto.
48. Auditorias Internas

.

49. Acciones Correctoras y Preventivas
50. Inspección y ensayo
51. Control y servicios no conforme
52. Control de actividades programadas y realizadas
53. Seguimiento y medición de los procesos
54. Técnicas Estadísticas

La fuente de la información primaria para la recolección de la información es la Unidad de Calidad ISO 9000:2000, obteniendo la misma de la Base de Datos de dicha Unidad.

Los Servicios Certificados por la Institución, representan procesos, dentro de los cuales el uso de la Red de Datos, se vuelve esencial para el servicio a los clientes, especialmente porque muchos de ellos se brindan directamente en las diferentes zonas del país, donde se encuentran diseminadas las regionales de la Institución.

La fuente de información secundaria es cada una de las Oficinas Regionales, diseminadas en las cuatro zonas del país (Occidente, Central, Paracentral y Oriente). Cada una de estas oficinas funcionan de igual forma entre ellas, ya que los servicios que brindan son los mismos en cada una de ellas, con la diferencia de que el mercado objetivo al que se dirigen cambia de la siguiente manera:

Figura 06 - Mapa Cooperativo de El Salvador.
Censo Cooperativo 2005. Sep. 2005

.

1. Oficina Occidental: Santa Ana, Ahuachapan, Metapan y Sonsonate.
2. Oficina Central: San Salvador, Chalatenango y La Libertad.
3. Oficina Paracentral: San Vicente, La Paz, Cabañas y Cuscatlan.
4. Oficina Oriente: La Unión, Morazán y San Miguel.

Estas oficinas brindan los servicios a través de los departamentos de Fomento y Asistencia Técnica y Vigilancia y Fiscalización, los cuales permiten el seguimiento y asesoramiento a cada uno de los clientes que solicita dichos servicios. Mientras que los servicios de los departamentos de Jurídico y Registro, solo se puede realizar en la Oficina Central, estos servicios son demandados a través de los formularios que ISO 9000:2000, tiene registrados. Es por ello que se vuelve imprescindible el uso de la red de datos, transportando los documentos de solicitud de los clientes a la oficina central, para que en esta pueda ser resuelto según lo estipula cada uno de los procedimientos de los servicios en la Base de Datos de ISO 9000:2000.

Para el respaldo de todas las solicitudes realizadas por los clientes en cada una de las regionales, se envía el formulario en físico al respectivo departamento logrando con esto la trazabilidad de los mismos.

En la parte administrativa cada una de las oficinas regionales, se constituye como independiente, aunque únicamente en las desiciones administrativas, ya que los recursos para el funcionamiento de las mismas son suplidas por parte de la Unidad de Compras, instalada en la oficina central. En lo que respecta a la parte de recursos humanos es de igual forma, existe un Jefe responsable por la oficina regional, el cual tiene a su cargo el recurso humano y físico, para poder realizar las diferentes labores; no obstante es en la oficina central donde se encuentra el departamento de recursos humanos el cual es que verifica el trabajo de todo el personal de la Institución, además de la contratación del mismo.

3.2 DELIMITACION DE LA INVESTIGACION.

.

3.2.1 DELIMITACIÓN GEOGRÁFICA.

La delimitación del trabajo en la parte geográfica serán las oficinas con las que cuenta la organización a nivel nacional de la manera siguiente:

1. Oficina Occidental: Santa Ana, Ahuachapan, Metapan y Sonsonate.
2. Oficina Central: San Salvador, Chalatenango y La Libertad.
3. Oficina Paracentral: San Vicente, La Paz, Cabañas y Cuscatlan.
4. Oficina Oriente: La Unión, Morazán y San Miguel.

Cada una de estas oficinas tiene a su cargo un número exacto de clientes a los cuales brinda el servicio, pudiendo incrementarse este numero a partir de la solicitud de nuevos clientes, que deseen conformar una Asociación Cooperativa.

3.2.1.1 IMPACTO DE SUSPENSIÓN DE SERVICIOS

El impacto en el caso que se suspendiera los servicios en cualquiera de las regionales seria grande, ya que los clientes de cada una de las zonas tendrían que viajar distancias largas para poder ser atendidos aun en los servicios más esenciales que hasta el momento se encuentran descentralizados en las oficinas regionales. Por lo que se puede suponer que habría una disminución en la cantidad de solicitudes, basándonos en que menos clientes estarían dispuestos a viajar distancias largas para la atención a sus demandas.

En pocos años esto afectaría la organización hasta el punto en que podría, por la cantidad de clientes, cerrar sus operaciones. Sin mencionar que por el tipo de servicio que se presta a los clientes, estos se verían afectados directamente en sus empresas cooperativas, teniendo uno efecto en cadena a la economía familiar de cada uno de ellos.

En el caso de una suspensión de servicios en la oficina central; detendría todos los procesos de servicios al cliente, aun en las regionales, ya que es esta oficina donde se encuentra la base para la atención y complemento de todos los

.

servicios que la institución brinda. Por lo que la organización cerraría inmediatamente sus operaciones.

3.2.2 DELIMITACIÓN TEMPORAL.

La delimitación temporal esta dada por el tiempo en el que se ha estipulado terminar el trabajo de graduación, el cual esta determinado para una máximo de seis meses, apoyado en el Reglamento de Graduación de la Universidad Don Bosco.

Es importante mencionar que existe según el reglamentote graduación de la Universidad Don Bosco, prorrogas, pudiendo según sea el caso y la autorización debida, extender el cronograma hasta un máximo, el cual lo estipula el mismo reglamento.

3.3 DETERMINACION DE EL UNIVERSO Y LA MUESTRA.

A continuación se presenta el mapa muestral:

Departamento	Puesto	Numero de Encuestados
Administracion Superior	Presidencia	1
	Vicepresidencia	1
Juridico	Jefe del Departamento	1
Fomento y Asistencia Tecnica	Jefe del Departamento	1
Vigilancia y Fiscalizacion	Jefe del Departamento	1
Planificacion e Informatica	Tecnicos	3
Registro Cooperativo	Jefe del Departamento	1
Regional Occidente	Jefe del Departamento	1
	Asesor Cooperativo	2
	Auditor de Cooperativas	1
Regional Central	Jefe del Departamento	1
	Asesor Cooperativo	1
	Auditor de Cooperativas	1
Regional Paracentral	Jefe del Departamento	1
	Asesor Cooperativo	1
	Auditor de Cooperativas	1
Regional Oriente	Jefe del Departamento	1
	Asesor Cooperativo	1
	Auditor de Cooperativas	1

El total de encuestas realizadas es de 22, las cuales se dividieron de la siguiente forma:

- Encuesta Administrativa: Los encuestados son todas los personeros de la Institución que pertenecen a los departamentos administrativos y que utilizan los servicios de red.
- Encuesta Técnica: Los encuestados son aquellos que pertenecen al departamento de Informática y que manejan la red de datos.

Los departamentos que se muestran en la figura anterior son los que se tomaron como mapa muestral en los cuales se entrevistaron a cada uno de los Jefes de los Departamentos a excepción de las Oficinas Regionales en los cuales se entrevisto también a miembros de la Oficina, además de el Jefe Regional..

3.4 PRESENTACION DE LA INFORMACION

Antes de realizar el análisis de cada pregunta cabe mencionar que durante el proceso de Investigación para poder recavar la información debida, se crearon dos cuestionarios, uno que era puramente del área administrativa y el otro del área técnica. En el cuestionario del área Administrativa se redactaron doce preguntas, a las cuales se agregaron once más para el área Técnica.

A continuación se presentan cada una de las encuestas de la siguiente forma:

- Pregunta
- Objetivo
- Tabla de resultados
- Grafica
- Análisis

Es importante mencionar además que las encuestas tanto administrativa como técnica, se muestran en la misma pregunta, especificando donde así lo requiere, pero haciendo al final un solo análisis de las respuestas.

.

3.4.1 ENCUESTA

Pregunta 1:

¿Quiénes de su departamento tiene acceso a la red de datos?

Objetivo:

Determinar la cantidad de usuarios que tiene acceso a la red de datos y conocer los cargos que desempeñan los mismos dentro de la organización.

Cuadro de Respuestas:

Administrativa

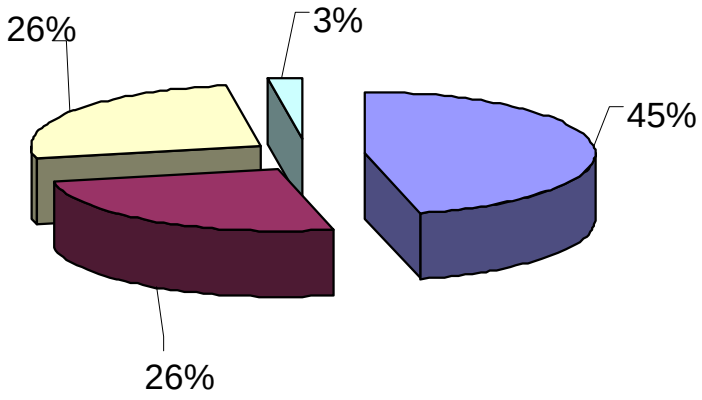
Pregunta	Respuesta	Porcentaje
Jefe	18	45%
Secretaria	10	26%
Asistente o Técnico	10	26%
Otros	1	3%

Técnica

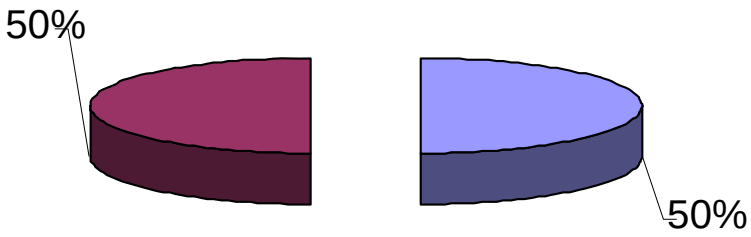
Pregunta	Respuesta	Porcentaje
Jefe	3	50%
Secretaria	0	0%
Asistente o Técnico	3	50%
Otros	0	0%

Gráfica:

Administrativa



Técnica



Análisis:

El resultado obtenido de las encuestas permite conocer que en su mayoría tanto en la parte administrativa como en la técnica, son los dirigentes de la organización los que tienen el acceso a los recursos de la red, estando los operativos en un segundo plano. Con esto podemos observar que es necesaria la determinación de políticas que permitan el desarrollo continuo del uso de la red de datos priorizando las mismas según el puesto en el cual se desempeñe.

Pregunta 2:

¿A qué tipo de servicios internos de red tiene acceso?

Objetivo:

Determinar la accesibilidad que tienen los usuarios a los diferentes servicios de red de datos.

Cuadro de Respuestas:

Administrativa

Pregunta	Respuesta	Porcentaje
Base de Datos	16	52%
Internet	15	48%
Servicios de Impresión y Compartir archivos	0	0%
Otros	0	0%

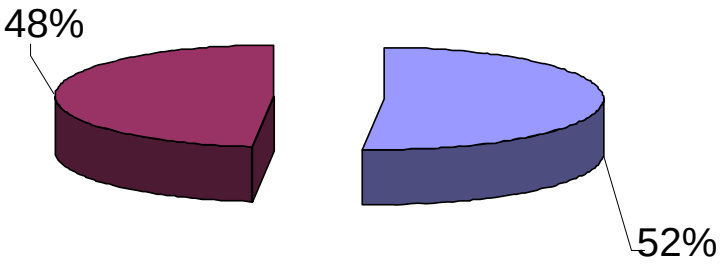
.

Técnica

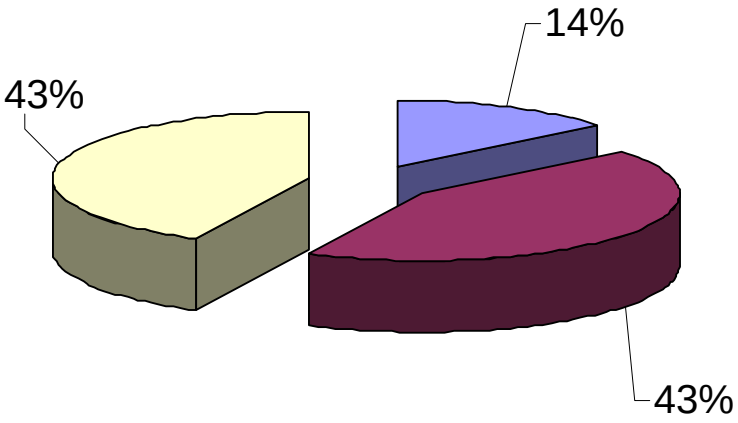
Pregunta	Respuesta	Porcentaje
Base de Datos	1	14%
Internet	3	43%
Servicios de Impresión y Compartir archivos	3	43%
Otros	0	0%

Gráfica:

Administrativa



Técnicas



Análisis:

Los datos muestran que los servicios de red de datos, a los que más tienen acceso, tanto en la encuesta administrativa como en la técnica, los usuarios son los servicios de impresión y compartir archivos y después de ese seria el Internet. Lo importante de esto es que podemos ver que es necesaria la contingencia para la continuidad de los mismos servicios, procurando que la Institución brinde los servicios correspondientes a sus clientes.

.

Pregunta 3:

¿Cuáles son los servicios internos de red que más utiliza?

Objetivo:

Conocer cuales son los servicios de red de datos que mas demandan los usuarios.

Cuadro de Respuestas:

Administrativa

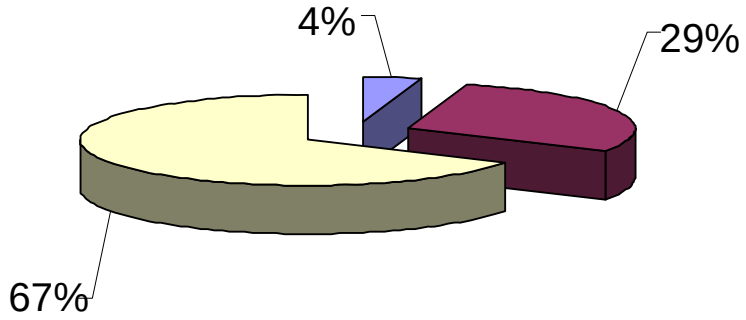
Pregunta	Respuesta	Porcentaje
Base de Datos	1	4%
Internet	7	29%
Servicios de Impresión y Compartir archivos	16	67%
Otros	0	0%

Técnica

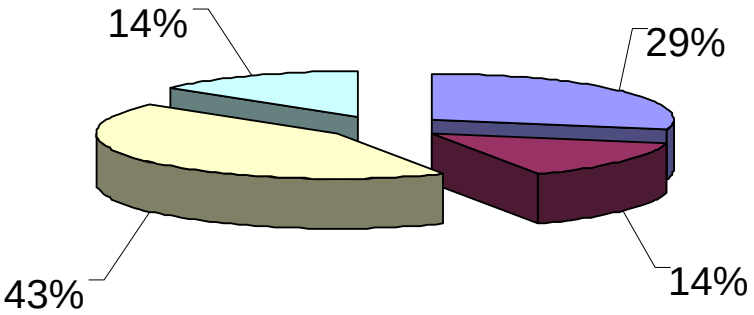
Pregunta	Respuesta	Porcentaje
Base de Datos	2	29%
Internet	1	14%
Servicios de Impresión y Compartir archivos	3	43%
Otros	1	14%

Gráfica:

Administrativa



Técnica



Análisis:

Los datos que se recolectaron a través de la encuesta muestran que el servicio de impresión y compartir archivos, dentro de los servicios de la red de datos, es el mas prioritario para la Institución, seguido de el Internet. Por lo anterior los usuarios exponen que para brindar servicios a los clientes de la Institución, necesitan prioritariamente la continuidad de la red de datos.

Pregunta 4:

¿Con qué tipos de servicios de red tiene más problemas de accesibilidad?

Objetivo:

Determinar con que servicios de red de datos los usuarios encuentran mayor dificultad en el uso de los mismos.

Cuadro de Respuestas:

Administrativa

Pregunta	Respuesta	Porcentaje
Base de Datos	4	19%
Internet	10	48%
Servicios de Impresión y Compartir archivos	7	33%
Otros	0	0%

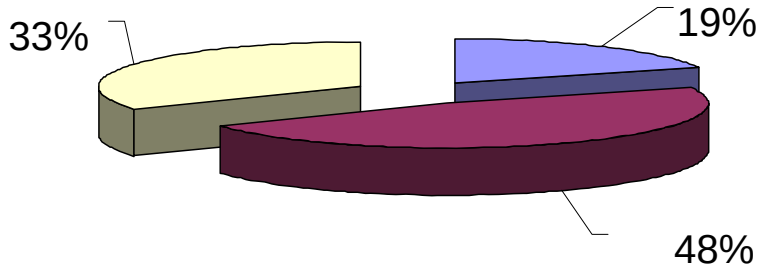
Técnica

Pregunta	Respuesta	Porcentaje
Base de Datos	2	40%
Internet	3	60%
Servicios de Impresión y Compartir archivos	0	0%
Otros	0	0%

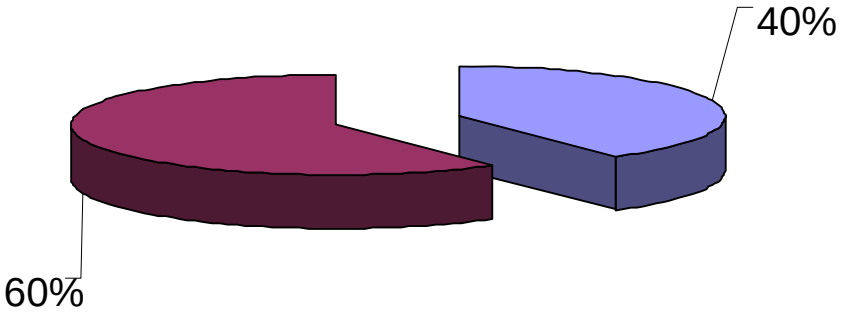
Gráfica:

.

Administrativa



Técnica



Análisis:

El resultado obtenido de las encuestas nos permite conocer que el servicio de red de datos que más problema da a los usuarios a la hora de accesarlo es el de Internet, esto se repite tanto en la encuesta administrativa como en la técnica. En la parte administrativa es importante notar, que uno de los servicios de red de datos más usados, es el de servicios de impresión y de compartir archivos, pero también este es uno de los que más problemas les genera. Por lo anterior los usuarios expresan que es imprescindible para ellos, a la hora de brindar los servicios a los clientes, el servicios de impresión y compartir archivos, con lo que muestran la importancia de tener un respaldo o procedimiento que permita el desarrollo normal de este servicio, aun y cuando existan problemas o amenazas de cualquier clase.

Pregunta 5:

¿Cuál es la causa por la que se le dificulta el acceso a los servicios de red de datos?

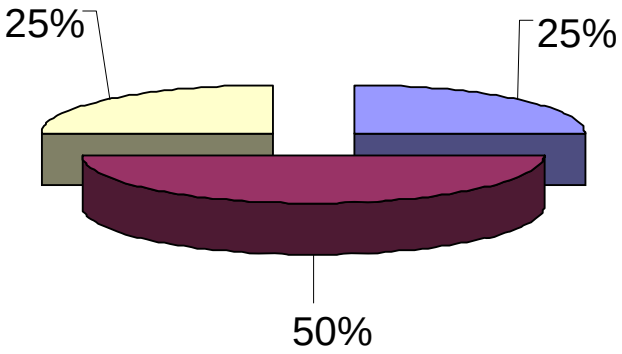
Objetivo:

Puntualizar las causas por la cuales a los usuarios, se les dificulta el hacer uso de los servicios de la red.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Equipo Informático (obsoleto)	1	25%
Conexión Lenta	2	50%
Otros	1	25%

Gráfica:



Análisis:

Según los resultados obtenidos de la encuesta el problema mas grave se encuentra en la velocidad con la cual los usuarios pueden utilizar los servicios de red, lo cual les perjudica a la hora de brindar los servicios. Además es importante mencionar que uno de los encuestados menciono que son los equipos la causa por la cual hay problemas en el acceso a la red y el otro que es el proveedor de los servicios externos el que hace difícil el acceso a los servicios de red de datos. Por lo anterior muestra que las razones principales se encuentran, en el recurso tecnológico con el que cuenta cada usuario y muestra la necesidad de tener políticas y procedimientos en dos áreas, la primera seria la cantidad de usuarios que la red de datos debe de tener lo cual depende de la velocidad del enlace con el que se cuenta, y la otra arrea, seria la actualización de los equipos informáticos, cada cierto periodo de tiempo determinado por la misma Institución.

.

Pregunta 6:

¿Cómo califica a su red de datos?

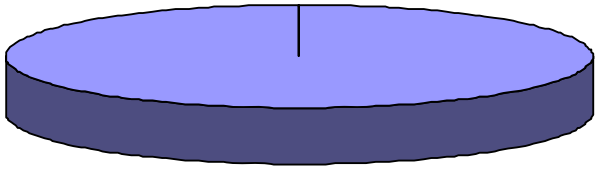
Objetivo:

Determinar la seguridad con la que cuenta el usuario en su red de datos, y la razón por la cual la considera de esa manera.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Segura	0	0%
Insegura	3	100%

Gráfica:

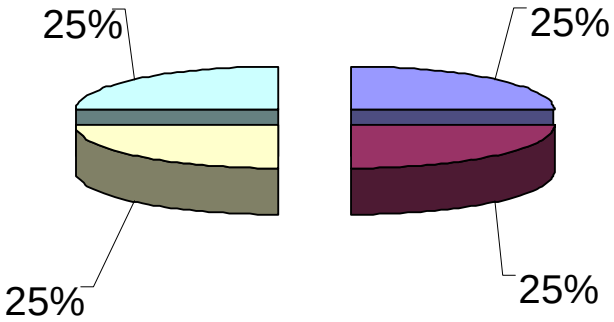


100%

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Manejo de Password	1	25%
Servicio Continuo	1	25%
Mantenimiento Adecuado	1	25%
Otros	1	25%

Gráfica:



Análisis:

Los resultados permiten conocer que todos los usuarios consideran a su red insegura y las razones son variadas. Uno de ellos agrego en otros la razón de que

.

hay vulnerabilidad de acceso por medio del Internet. Esto demuestra que los usuarios de la red de datos, actualmente no se sienten conformes con los procedimientos o políticas existentes para la seguridad en la red, y hace énfasis en la importancia que existe de mejorar o crear nuevas políticas o procedimientos que permitan un nivel más alto de seguridad.

Pregunta 7:

¿Qué tipo de amenazas tecnológicas a experimentado haciendo uso de su red de datos?

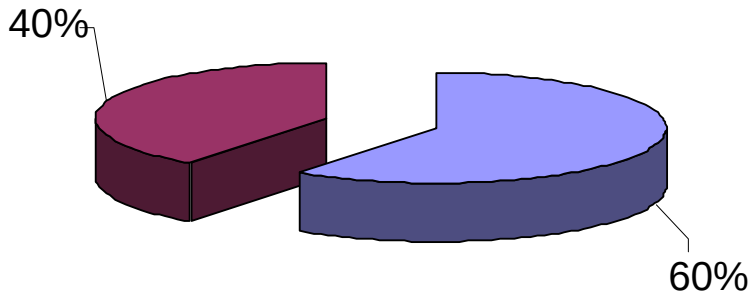
Objetivo:

Determinar cuales han sido las causas por las que el usuario ha tenido mayores dificultades, en el uso de la red de datos.

Cuadro de Respuestas:

Pregunta	Respuestas	Porcentaje
Accesos no autorizados Internos o Externos	0	0 %
Otros	0	0%
Spyware	2	40%
Virus	3	60%

Gráfica:



Análisis:

Los resultados muestran que son los Virus tecnológicos los que más han causado daños o dificultades a la red de datos y que los Spyware ocupan un segundo lugar. Por lo anterior los usuarios muestran la vulnerabilidad que tienen sus documentos o sus equipos al estar unidos a la red de datos, ya que estos pueden en cualquier momento ser infectados por amenazas tecnológicas antes descritas.

.

También los usuarios expresan la necesidad de tener en primer lugar políticas que les permitan hacer el resguardo de los documentos mas importantes y en segundo lugar de procedimientos dicten la forma en el como se actuara en el momento, en que se de uno problema de estos.

Pregunta 8:

¿Qué tipo de amenazas naturales ha experimentado que interfieren en el uso de su red de datos?

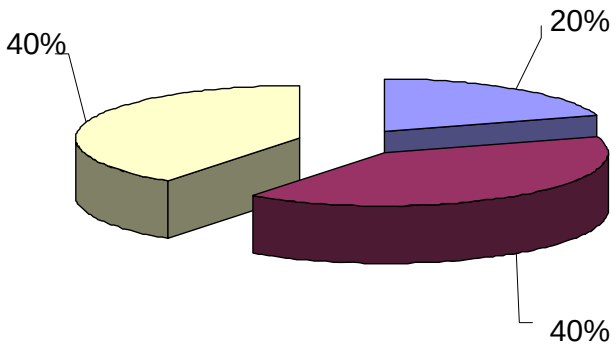
Objetivo:

Determinar las principales causas naturales, a las que la Institución se ha enfrentado y que ha impedido el desarrollo normal en el uso de la red de datos.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Terremotos	2	40%
Inundaciones	0	0%
Incendios	1	20%
Sequías	0	0%
Granizo	0	0%
Erupciones	0	0%
Otros	2	40%

Gráfica:



Análisis:

Los resultados muestran que las amenazas naturales mas frecuentes que han sucedido en la Institución son los terremotos, evitando el uso normal de los recursos de red, además de los incendios. También los usuarios comentaron en

.

otros, que las fallas en el servicio de electricidad es uno de los problemas que han experimentado dentro de la Institución. Por lo anterior es necesario que la Institución implemente una serie de medidas con las cuales puede resolver cualquiera de las amenazas que se diere en la misma. Es por ello, la importancia de crear la contingencia para prevenir cualquier desastre y que los servicios no se vean interrumpidos. Es importante mencionar que, la normas de calidad ISO, requieren de salvaguardar o contingencias para el continuo servicio a los clientes de la Institución.

Pregunta 9:

¿Qué tipo de consecuencias genera la interrupción de los servicio de su red de datos?

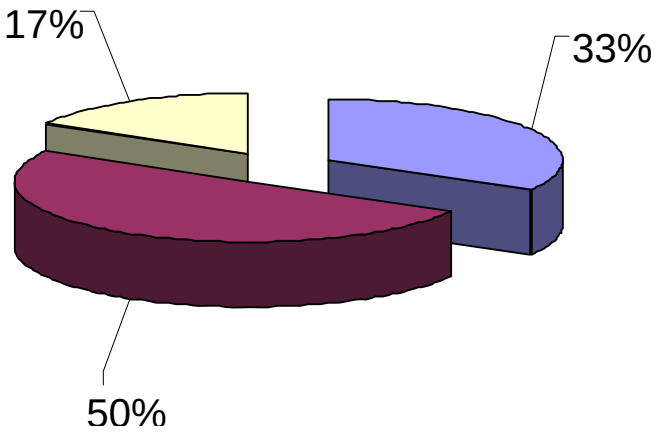
Objetivo:

Especificar los resultados que se generan a raíz de la interrupción de los servicios de la red.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Mala atención a los clientes	2	33%
Incumplimiento en el tiempo de entrega	3	50%
No cumplimiento de los procesos establecidos	1	17%
Otros	0	0%

Gráfica:



.

Análisis:

Los resultados muestran que la consecuencia principal es el incumplimiento de los tiempos de entrega de un servicio, esto es debido a que la Institución esta Certificada en normas ISO 9000:2000, lo cual exige a la misma el cumplimiento de los tiempos estipulados por cada servicio; otra de las consecuencias es que al no tener los servicios de la red disponibles, no se pueden cumplir los procesos y procedimiento establecidos para cada servicio. Esto también genera la mala atención a los clientes ya que no se pueden satisfacer a los mismos en sus demandas. Por lo que es necesario que la Institución cuente con un Plan de contingencia permitiendo tener alternativas para la atención de los clientes en todo momento.

Pregunta 10:

¿Qué ventajas se considera se obtienen al tener políticas de uso de la red de datos?

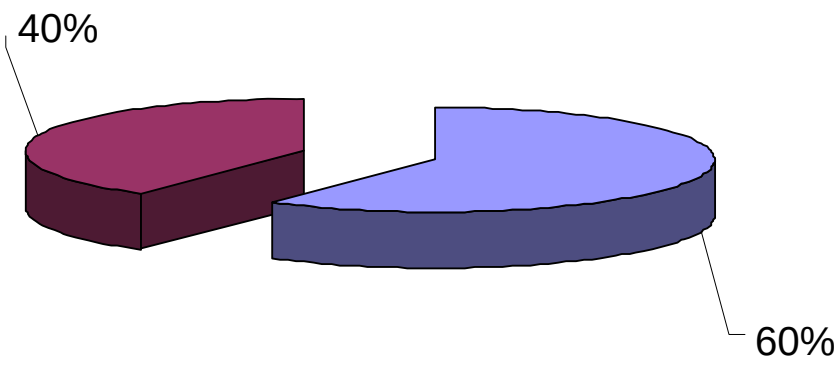
Objetivo:

Determinar la importancia de contar con las políticas y procedimientos para el uso de la red.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Seguridad	2	40%
Confiabilidad	0	0%
Control	3	60%
Otros	0	0%

Gráfica:



Análisis:

Según los resultados obtenidos en la encuesta, los usuarios consideran como ventaja principal el control, que se genera a través de tener las políticas que dicten la normativa, a la vez consideran que otra de las ventajas es la seguridad en el uso de la red de datos. Por lo que los usuarios expresan, se puede mencionar que es necesario el uso de las políticas y procedimientos para el uso de la red, dado que les genera ventajas en el trabajo que se realiza a diario.

Pregunta 11:

¿Cómo calificaría su equipo informático?

Objetivo:

Determinar el tipo de equipos de computo con lo que se cuenta en la Institución.

Cuadro de Respuestas:

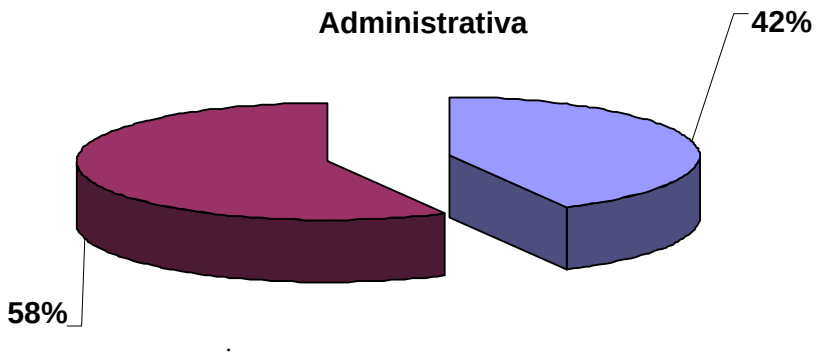
Administrativa

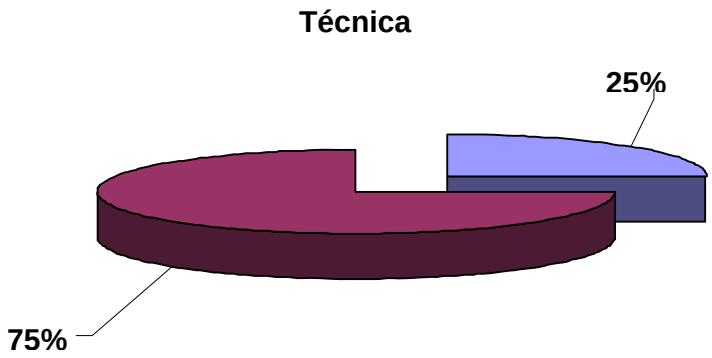
Pregunta	Respuesta	Porcentaje
Obsoleto	8	42%
Funcional	11	58%
Tecnológicamente avanzado	0	0%
Otros	0	0%

Técnica

Pregunta	Respuesta	Porcentaje
Obsoleto	0	0%
Funcional	1	25%
Tecnologicamente Avanzado	3	75%
Otros	0	0%

Gráfica:





Análisis:

El resultado obtenido de las encuestas nos hacer saber que la organización cuenta con el equipo adecuado para las funciones diarias que dicha organización presta esto tanto en la encuesta que se le paso al personal administrativo como al técnico, aunque no hay una estandarización de los equipos y en algunas localidades el equipo no es el adecuado. La encuestas muestran además que un poco menos de la mitad de los usuarios administrativos son lo que consideran su equipo obsoleto para las funciones que realiza y que afecta en el trabajo diario, por otro lado en la encuesta realizada al personal técnico la mayoría considera que su equipo es de una tecnología avanzada y la otra parte la considera funcional, para desarrollar las actividades que se le encomiendas.

Por lo anterior podemos mencionar, que los equipos de computo mas avanzados tecnológicamente se encuentran en las áreas técnicas, a la vez se muestra que la institución tiene el equipo necesario para poder brindar el servicio adecuado a los clientes. Pero también es importante mencionar que se necesitan políticas que permitan la actualización de los equipos cada cierto periodo, para que los servicios continúen brindándose en todo momento.

Pregunta 12:

¿Cómo considera su servicio de red de datos?

.

Objetivo:

Especificar la forma en que el usuario define, en relación a la continuidad, su servicio de red, en el trabajo que realiza a diario.

Cuadro de Respuestas:

Administrativa

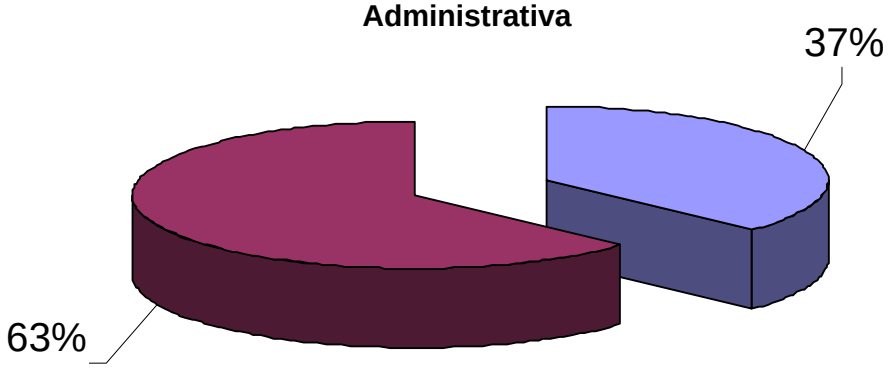
Pregunta	Respuesta	Porcentaje
Estable	7	37%
Inestable	12	63%

Técnica

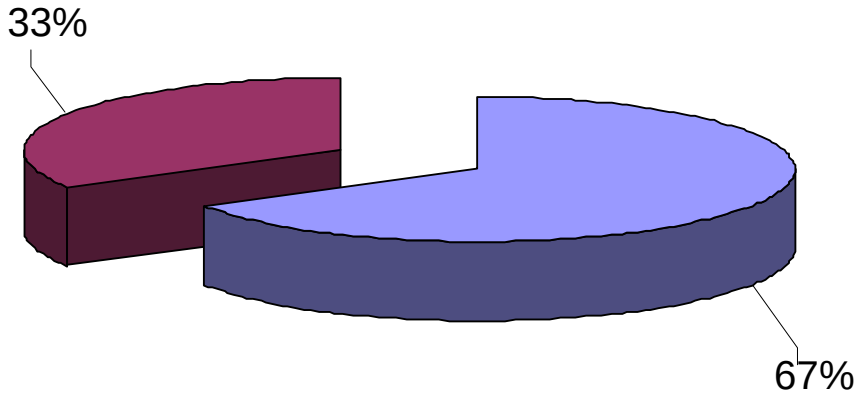
Pregunta	Respuesta	Porcentaje
Estable	2	67%
Inestable	1	33%

Gráfica:

Administrativa



Técnica



Análisis:

El resultado obtenido de las encuestas nos hace saber que dentro de la organización, la calidad de los servicios internos de la red de datos no es la más

adecuada ya que según los datos, la red es muy inestable, esto tanto para los usuarios administrativos y técnicos. Por lo que es necesario determinar los estándares mínimos y máximos en que la red de datos tendría que funcionar, ya sea estos por velocidad, ancho de banda u otros. Además es necesario identificar los momentos en los cuales la red se considera inestable y determinar la forma en la cual se prevee o resuelve dicho problema.

Pregunta 13:

¿Cuál es el promedio en un día de la semana, que se ha interrumpido su servicio de red de datos?

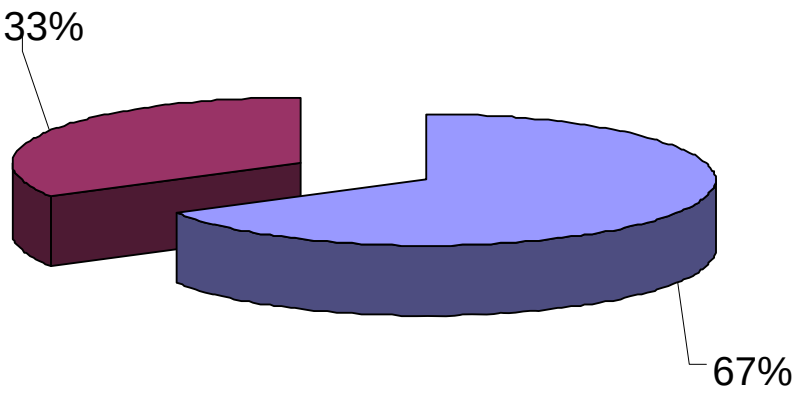
Objetivo:

Determinar la frecuencia con la cual se interrumpe el servicio de la red de datos.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
1 a 5 veces	2	67%
6 a 10 veces	1	33%
10 o mas veces	0	0%
Ninguna de las anteriores	0	0%

Gráfica:



Análisis:

Los resultados muestran que el servicio en la red de datos en un día de la semana cualquiera, falla entre una y diez veces, lo que expone la importancia que tiene el contar con la contingencia adecuada para solventar cada uno de los problemas y además muestra que es necesario realizar análisis continuos a la red

.

para determinar los problemas o posibles problemas dentro de la misma. La frecuencia con la que actualmente se dan las interrupciones, es preocupante para la Institución, ya que la razón de ser de la misma es el brindar servicios a sus cliente, por lo que es importante que la Institución cuente con las políticas y procedimientos que le permitan actuar, para evitar o solventar dichas interrupciones.

Pregunta 14:

¿Qué tipo de conexión utiliza para comunicarse en la red de datos?

Objetivo:

Determinar la forma física, por la que esta compuesta la red de datos de la Institución.

Cuadro de Respuestas:

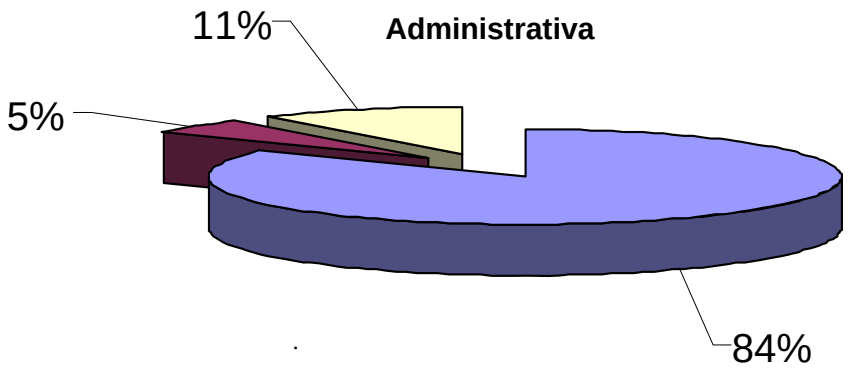
Administrativa

Pregunta	Respuesta	Porcentaje
Cable de Red	16	84%
Wireless	1	5%
Modem	2	11%
Otros	0	0%

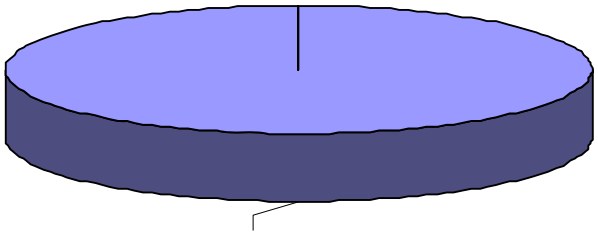
Técnica

Pregunta	Respuesta	Porcentaje
Cable de red	3	100%
Wireless	0	0%
Modem	0	0%
Otros	0	0%

Gráfica:



Técnica



100%

Análisis:

El resultado obtenido de las encuestas nos hace saber que la conexión o comunicación de los diferentes equipos informáticos de la organización se realiza a través de dos formas, y que en su gran mayoría son por medio del cable de red, en la parte administrativa, ya que en la parte técnica se realiza en su totalidad a través del cable de red. Por lo anterior es necesario establecer las políticas y procedimientos para mantener la estructura física en buen estado y además determinar en los mismos los mantenimientos periódicos, debido a la durabilidad de todo el cableado.

Pregunta 15:

¿Qué tipo de hardware cuenta, para dar seguridad a su red de datos?

Objetivo:

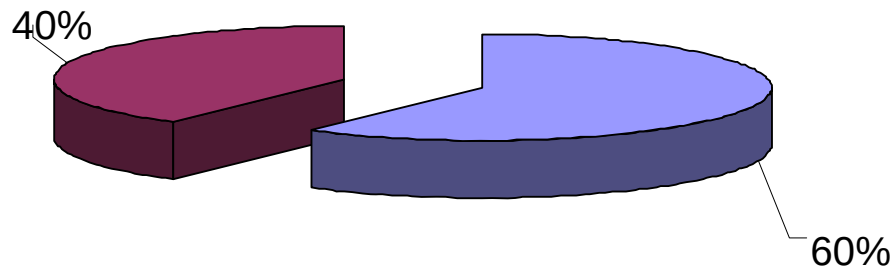
Detallar el equipo informático con el que cuenta la institución para brindar seguridad a su red de datos.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Firewall	3	60%
Router	2	40%
Otros	0	0%

.

Gráfica:



Análisis:

Los datos muestran que los recursos tecnológicos con lo que cuenta la Institución son en su mayoría Firewall y los demás son Router. Por lo anterior se puede entender que la Institución podría implementar una serie de medidas a través de estos dispositivos de red de datos brindando un nivel de seguridad el cual dependerá de la capacidad de los mismos. Es por ello la importancia, que dentro de las políticas se establezca los estándares con los que estarían configurados los equipos, para la protección de la red de datos.

Pregunta 16:

¿Qué tipo de software cuenta para evitar daños a su red de datos?

Objetivo:

Determinar las herramientas con las que cuentan los usuarios de la red de datos, para poder evitar daños a sus equipos.

Cuadro de Respuestas:

Administrativa

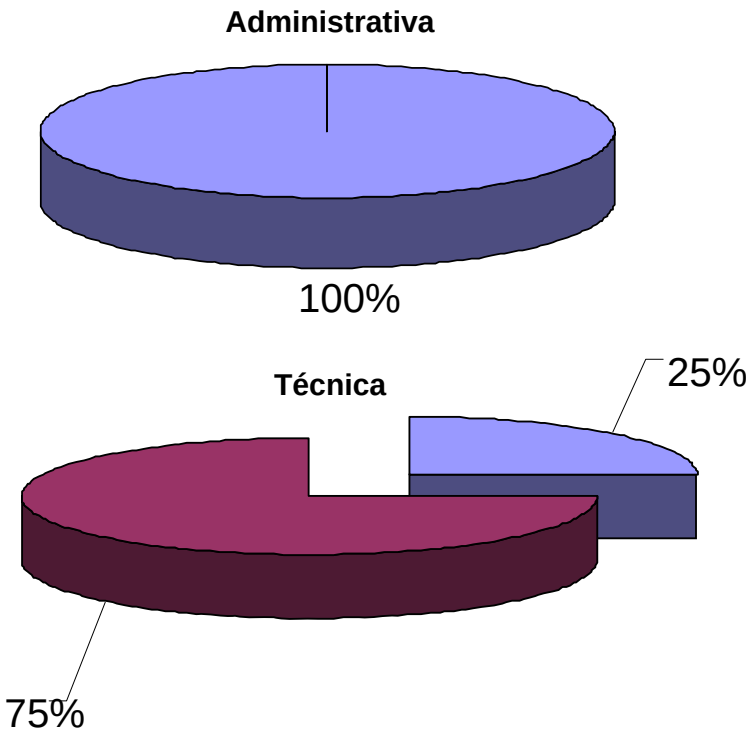
Pregunta	Respuesta	Porcentaje
Firewall	0	0%
Antivirus	19	100%
Antispyware	0	0%
Todos	0	0%

Técnica

Pregunta	Respuesta	Porcentaje
Firewall	1	25%
Antivirus	3	75%
Antispyware	0	0%
Todos	0	0%

.

Gráfica:



Análisis:

El resultado obtenido de las encuestas nos hace saber que la organización cuenta con pocas alternativas en lo que respecta a software para poder evitar cualquier ataque de un agente externo hacia dicha red de datos. Del total de encuestados todos coincidieron en que la red de datos dentro de la organización sólo tiene como protección basada en software, lo que es el antivirus, en la parte administrativa; y en la parte técnica el porcentaje sigue siempre alto ya que la mayoría considera que la única herramienta que se tiene en este caso es el Antivirus y solo un usuario dice tener el firewall como herramienta. Por lo que los usuarios expresan es necesario el poder implementar nuevas herramientas que permitan aumentar la seguridad dentro de sus equipos y que a la vez, evite los daños o posibles daños que se puedan dar en los mismos.

Pregunta 17:

¿Cada cuanto tiempo recibe mantenimiento su red de datos (hardware y software?

.

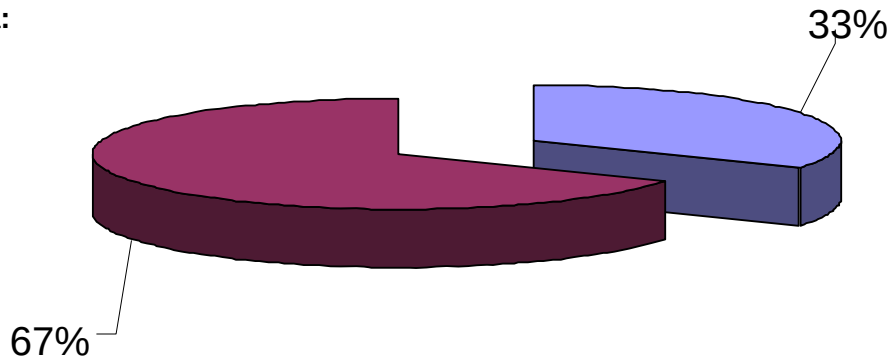
Objetivo:

Conocer la frecuencia con la cual se revisa el estado de la red de datos. Estas revisiones podrían darse a través de software o de hardware.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Mensual	1	33%
Trimestral	2	67%
Semestral	0	0%
Annual	0	0%
Ninguno	0	0%

Gráfica:



Análisis:

Los datos muestran que el tiempo en que se recibe el mantenimiento de la red de datos, es de manera trimestral en su mayoría y que algunos de estos procesos se realizan además de forma mensual.

Es importante que se tome en cuenta estos periodos en los que actualmente se realizan los mantenimientos, pero a la vez es necesario evaluar los mismos y que se determine cuales serian las mejores propuestas y que se independice e identifique los equipos informáticos que los requieren más continuos y aquellos que puedan ser más espaciados en sus periodos. Con esto se podrán crear las respectivas políticas para el mantenimiento correctivo o preventivo de los equipos.

Pregunta 18:

.

¿Conoce usted la importancia de ISO dentro de los procesos que realiza a diario?

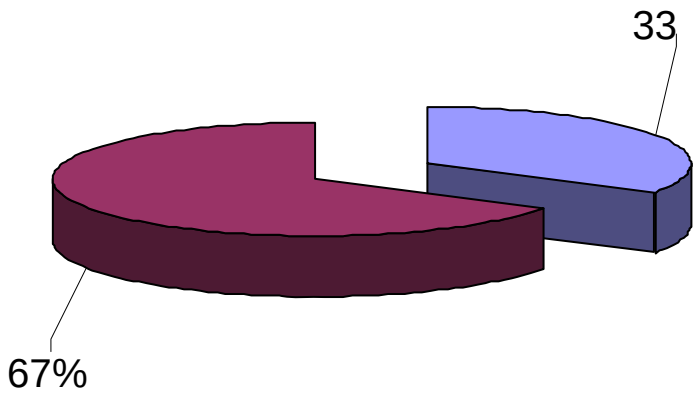
Objetivo:

Determinar la importancia, para los usuarios el contar con Normas de Calidad y el conocimiento de estos de las mismas.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Es extremadamente importante	1	33%
Es importante pero conoce poco	2	67%
No aplica ISO en su trabajo	0	0%

Gráfica:



Análisis:

Los datos muestran que la mayoría consideran importante la aplicación de la normativa ISO, en los procesos que se desarrollan a diario, pero también se puede observar que es necesario un mayor conocimiento de la normativa para poder aplicarla en el mejoramiento de los mismos procesos. La mecanización de los procesos es importante para el quehacer institucional, pero para ello también se requiere el personal se capacite en la normativa de calidad y que se puedan crear las políticas y procedimientos de cada uno de los servicios, a la ves de darlos a conocer a los usuarios.

Para una Institución que esta certificada en normas de calidad, el conocimiento de las mismas es imprescindible y mas aun cuando estas normas, tienen como lema la “mejora continua”, lo cual conlleva la aplicabilidad de las normas por parte de los usuarios, haciendo necesario que cada uno de estos tenga pleno conocimiento de los procesos.

.

Pregunta 19:

¿Cómo beneficiaria a la organización el contar con todos sus servicios online?

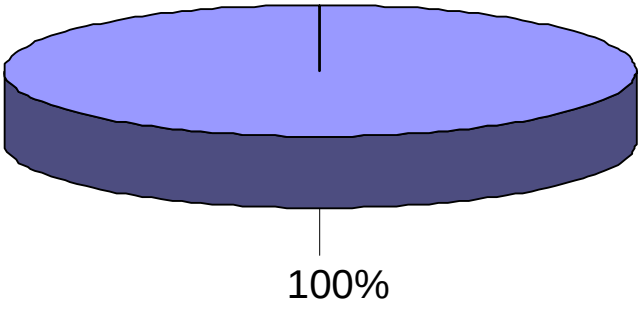
Objetivo:

Establecer el grado de importancia que tiene para el usuario, el contar con los servicios de la Institución en línea.

Cuadro de Respuestas:

Pregunta	Respuesta	Porcentaje
Altamente	3	100%
No habría diferencia	0	0%
No beneficiaría en nada	0	0%

Gráfica:



Análisis:

La encuesta revela que todos están de acuerdo en que es necesario contar con los servicios en línea para el mejor desarrollo del trabajo diario. Por lo que muestra que es necesaria la implementación del desarrollo de servicios en línea y a la vez de asegurar que estos servicios puedan será accesados por los usuarios en cualquier momento en el que este los requiera.

Es importante mencionar, que la continuidad de los servicios de red es imprescindible para los usuarios, en especial para este tipo de nuevo servicio, por lo que es necesario determinar las políticas y procedimientos para tener la respectiva contingencia y que esta sea aplicada en los momentos oportunos, según sea el caso.

.

Pregunta 20:

¿Cuál sería la importancia de tener los servicios de su red de datos las 24 horas del día los 7 días de la semana?

Objetivo:

Determinar el impacto y la importancia que tendría el ofrecer los servicios internos de red las 24 horas del día los 7 días de la semana.

Cuadro de Respuestas:

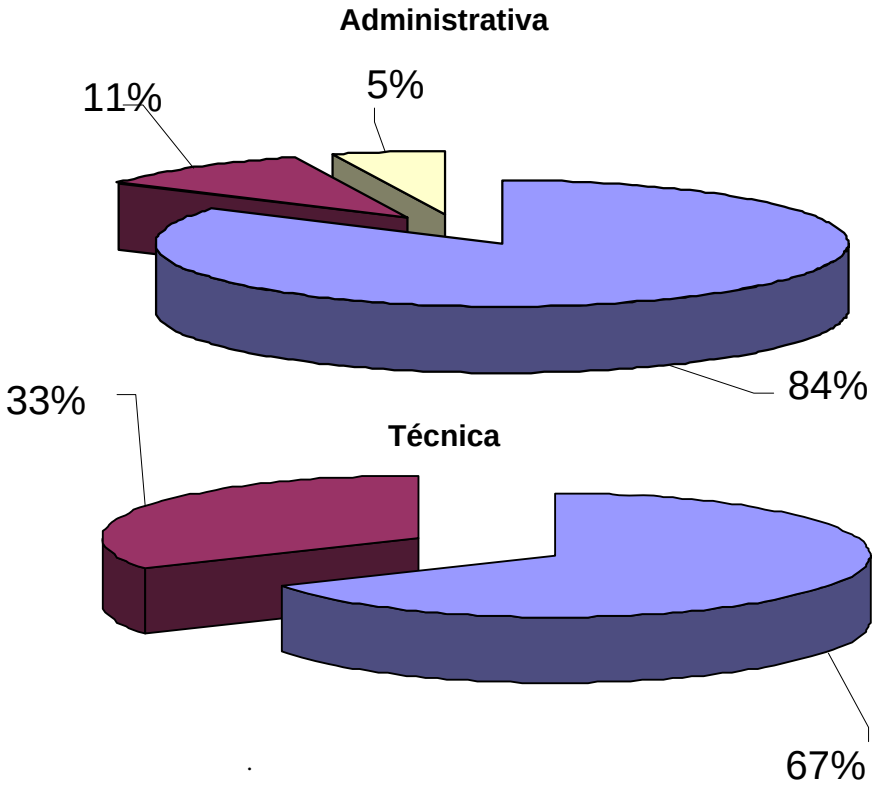
Administrativa

Pregunta	Respuesta	Porcentaje
Altamente	16	84%
No habría diferencia	2	11%
No beneficiaría en nada	1	5%

Técnica

Pregunta	Respuesta	Porcentaje
Altamente	2	67%
No habría diferencia	1	33%
No beneficiaría en nada	0	0%

Gráfica:



Análisis:

El resultado obtenido de las encuestas nos hace saber que la organización se vería beneficiada grandemente si contará con los servicios internos de red, que utiliza en sus transacciones diarias y que no se vería limitada, a solo contar con dichos servicios durante las horas hábiles. La misma opinión se pudo observar tanto en la encuesta administrativa como en la técnica. También se conoció que solo un pequeño grupo menciona que no habría diferencia en tal sentido y solo un usuario menciona que no beneficiaria en nada. Por lo anterior es necesario la implementación de los servicios las 24 horas y los 7 días de la semana, para que la institución cumpla con el lema de la normativa de calidad que es la "mejora continua". Además es importante mencionar que los usuarios de la red demandan que los servicios puedan ser accesados en cualquier momento para brindar un mejor servicio a sus clientes.

Pregunta 21:

¿Cómo beneficiaría su trabajo la mecanización de los procesos?

Objetivo:

Determinar los beneficios que se obtendrían, al implementar la mecanización de todos los servicios que ofrece el Instituto.

Cuadro de Respuestas:

Administrativa

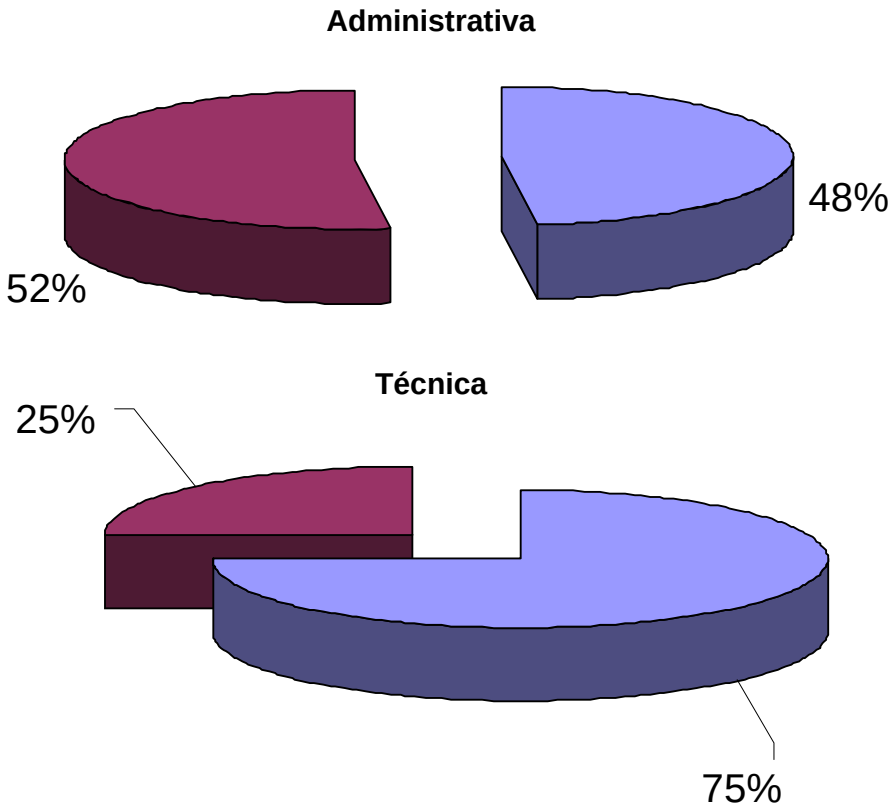
Pregunta	Respuesta	Porcentaje
Orden en la forma de realizar los procesos	13	48%
Resultados más efectivos al darse un problema	14	52%
No beneficiaría en nada	0	0%

Técnica

Pregunta	Respuesta	Porcentaje
Orden en la forma de realizar los procesos	3	75%
Resultados más efectivos al darse un problema	1	25%
No beneficiaría en nada	0	0%

.

Gráfica:



Análisis:

El resultado obtenido de las encuestas nos hace saber que la organización se vería beneficiada grandemente si contará con una mecanización de los procesos que la misma realiza para la consecución de sus objetivos. Además, demuestra firmemente que la toda la organización cree que la mecanización de los procesos los ayudaría grandemente. Del total de encuestados no hubo ninguno que se opusiera o dijera que esto no ayudaba a la organización. Por lo que es necesario crear las políticas y procedimientos, por medio de los cuales se reglamentara la mecanización de los procesos, ordenando la forma en que cada uno de ellos es aplicado en cada uno de los servicios, mejorando de esta manera la atención a los clientes.

Pregunta 22:

¿Qué tipo de servicios consulta de manera continua?

.

Objetivo:

Determinar los servicios que los usuarios utilizan con mayor frecuencia.

Cuadro de Respuestas:

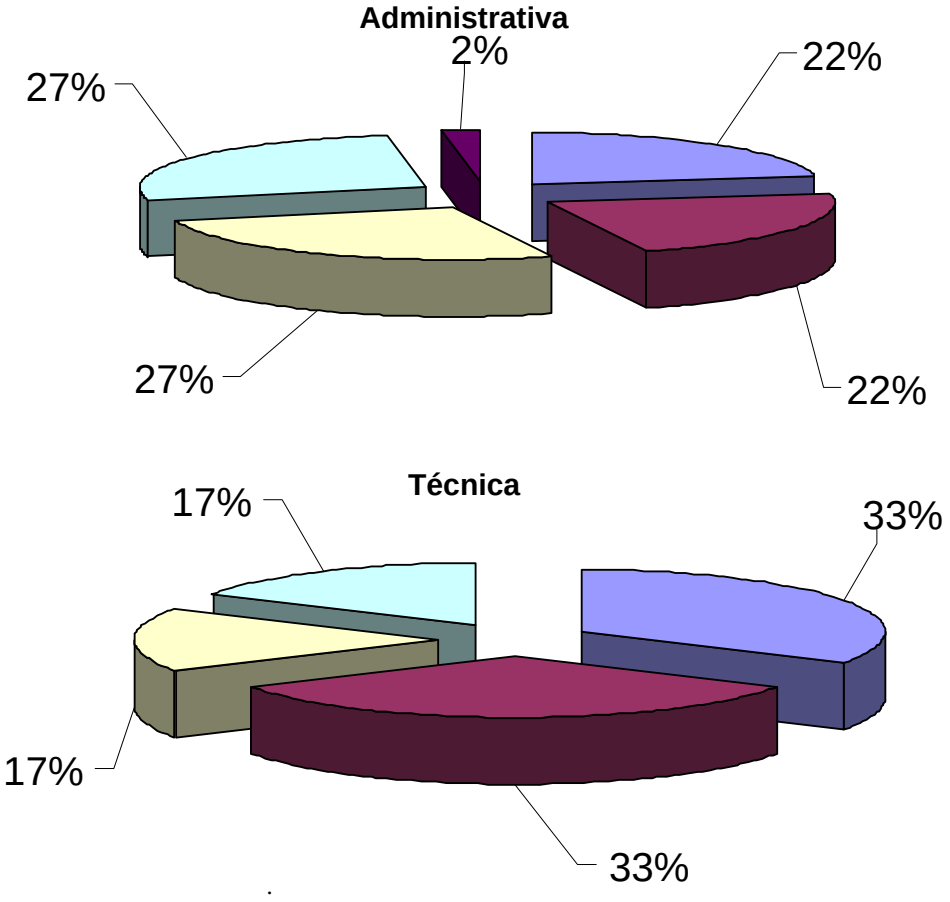
Administrativa

Pregunta	Respuesta	Porcentaje
Registro	10	22%
Jurídico	10	22%
Fiscalización	12	27%
Fomento	12	27%
Otros	1	2%

Técnica

Pregunta	Respuesta	Porcentaje
Registro	2	33%
Jurídico	0	0%
Fiscalización	2	33%
Fomento	1	17%
Otros	1	17%

Gráfica:



Análisis:

El resultado obtenido de las encuestas nos hace saber cuales son los tipos de servicios más utilizados por las personas que laboran dentro de la organización, son los del departamento de Vigilancia y Fiscalización.

Por lo anterior se puede determinar que es necesario, que se tome en cuenta la frecuencia en que los usuarios utilizan los servicios, ya que de esto depende la forma en la cual se podría implementar una futura mecanización de los mismos. Es también importante mencionar, que es imprescindible una ves implementado este servicio el contar con la red de datos en todo momento y tener a la vez las respectivas contingencia para cada uno de los posibles problemas, donde se planteen las respectivas políticas y procedimientos, según sea el caso.

Pregunta 23:

¿Qué tipo de servicios desearía tener los 7 días y las 24 horas de la semana?

Objetivo:

Determinar la demanda que los usuarios de la red tienen, en razón de la prestación de los servicios.

Cuadro de Respuestas:

Administrativa

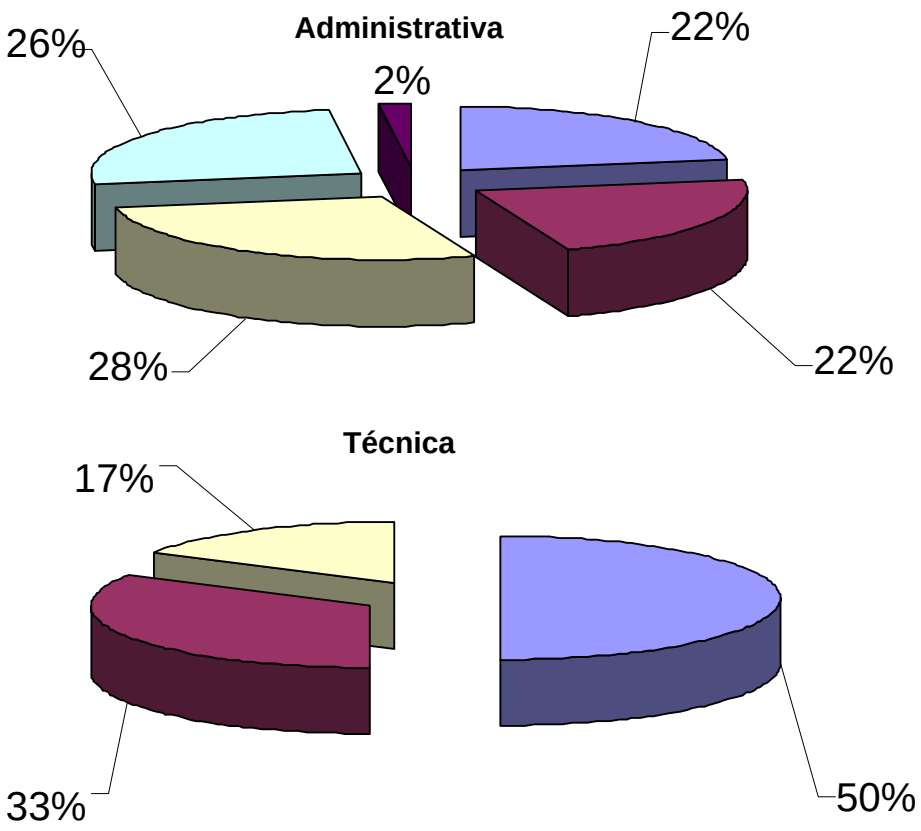
Pregunta	Respuesta	Porcentaje
Registro	12	22%
Jurídico	12	22%
Fiscalización	15	28%
Fomento	14	26%
Otros	1	2%

Técnica

Pregunta	Respuesta	Porcentaje
Registro	3	50%
Jurídico	0	0%
Fiscalización	2	33%
Fomento	1	17%
Otros	0	0%

.

Gráfica:



Análisis:

La encuesta nos permite conocer que los usuarios desearían tener la mayoría de los servicios las 24 horas al día, los 7 días de la semana, permitiendo con esto brindar un mejor servicio a sus clientes. También nos indica la necesidad que existe dentro de los usuarios de la red de datos, de poder tener un servicio de red disponible en cualquier momento y la importancia de tener contingencia en el mismo.

3.5 SITUACIÓN ACTUAL.

En la institución los servicios de la red de datos, se encuentran a disponibilidad de la mayoría de los usuarios, los cuales tienen el acceso a todos los servicios con que la red de datos dispone. No obstante es importante mencionar que las características de seguridad y de estabilidad en la red de datos no son los adecuados, dado que muchos de los problemas a los que los usuarios se enfrentan son por la falta de estas dos características de la red de datos. Cabe

mencionar que la falta de equipo de tecnología avanzada, permite que la red de datos pueda sufrir fallas o ataques, generando con esto problemas a los usuarios de la misma.

De los servicios de la red de datos que son prestados dentro de la Institución, el que es mas importante es el de impresión y compartir archivos y el de Internet, pero igualmente son los que mas problemas dan a los usuarios a la hora de accesarlos, sin determinar la forma inmediata de la solución de estos problemas.

Para una Institución, en la que la principal razón de ser es la de brindar Servicios a sus clientes, no se puede dar el lujo de la suspensión de los mismos, ni tampoco que estos sean lentos o incumplan los tiempos estimados para cada uno de los servicios según sea el caso, lo cual esta determinado por las Normas de Calidad ISO 9000:2000. Las interrupciones de los servicios ya sean estas por causas naturales o tecnológicas requieren de una solución inmediata de cómo resolver dicho problema y que la misma vaya acorde a el quehacer de la institución.

Las ventajas de contar con un plan contigencial dentro de la Institución para la red de datos descansan principalmente en la solución de problemas, el control y orden en la forma de hacer los procesos o procedimientos ya sea que estos estén dentro de la Normas de calidad o que se creen mas adelante.

La protección de la red Institucional tiene como base fundamental el Antivirus en el área de software y en la de hardware el router y firewall. Es necesario determinar la manera en la cual entran a funcionar estos dos dispositivos de red para brindar una mayor seguridad a los usuarios y evitar problemas actuales y futuros, para lo cual se hace necesaria la creación de la contingencia en cualquiera de los casos.

Por medio de la encuesta se puede mencionar que los usuarios están concientes en que la normativa de ISO, es necesaria y que ayuda a ordenar y agilizar los procesos para brindar un mejor servicio a los clientes, y que es prioritario la implementación de contar con los servicios que la institución ofrece de forma

.

continua, lo que significa las 24 horas y los 7 días de la semana, y que estos a su ves se puedan acceder a través de la red de datos.

Para que la Institución mejore en la prestación de los servicios a sus clientes es necesario, que los mismos puedan ser accesados en cualquier momento de la semana por todos sus clientes.

.

CAPITULO IV

PLAN CONTINGENCIAL

.

4.1.1 INTRODUCCION

Derivado de la importancia que tiene el Instituto Salvadoreño de Fomento Cooperativo, en brindar los servicios respectivos a las Asociaciones Cooperativas de El Salvador, y el hecho de estar preparados para responder a la variedad de circunstancias que se salgan fuera de control de las actividades normales y que afecten la integridad física de los clientes y colaboradores, así como la imagen de la Institución, se desarrolló el presente Plan de Contingencia, para cada una de las áreas criticas en donde se interrumpan las operaciones normales de la institución, debido a causas de origen natural o provocadas.

Cada uno de los planes en mención están enfocados a orientar las acciones inmediatas, de forma preventiva, así como las que habrán de realizarse durante y al finalizar la crisis, con el propósito de responder efectiva y rápidamente, minimizar los riesgos de perdidas humanas, salvaguardar los bienes y la información, así como la imagen ante publicidad negativa hacia la Institución.

El Plan consta de una parte introductoria, objetivos generales y específicos, criterios, la definición de la forma en que esta integrado el Comité de Contingencia, la enumeración de los Centros de Operaciones y un detalle de los planes, los cuales incluyen guías rápidas, las que son los pasos detallados a seguir antes, durante y después de la contingencia.

El presente Plan tiene vigencia indefinida y se estará actualizado una vez al año o cuantas veces sea necesario revisar procedimiento o agregar nuevos planes al mismo.

4.1.2 CRITERIOS

Para la ejecución de todas las acciones a realizar en los diferentes Planes de Contingencia, se deberá considerar y tomar en cuenta, atendiendo, en orden de prioridad los siguientes criterios:

.

1. La seguridad de la integridad física de los clientes y colaboradores.
2. Salvaguardar los bienes y la información, sin que por ello se ponga en peligro la integridad física de las personas.
3. Minimizar el riesgo de daño a la imagen Institucional de la Empresa y sus servicios.
4. Protección de la empresa de cualquier problema o acontecimiento, en el que se pueda ver involucrada la misma de una forma negativa.

4.1.3 OBJETIVOS

A continuación se presentan los objetivos por los cuales ha sido diseñado el Plan de contingencia:

4.1.3.1 GENERAL

1. Tomar acciones inmediatas y efectivas para minimizar los riesgos que afecten la integridad física de los clientes y colaboradores, así mismo salvaguardar los bienes de las diferentes unidades u oficinas de la Empresa y sus servicios, que pudieran derivarse de cualquiera de las contingencias enumeradas en este manual, afectando la operatoria normal de la institución y la atención al cliente.

4.1.3.2 ESPECIFICOS

1. Estandarizar y consolidar los planes de contingencia aplicables a las diferentes unidades u oficinas de la Institución.
2. Uniformizar los criterios para la toma de decisiones en situaciones de crisis.
3. Disponer de guías rápidas de acción para áreas u oficinas específicas de la Organización que permitan el reestablecimiento inmediato a la normalidad de las operaciones.
4. Llevar a cabo acciones inmediatas en búsqueda de la satisfacción de nuestros clientes (externos e internos), ante situaciones que generen publicidad negativa.

.

5. Prevenir la perdida de vidas humanas al integrar los esfuerzos de forma efectiva y rápida, en respuesta a los diferentes desastres.

4.1.4 COMITÉ DE CONTINGENCIA

4.1.4.1 INTEGRACION

El Comité de Contingencia estará compuesto por el Comité Ejecutivo del Instituto Salvadoreño de Fomento Cooperativo, en el cual se encuentra el Presidente Ejecutivo, la Vicepresidenta y los jefes de todas las áreas u oficinas de la Institución. De la misma forma será la jerarquía dentro del Comité de Contingencias estando presidido por el Presidente Ejecutivo, la Vicepresidenta y los jefes de todas las áreas u oficinas; en caso que no se encuentre los dos principales ejecutivos de la presidencia, será responsabilidad de los mismos nombrar el encargado, mientras se encuentren ausentes.

4.1.4.2 FUNCIONES Y RESPONSABILIDADES DEL COMITÉ

Inicialmente definirán el lugar donde se encontraran los centros de operaciones.

Las funciones principales realizadas por el personal a cargo del manejo de contingencias en el Centro de Operación de Contingencias incluyen:

1. Coordinar todas las actividades necesarias para implementar planes de contingencia.
2. Autoridad ejecutiva para la implementación de políticas y acciones a seguir en cada contingencia.
3. Establecimiento de prioridades.
4. Recolección de información y evaluación.
5. Evalúa el impacto de la contingencia.
6. Activar los procesos de respuesta de contingencias.
7. Coordinación de recursos.
8. Administración de los medios de comunicación.

.

9. Información al público.

4.1.4.3 FUNCIONES Y RESPONSABILIDADES DEL COORDINADOR

1. Convocar al comité.
2. Activar Centro de Operaciones.
3. Monitorear la implementación de las decisiones.
4. Establecer o determinar la existencia de contingencia y plan a seguir.
5. Crear y Ejecutar el Plan de Evacuación y otros que sean necesarios.

El coordinador debe estar en una posición desde la que pueda estar al tanto de la situación actual y manejar la operación. El Presidente Ejecutivo, es el coordinador de contingencias, en su ausencia el ejecutivo a cargo será las personas que el mismo designe, en orden jerárquico según la designación.

4.1.4.4 GRUPOS DE APOYO

Dependiendo el tipo de contingencia o evento, el comité de contingencia, coordinara la participación de los Grupos de Apoyo, los cuales se encuentran integrados por los jefes de las áreas u oficinas. Dentro de estos grupos de apoyo se encuentran:

1. Brigadas de Emergencia.
2. Comité de Seguridad.
3. Comité Evaluador.
4. Unidades de apoyo.

La integración de estos grupos y otros que se puedan crear, los conformaran los empleados de la Institución, a los cuales se les tendrá que capacitar con la finalidad de que estén preparados según el grupo de apoyo en cual estuviesen. Estarán a cargo de un Coordinador dentro de cada grupo de apoyo y dependerán directamente del Comité de Contingencia.

.

4.1.5 CENTROS DE OPERACIONES

El Centro de Operaciones de Contingencia, es un lugar diseñado para recolectar la información y realizar el análisis de contingencia. Es el lugar donde se toman las decisiones ejecutivas, relacionadas con las políticas a seguir en una situación de emergencia, lo que da como resultado la coordinación de recursos y la atención a la situación de contingencia.

4.1.5.1 UBICACIONES

A continuación se presentan las ubicaciones en las cuales funcionaran los centros de operaciones:

1. **Centro de Operaciones 1 (primario)**: Oficina Central, Calle la Mascota, Centro Comercial La Mascota, Edificio 2; San Salvador, San Salvador.
2. **Centro de Operaciones 2:** Oficina Occidental, 6º Avenida Sur, entre 17 y 19 calle poniente Nº 112; Santa Ana, Santa Ana.
3. **Centro de Operaciones 3:** Oficina Paracentral, Avenida José Maria Cornejo Nº 19; San Vicente, San Vicente.
4. **Centro de Operaciones 4:** Oficina Oriental, Avenida José Matías Delgado Nº 408; San Miguel, San Miguel.

4.1.5.2 RECURSOS

A continuación de presentan los recursos físicos que se requieren para cada uno de los centros de operaciones:

1. Teléfonos (con línea directa, móviles, fax)
2. Facilidad de mensajería
3. Facilidad de grabación de voz y video
4. Facilidad de servicios noticieros de televisión, radio y prensa
5. Acceso a Internet / correo electrónico
6. Computadora con software e impresora

7. Teléfono de conferencia (portátil)
8. Equipo de oficina (proyector, fotocopiadora, trituradora de papel, gabinetes seguros)

4.1.5.3 ADMINISTRACION Y LOGISTICA

A continuación se presenta la forma en la cual se tendrá que llevar el control de los sucesos y de todo aquello con que acontece dentro del Comité de Contingencias y demás en que dicho Comité realice.

1. Reportes y notificación de incidentes / Chequeo de reportes (check list)
2. Listados de datos de personal, comités de la Organización, jefes de áreas u oficinas, teléfonos de emergencia, comisarías PNC, ambulancias, bomberos.
3. Veinticuatro horas de acomodación
4. Planes de contingencia
5. Mapas y planos de oficinas.
6. Reloj
7. Guía telefónica
8. Medios de protección de material confidencial
9. Presupuesto de operación

4.1.6 PLAN DE MANTENIMIENTOS (EQUIPO INFORMATICO).

El plan de mantenimientos estará a cargo de la Comisión de Mantenimiento, la misma la conformaran el Jefe de Informática, el Asesor Jurídico y la Jefe de la UACI.

Será el Jefe de Informática, el encargado de presentar anualmente un cronograma en el cual se detalle las fechas y en cuales oficinas se realizara el mantenimiento, dichas fechas serán propuestas y podrán ser modificadas según

.

se requiera y se acuerde entre el Jefe de esta área y la empresa a la que se haya contratado para el mismo.

Los mantenimientos de equipo informático y de revisión de enlaces físicos de red (cableado de red interna, ejecutado por el personal técnico del departamento de informático) se realizaran en el año, como a continuación se presenta:

Fechas/Oficinas	Central	Occidental	Paracentral	Oriental
Bimestre1	Febrero Semana 3	Febrero Semana 4	Febrero Semana 4	Febrero Semana 4
Bimestre 2	Abril Semana 3	Abril Semana 4	Abril Semana 4	Abril Semana 4
Bimestre 3	Junio Semana 3	Julio Semana 4	Julio Semana 4	Julio Semana 4
Bimestre 4	Agosto Semana 3	Agosto Semana 4	Agosto Semana 4	Agosto Semana 4
Bimestre 5	Octubre Semana 3	Octubre Semana 4	Octubre Semana 4	Octubre Semana 4
Bimestre 6	Diciembre Semana 2	Diciembre Semana 3	Diciembre Semana 3	Diciembre Semana 3

Los enlaces físicos de la red, se revisaran para poder prevenir los posibles problemas ocasionados por el mismo, en caso de estar dañado de alguna manera cualesquiera de los cables o conectores, se procederá a realizar el cambio, informando al Jefe del Departamento de Informática de lo acontecido y de la solución del mismo, para que este autorice la operación y extienda la información al Jefe del área u oficina.

4.1.7 EVALUACION DE LA PROBLEMATICA

En este procedimiento se definen los pasos a seguir para activar la respuesta a la contingencia que se presente, de tal forma que arranque los diferentes planes realizados por la Institución. EL coordinador del comité de contingencias, es quien realiza este procedimiento dirigiendo al grupo de ejecutivos del comité y a los grupos de apoyo.

.

4.1.7.1 PASO 1.

El comité de contingencias debe identificar y dimensionar la contingencia o incidente que suceda considerando los siguientes criterios:

1. Interrupciones parciales, totales y temporales o continuas de las operaciones normales de la(s) unidad(es) de la Organización.
2. Daños a las instalaciones y/o activos de la empresa.
3. Daños físicos a la salud e integridad de los clientes, colaboradores y público en general que se encuentre dentro o cercano a las instalaciones de la Organización.

4.1.7.2 PASO 2.

Medición del Impacto del incidente.

1. Recabar información de la situación y crear deposito de datos
2. Hesitación de daños iniciales
3. Necesidad de atención medica
4. Evaluación de problemas críticos de los recursos (personal, transporte, servicios públicos, rutas de acceso a unidades críticas, comunicaciones, etc.)
5. Consideración de cierre controlado de unidades.

4.1.7.3 PASO 3.

Activación de Planes de Contingencia

1. Asignación a ejecutivos presentes de las funciones de las siguientes áreas: seguridad, recursos humanos y sistemas de información.
2. De acuerdo a la crisis y los problemas que se presenten, cada área operativa deberá ejecutar los planes correspondientes a su gestión:
    a. Incendios
    b. Inundaciones

c. Terremotos
d. Erupciones
e. Suspensión de Servicio (Energía Eléctrica, Comunicación).
f. Daño de Equipo
g. Violación de Seguridad de la Red de Datos
h. Asaltos y Robos (Equipo Informático)

3. Monitoreo constante de la situación y reajuste de los planes, considere sucesiones de mando, imagen de la empresa, necesidades de efectivo.

4.1.7.4 PASO 4.

Comunicación.

El coordinador de comité de contingencias es el responsable de informar oficialmente a través de los medios de comunicación sobre el status y situación de la contingencia utilizando para ello: correo electrónico, boletín impreso, correo de voz, etc.

En el caso de las comunicaciones a entidades externas, la actividad debe ser realizada por el presidente ejecutivo a través del Departamento de Comunicaciones.

El Departamento de Comunicaciones, debe elaborar un programa por separado de comunicación e información a los diferentes medios, tomando en consideración:

1. Naturaleza y gravedad de la contingencia
2. Grupos afectados

.

4.1.7.5 PASO 5.

Recuperación.

En este paso el comité de contingencias debe realizar los planes y acciones correspondientes para el retorno a las operaciones normales, considerando lo siguiente:

1. Aseguramiento de las Instalaciones.
2. Control de los equipos
3. Apertura de las áreas en instalaciones alternativas.
4. Desactivación de grupos de apoyo
5. Revisión del Impacto final
6. Revisión de los planes de contingencia
7. Administración de seguros (recuperación de activos)

4.1.8 GUÍAS

Con el propósito de que ejecutivos y jefes de departamento, puedan contar con guías rápidas de fácil utilización que les permitan responder inmediatamente a la contingencia que suceda, se diseñaron dos tipos de guías:

A. General
B. Especificas

4.1.8.1 GENERAL

Indican el procedimiento general básico a seguir en cualquier contingencia, para ejecutivos y jefes de departamento:

.

4.1.8.1.1 GUÍA GENERAL PARA EJECUTIVOS Y JEFES DE DEPARTAMENTO.

Esta guía aplica para todos los ejecutivos y jefes de departamento, incluyendo los jefes regionales de las diferentes zonas.

Para todas aquellas situaciones y/o eventos catastróficos que puedan presentarse en la organización o en el país, y que afecten o puedan afectar las instalaciones, al personal y/o a los clientes y otros dentro de la empresa, así como a la continuidad de operaciones normales, para lo cual los ejecutivos o jefes de departamentos deberán realizar el siguiente procedimiento:

Situaciones de Crisis que afecten a Toda la Organización, al País o a la Región.

1. Recabara información tan pronto como sea posible, acerca de la situación de las áreas bajo su cargo y evaluar el impacto del evento en su área u oficina.
2. Presentarse a las ubicaciones definidas como Centro de Operaciones a más tardar 60 minutos luego de sucedido el evento.
3. Si no le es posible presentarse debe llamar al Centro de Operaciones e informar de su condición y enviara a su suplente.
4. El ejecutivo o jefe de departamento en el Centro de Operaciones deberá ejecutar su plan, de acuerdo al manual de contingencias, dependiendo del tipo de contingencia.
5. El ejecutivo contactara a su grupo primario para verificar la disponibilidad del mismo, para lo que sea necesario realizar de acuerdo al plan.

4.1.8.1.2 CENTRO DE OPERACIONES.

Una vez en el Centro de Operaciones, el comité de contingencias asume la dirección y el control de la situación de Emergencias, siendo el coordinador general de las actividades para realizar los planes de contingencia el Presidente

Ejecutivo, en su ausencia el ejecutivo a cargo será de acuerdo al orden siguiente: Vicepresidente Ejecutivo, Ejecutivo designado por el Consejo de Administración de la Institución.

Situaciones de Crisis que afecten a una unidad/ grupo de unidades de la empresa.

1. El ejecutivo o jefe de departamento responsable de la operación de la unidad afectada, deberá presentarse según sea el caso, en un máximo de 60 minutos al lugar de los hechos.
2. El responsable llamara inmediatamente a los encargados de la seguridad, auditoria y seguros, para que estos se presenten en el lugar de los hechos. En caso de que algún personal de la unidad haya sufrido algún daño, el Jefe de Recursos humanos deberá presentarse a la brevedad posible.
3. El responsable coordinara, con el personal presente, la evaluación de la situación. Dependiendo del impacto de la misma coordinaran con el personal, la contingencia que se pueda llevar a cabo, para que se puedan tomar las acciones correspondientes.

4.1.8.1.3 COMUNICACIONES

El responsable o jefe de la unidad será el encargado de comunicarse con el Presidente Ejecutivo, informando según sea el caso, el evento extraordinario que ha ocurrido, utilizando para ellos lo siguientes herramientas: Correo electrónico, Celular y teléfono fijo.

4.1.8.2 ESPECIFICAS

Indican paso a paso el procedimiento básico a seguir en cada contingencia:

B-1. Incendios
B-2. Inundaciones
B-3. Terremotos

.

B-4. Erupciones Volcánicas

B-5. Suspensión de Servicio (Energía eléctrica, comunicación de datos)

B-6. Daño de Equipo Informático

B-7. Violación de Seguridad de la Red de Datos

B-8. Asaltos y Robos

4.1.8.2.1 INCENDIOS

4.1.8.2.1.1 EN LOS ALREDEDORES DE LA UNIDAD.

1. Active las brigadas de emergencia para identificar riesgos de que se incendie la unidad.
2. Avise al Presidente Ejecutivo o encargado del despacho, y a las unidades de Bomberos informando sobre el Incendio.
3. Avise a su jefe inmediato de la situación.
4. Resguardar documentos importantes si es posible de la empresa impresos, en medios magnéticos y/o deposítelos en caja fuerte si esta disponible, así como cheques, documentos importantes, etc., sin arriesgar la integridad física de las personas presentes.
5. Evalué el avance de la contingencia conjuntamente con su Jefe Inmediato y consideran la posibilidad de cambio de ubicación o cierre parcial o total de la unidad afectada.
6. Espere autorización del jefe Inmediato.
7. Implemente el Plan de evacuación.

4.1.8.2.1.2 EN LA UNIDAD

1. Active la señal de alarma audible
2. Active su brigada de emergencias para sofocar el fuego, y continué operación normal en caso de ser conato.
3. En caso de ser un conato, aislé el área y proceda a avisar a su jefe inmediato y llame a bomberos.

.

4. Si no es controlable el conato y se declara incendio, evacue la unidad de acuerdo a su Plan de Evacuación.
5. Resguarde documentos importantes de la empresa si es posible impreso o en medios magnético y/o deposítelos, si es posible, en caja fuerte si esta disponible, así como cheques, documentos importantes, etc., sin arriesgar la integridad física de las personas presentes.
6. Evalué el avance de la contingencia conjuntamente con su Jefe Inmediato y consideran la posibilidad de cambio de ubicación o cierre parcial o total de la unidad afectada.
7. Espere autorización de jefe Inmediato
8. Implemente el Plan de Evacuación.

4.1.8.2.2 INUNDACIONES.

4.1.8.2.2.1 CON UNIDAD ABIERTA.

1. Active brigadas de Emergencia.
2. Evalué daños a las personas, instalaciones y equipos.
3. Avise a el Presidente Ejecutivo o encargado del despacho, para que proceda a comunicarse con todos los ejecutivos o jefes de departamento relacionados con la contingencia (Recurso humano, responsable del área, seguridad, auditoria, seguros, etc.) y con su Jefe Inmediato para enterarlo de la situación general de su unidad.
4. Resguarde documentos importantes de la empresa si es posible impreso o en medios magnético y/o deposítelos, si es posible, en caja fuerte si esta disponible, así como cheques, documentos importantes, etc., sin arriesgar la integridad física de las personas.
5. Evalúa el avance de la contingencia conjuntamente con su jefe Inmediato y consideran posibilidad de cierre de unidad.
6. Espere autorización de jefe Inmediato
7. Implemente el Plan de Evacuación.

.

4.1.8.2.2.2 CON UNIDAD CERRADA.

1. Active Brigadas de Emergencia
2. Integre grupos de apoyo
3. Evalué daños a las instalaciones (techos, caídas de agua, drenajes, etc.)
4. Avise al Presidente Ejecutivo o encargado del despacho, para que proceda a comunicarse con todos los ejecutivos o jefes de departamento relacionados con la contingencia (Recurso humano, responsable del área, seguridad, auditoria, seguros, etc.) y con su Jefe Inmediato para enterarlo de la situación general de su unidad.
5. Proceda a evacuar la mayor cantidad de activos en los lugares que se consideren seguros, si arriesgar la integridad física de las personas.
6. Evalué conjuntamente con el Jefe Inmediato la posibilidad de abrir parcialmente la unidad.

4.1.8.2.3 TERREMOTOS

4.1.8.2.3.1 CON UNIDAD ABIERTA.

1. Active las brigadas de Emergencias.
2. Evalué daños a personas e instalaciones; en caso de heridos y/o muertos proceda de acuerdo al Plan de Contingencia de Accidentes.
3. Avise al Presidente Ejecutivo o encargado del despacho, para que proceda a comunicarse con todos los ejecutivos o jefes de departamento relacionados con la contingencia (Recurso humano, responsable del área, seguridad, auditoria, seguros, etc.) y con su Jefe Inmediato para enterarlo de la situación general de su unidad.
4. Resguardar documentos importantes de la empresa impresos o en medio magnético y/o deposítelos, si es posible, en caja fuerte si esta disponible, así como cheques, documentos importantes, etc., sin arriesgar la integridad física de las personas.

.

5. Evalúa el avance de la contingencia conjuntamente con su jefe Inmediato y consideran posibilidad de cierre de unidad.
6. Proceda a Implementar el Plan de Evacuación
7. Espere instrucciones Comité de Contingencias.

4.1.8.2.3.2 CON UNIDAD CERRADA.

1. Preséntese a su unidad a mas tardar 1 hora después de haber ocurrido el hecho; de no ser posible envié a su segundo o tercero a bordo según sea el caso.
2. Active brigadas de emergencia
3. Evalué daños a las instalaciones; sin arriesgar la integridad física de las personas.
4. Avise al Presidente Ejecutivo o encargado del despacho, para que proceda a comunicarse con todos los ejecutivos o jefes de departamento relacionados con la contingencia (Recurso humano, responsable del área, seguridad, auditoria, seguros, etc.) y con su Jefe Inmediato para enterarlo de la situación general de su unidad.
5. Evalué conjuntamente con el Jefe Inmediato la posibilidad de abrir parcialmente la unidad
6. Espere autorización del Jefe Inmediato.

4.1.8.2.4. ERUPCIONES VOLCÁNICAS.

4.1.8.2.4.1. EN LOS ALREDEDORES DE LA UNIDAD.

1. Active la alarma audible respectiva.
2. Active las brigadas de emergencia para identificar riesgos de daños en la unidad.
3. Avise al Presidente Ejecutivo o encargado del despacho, y a las unidades de Socorro informando sobre la contingencia.
4. Avise a su jefe inmediato de la situación.

.

5. Resguardar documentos importantes si es posible de la empresa impresos, en medios magnéticos y/o deposítelos en caja fuerte si esta disponible, así como cheques, documentos importantes, etc., sin arriesgar la integridad física de las personas presentes.
6. Evalué el avance de la contingencia conjuntamente con su Jefe Inmediato y consideran la posibilidad de cambio de ubicación o cierre parcial o total de la unidad afectada.
7. Espere autorización del jefe Inmediato.
8. Implemente el Plan de evacuación.

4.1.8.2.4.2 EN LA UNIDAD

1. Active la señal de alarma audible
2. Active las brigadas de emergencias para sofocar el fuego causado por la lava.
3. Aislé el área y proceda a avisar a su jefe inmediato y llame a bomberos.
4. Evacue la unidad de acuerdo a su Plan de Evacuación.
5. Resguarde documentos importantes de la empresa si es posible impreso o en medios magnético y/o deposítelos, si es posible, en caja fuerte si esta disponible, así como cheques, documentos importantes, etc., sin arriesgar la integridad física de las personas presentes.
6. Evalué el avance de la contingencia conjuntamente con su Jefe Inmediato y consideran la posibilidad de cambio de ubicación o cierre parcial o total de la unidad afectada.
7. Espere autorización de jefe Inmediato
8. Implemente el Plan de Evacuación.

.

4.1.8.2.5 SUSPENSIÓN DE SERVICIOS

4.1.8.2.5.1 ENERGÍA ELÉCTRICA.

1. Contacte al Jefe de Servicios Generales para que este proceda a arrancar planta de emergencia, asegurándose contar con suficiente combustible (su tanque debe estar lleno).
2. El Jefe de Servicios Generales o encargado de la planta, solicitara el suficiente combustible para el funcionamiento correcto de las diferentes plantas eléctricas, de las unidades, según sea el caso. Para ello tendrá en reserva la cantidad necesaria para poder llenar el tanque de la planta y solicitara el dinero necesario para poder hacer la compra de una cantidad igual, en caso de ser necesario.
3. En caso de no haber resuelto la problemática, proceda a revisar su Plan de Contingencia de Suspensión del Servicio, en el apartado de energía eléctrica.

4.1.8.2.5.2 COMUNICACIÓN DE DATOS.

1. Proceda a identificar las áreas en la cuales no se tiene la comunicación. El departamento de Informática será el encargado de evaluar y verificar la problemática, hasta volver a las operaciones normales.
2. Informe al Jefe de Informática de las áreas que no cuentan con el servicio de comunicación.
3. Recabe información acerca de la falla y los equipos que tienen esa falla.
4. Solicite la ayuda de un técnico informático para que este pueda brindar las posibles soluciones a las fallas identificadas.
5. El Jefe de Informática o el Técnico designado, consulta con los proveedores de servicios de comunicación para identificar si la falla es externa.
6. En caso de ser el enlace de red externo, proceda a cambiar el enlace de cable al enlace de cable de back up.

.

7. Indique a las unidades a que utilicen los servicios de back up, como lo son el fax, correo u otros ya identificados por el responsable de la unidad.
8. Si la falla no ha podido ser resuelta y se ha identificado que es interna, proceda a revisar el Plan de Contingencia de Suspensión de Servicio.

4.1.8.2.6 DAÑO DE EQUIPO INFORMÁTICO

1. Informe de las fallas al Departamento de Informática.
2. El departamento de Informática evalúa el daño.
3. Se procede a realizar los back up del equipo, si aplica y según sea el caso.
4. El departamento de Informática procede a retirar el equipo, e instala un equipo provisional. Dejando dentro de este la información salvaguardada en los back up.
5. En caso de que la falla pueda ser resuelta en el lugar y en corto tiempo, proceda a informar al Jefe del Departamento de Informática, para que este pueda solicitar los materiales necesarios, según sea el caso.
6. En caso de no tener equipos disponibles, se tendrá que informar al Jefe del Departamento de Informática y este a su vez al Presidente Ejecutivo para llevar a cabo la correspondiente acción, según sea el daño del equipo y la importancia de mismo.
7. Una vez terminada la identificación proceda a revisar el Plan de Contingencia de Daño de Equipo.

4.1.8.2.7 VIOLACIÓN DE SEGURIDAD DE LA RED DE DATOS

1. Proceda a informar al Jefe de Informática.
2. El Jefe de Informática o su designado, realiza una identificación de la violación acontecida en el equipo.
3. Aislé el equipo para que se puede evaluar los daños y determinar si la violación ha sido externa o interna.
4. Proceda a realizar los back up del equipo(s).

.

5. Proceda a revisar las claves de acceso a los servicios, a los cuales tiene derecho el usuario(s) respectivo(s).
6. Actualice las herramientas utilizadas para evitar las violaciones dentro de los equipos.
7. En caso de no haber resuelto la problemática, proceda a revisar el Plan de Contingencia de Violación de Seguridad de la Red de Datos, el cual se encuentra en este mismo documento en la sección de Planes de Contingencia.

4.1.8.2.8 ASALTOS Y ROBOS DE EQUIPO INFORMÁTICO

1. Avise a el Jefe de Informática, para que este proceda a comunicarse con todos los ejecutivos relacionados con la contingencia (Recursos Humanos, Auditoria, seguridad, Seguros, Jurídicos, etc.,).
2. Active su brigada de emergencia para evaluar daños a personas e instalaciones y equipo.
3. En caso de heridos y/o muertos proceda de acuerdo al Plan de Contingencias de Accidentes.
4. Espere autorización del Jefe Inmediato.
5. Implemente Plan de Evacuación de ser necesario.
6. Coordinar con el Jefe de Recursos Humanos apoyo psicológico posterior a la contingencia a colaboradores afectados emocionalmente a través de terapia de grupo y/o tratamiento individual con profesionales autorizados.
7. Evaluar perdidas materiales de colaboradores con el Jefe de Recursos Humanos.

.

4.1.9 PLANES DE CONTINGENCIA.

4.1.9.1 INCENDIOS

Plan de Contingencia del área:	INCENDIOS
Ejecutivo Responsable:	Jefe de Servicio Generales
Ejecutivo Suplente:	Designado de Presidente Ejecutivo

A. Introducción.

EL presente plan de contingencia, pretende minimizar el riesgo de incendio en las instalaciones de la Organizaron, sin embargo es aplicable a cualquier situación que presente amenaza de incendio.

B. Objetivos.

Contrarrestar lo antes posible el daño provocado a causa de un conato de incendio o incendio declarado como tal.

Proteger la vida de las personas que se encuentren cercanas y en el lugar del incendio, así como proteger los activos de la Organización.

C. Plan de Contingencias

En caso de: INCENDIO.

Realice las siguientes Actividades:

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
Incendios en los alrededores de la Unidad	1. Active brigadas de emergencia para identificar riesgo de que se incendie la unidad. 2. Avise al Jefe de Servicios Generales y a los jefes relacionados con el área u oficina, además de anunciarlo a las	Jefe del área u oficina.	Extintores

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	unidades de Bomberos. 3. Si es posible, remueva documentos importantes de la empresa impresos o en medios magnéticos y/o deposítelos en caja fuerte si esta disponible, no arriesgue su integridad física. 4. Para volver a operar normalmente, espere autorización de los ejecutivos encargados.		
Procedimiento en caso de Incendio en el área u oficina.	1. Si se cuenta con un sistema de aviso audible para emergencias, hágalo funcionar para alertar al personal. 2. Hacer uso del equipo adecuado para el caso particular (tipo de extintor, mangueras, hidrantes, arena, etc.) 3. Si es necesario, pedir ayuda a Cuerpos Especializados. Reportar dirección clara y correcta. 4. Implemente el Plan de Evacuación, de acuerdo a la estructura del edificio y rutas de evacuación. 5. Si es posible, remueva documentos importantes de la empresa, impreso o en medios magnéticos y/o deposítelos en la caja fuerte si esta disponible. NO ARRIESGUE SU INTEGRIDAD FISICA.	Jefe Responsable del área.	Señal Audible Extintores Hidrantes Bomberos Plan de Evacuación
Después del Incendio	1. Evalué los daños ocasionados, e informe al Jefe de Servicios Generales y a los Jefes relacionados al área u oficina y al Comité de Contingencia. 2. Establezca de ser necesario un mecanismo de seguridad, para la protección de los activos que se puedan rescatar, en conjunto con el Jefe de Servicios Generales y Jefes relacionados al área u oficina. 3. Recupere toda aquella información que se halla podido almacenar en los lugares seguros, como las cajas	Jefe del área u oficina responsable. Comité de Contingencia	Personal de Seguridad del área u oficina.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	fuertes, ya sean estos documentos impresos y/o magnéticos. 4. Informar a los encargados de hacer efectivos los seguros de los activos. 5. El comité de contingencia, será el encargado de presentar el informe acerca de el estado del área u oficina, para que la Institución pueda informar a los medios respectivos la forma, fecha y lugar en el cual los servicios se prestaran nuevamente, ya sea temporal o de forma permanente.		

D. Procedimiento de Retorno a Operaciones Normales.

El procedimiento que se tendrá que seguir para volver a las operaciones normales será el siguiente:

1. Informe de daños del Comité de Contingencia.
2. Verificación del equipo dañado, y evaluación del alquiler o restitución del mismo.
3. Evaluación de la necesidad de alquilar un nuevo local, verificando la necesidad de contratar los servicios de comunicación de datos.
4. Verificación de la seguridad de lo dañado o recuperado y de todo lo nuevo adquirido.
5. Determinación de cuales servicios son prioritarios para los clientes.
6. Determinación del tiempo en el cual se volverá a normalizar las operaciones en su totalidad.
7. Informe final y de planificación para volver a las operaciones normales.

.

4.1.9.2 INUNDACIONES.

Plan de Contingencia del área:	INUNDACIONES
Ejecutivo Responsable:	Jefe de Servicio Generales
Ejecutivo Suplente:	Designado de Presidente Ejecutivo

A. Introducción.

Es el plan de acción a seguir en las unidades de la organización en caso de inundaciones.

B. Objetivos.

1. Minimizar el impacto provocado por el desastre ocurrido.
2. Minimizar el daño que puede producir en la organización un desastre, como lo es la inundación.

C. Plan de Contingencias

En caso de: INUNDACION.

Realice las siguientes Actividades:

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
Inundación	1. Este alerta a la información proporcionada por lo medios de comunicación o el Comité de Contingencias. 2. Revisar las instalaciones, principalmente techos, caídas de agua, drenajes pluviales de la área u oficina, drenajes municipales (tragantes) que se encuentren alrededor o cercanos. 3. Informar al Jefe de Servicios Generales de la situación particular y a los Jefes de las áreas u oficinas.	Comité de Contingencia. Jefe de las áreas u oficinas.	Recurso Humano de la Unidad. Radios, teléfonos y bocinas.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	4. Colocar en los niveles superiores los documentos impresos y/o magnéticos de la información. 5. Si la unidad se esta inundando, de aviso al comité de contingencias y al jefe del área u oficina. 6. Considere las posibilidades de ejecutar el Plan de evacuación. 7. Evalué e informe al comité de contingencias de los daños ocasionados. 8. Si el daño es mayor, proceda según “procedimiento de daños mayores”, el cual se encuentra a continuación.		
“Procedimiento de daños mayores”.	1. Cierre la Unidad. 2. En caso de heridos y/o muertos, proceda de a informar al Comité de Contingencia y espere instrucciones. 3. Evaluación de los daños, filimación o fotografías de los daños sufridos. 4. Realizar una evaluación de los daños ocurridos a las instalaciones, medios de comunicación, personal, etc. Enviando la información al centro de operaciones de contingencia, para que se evalué el curso de las acciones a seguir. 5. Inspección de áreas que se puedan habilitar para los clientes a la mayor brevedad. 6. Recolección de todos los documentos que haya sido almacenados en cajas fuertes o en lugares a los cuales no hayan sido afectados, según sea el caso. 7. Reubicar a los colaboradores según las áreas que se puedan aperturar parcialmente para brindar los servicios,	Jefe Responsable del área. Comité de Contingencia.	Guía general para ejecutivos y Jefes de departamento. Cámaras fotográficas, videocámaras.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	previa consulta con la empresa o encargado de los seguros de los activos dañados.		

D. Procedimiento de Retorno a Operaciones Normales.

El comité de contingencia por medio de sus representantes, revisa el estado físico de las instalaciones, evaluando la situación, determina la restauración de las operaciones normales, proporcionando instrucciones especificas, según el siguiente procedimiento:

1. Informe de daños del Comité de Contingencia.
2. Verificación del equipo dañado, y evaluación del alquiler o restitución del mismo.
3. Evaluación de la necesidad de alquilar un nuevo local, verificando la necesidad de contratar los servicios de comunicación de datos.
4. Verificación de la seguridad de lo dañado o recuperado y de todo lo nuevo adquirido.
5. Determinación de cuales servicios son prioritarios para los clientes.
6. Determinación del tiempo en el cual se volverá a normalizar las operaciones en su totalidad.
7. Informe final y de planificación para volver a las operaciones normales.

4.1.9.3 TERREMOTOS.

Plan de Contingencia del área:	TERREMOTOS
Ejecutivo Responsable:	Jefe de Servicio Generales
Ejecutivo Suplente:	Designado de Presidente Ejecutivo

.

A. Introducción.

Es el plan de acción a seguir en las unidades de la organización en caso de terremotos, en la búsqueda de un retorno rápido a operaciones normales evaluando y minimizando los daños dentro de las áreas u oficinas.

B. Objetivos.

1. Minimizar el impacto provocado por el desastre ocurrido.
3. Minimizar el daño que puede producir en la organización un desastre, como lo es un terremoto.

C. Plan de Contingencias

En caso de: TERREMOTO.

Realice las siguientes Actividades:

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
Durante un terremoto.	1. Activación inmediata de sistemas audibles de plan de evacuación. 2. Activar señales de alarma para emergencia. 3. Iniciar plan de evacuación. En unidades en las que se encuentren clientes, deberán guiarlos por las salidas de emergencias más próximas, buscando mantener la calma y auxiliando a quien lo requiera, para su pronta evacuación. (Si en los simulacros ensayo salir, hágalo).	Comité de Contingencia. Jefe de las áreas u oficinas.	Recurso Humano de la Unidad. Simulacros y simulaciones. Botiquín de primeros auxilios.
Después de un terremoto.	1. Evaluar el impacto del daño. 2. Comunicarse con el comité de contingencia y jefes del área u oficina. 3. Si hay lesionados, incendios o fugas	Jefe Responsable del área.	Teléfonos celulares, radios, etc.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	pida auxilio y recurra al respectivo manual de contingencia. 4. Infórmese por la radio u otros medios de comunicación de los avisos que darán las autoridades. 5. En caso de quedar atrapado conserve la calma, trate de comunicarse con el exterior golpeando con algún objeto. 6. Evaluación del daño, informando al comité de contingencias y jefes del área u oficina. 7. Si el daño es mayor, proceda según “procedimiento de daños mayores”, el cual se encuentra a continuación.	Comité de Contingencia.	
“Procedimiento de daños mayores”.	1. Cierre la Unidad. 2. En caso de heridos y/o muertos, proceda de a informar al Comité de Contingencia y espere instrucciones. 3. Evaluación de los daños, filimación o fotografías de los daños sufridos. 4. Realizar una evaluación de los daños ocurridos a las instalaciones, medios de comunicación, personal, etc. Enviando la información al centro de operaciones de contingencia, para que se evalué el curso de las acciones a seguir. 5. Inspección de áreas que se puedan habilitar para los clientes a la mayor brevedad. 6. Recolección de todos los documentos que haya sido almacenados en cajas fuertes o en lugares a los cuales no hayan sido afectados, según sea el caso. 7. Reubicar a los colaboradores según las áreas que se puedan aperturar parcialmente para brindar los servicios,	Jefe Responsable del área. Comité de Contingencia.	Guía general para ejecutivos y Jefes de departamento. Cámaras fotográficas, videocámaras.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	previa consulta con la empresa o encargado de los seguros de los activos dañados.		

D. Procedimiento de Retorno a Operaciones Normales.

El procedimiento que se tendrá que seguir para volver a las operaciones normales será el siguiente:

1. Informe de daños del Comité de Contingencia.
2. Verificación del equipo dañado, y evaluación del alquiler o restitución del mismo.
3. Evaluación de la necesidad de alquilar un nuevo local, verificando la necesidad de contratar los servicios de comunicación de datos.
4. Verificación de la seguridad de lo dañado o recuperado y de todo lo nuevo adquirido.
5. Determinación de cuales servicios son prioritarios para los clientes.
6. Determinación del tiempo en el cual se volverá a normalizar las operaciones en su totalidad.
7. Informe final y de planificación para volver a las operaciones normales..

4.1.9.4 ERUPCIONES VOLCANICAS

Plan de Contingencia del área: ERUPCIONES VOLCANICAS
Ejecutivo Responsable: Jefe de Servicio Generales
Ejecutivo Suplente: Designado de Presidente Ejecutivo

A. Introducción.

EL presente plan de contingencia, pretende minimizar el riesgo a consecuencia de las erupciones alrededor de las instalaciones de la Organizaron.

B. Objetivos.

1. Contrarrestar lo antes posible el daño provocado a causa de la erupción de algún volcán.
2. Proteger la vida de las personas que se encuentren cercanas y en el lugar donde se de la erupción (cualquier parte de las instalaciones), así como proteger los activos de la Organización.

C. Plan de Contingencias

En caso de: ERUPCIONES VOLCANICAS.

Realice las siguientes Actividades:

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
Erupciones volcánicas en los alrededores de la Unidad	1. Active brigadas de emergencia para identificar riesgo de que afecte a la unidad. 2. Avise al Jefe de Servicios Generales y a los jefes relacionados con el área u oficina, además de anunciarlo a las unidades de Bomberos. 3. Si es posible, remueva documentos importantes de la empresa impresos o en medios magnéticos y/o deposítelos en caja fuerte si esta disponible, no arriesgue su integridad física. 4. Para volver a operar normalmente, espere autorización de los ejecutivos encargados. 5. En caso de incendios alrededor de la unidad, verifique el “plan de contingencia incendios”.	Jefe del área u oficina.	Extintores
Procedimiento en caso de que la erupción	1. Si se cuenta con un sistema de aviso audible para emergencias, hágalo funcionar para alertar al personal.	Jefe Responsable del área.	Señal Audible

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
afecte directamente las instalaciones de su unidad o oficina.	2. Hacer uso del equipo adecuado para el caso particular (tipo de extintor, mangueras, hidrantes, arena, etc.), sin arriesgar la integridad física. 3. Alejar al personal del lugar donde ha sucedido el incidente, por las emanaciones de gases perjudiciales, para salvaguardar la integridad física del mismo. 4. Solicitar ayuda a Cuerpos Especializados. Reportar dirección clara y correcta. 5. Implemente el Plan de Evacuación, de acuerdo a la estructura del edificio y rutas de evacuación. 6. Si es posible, remueva documentos importantes de la empresa, impreso o en medios magnéticos y/o deposítelos en la caja fuerte si esta disponible. NO ARRIESGUE SU INTEGRIDAD FISICA.		Extintores Hidrantes Bomberos Plan de Evacuación
Después de la Erupción.	1. Evalué los daños ocasionados, e informe al Jefe de Servicios Generales y a los Jefes relacionados al área u oficina y al Comité de Contingencia. 2. Establezca de ser necesario un mecanismo de seguridad, para la protección de todos los empleados y de ser posible los activos que se puedan rescatar, en conjunto con el Jefe de Servicios Generales y Jefes relacionados al área u oficina. 3. Recupere toda aquella información que se halla podido almacenar en los lugares seguros, como las cajas fuertes, ya sean estos documentos impresos y/o magnéticos. 4. Informar a los encargados de hacer efectivos los seguros de los activos. 5. El comité de contingencia, será el	Jefe del área u oficina responsable. Comité de Contingencia	Personal de Seguridad del área u oficina.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	encargado de presentar el informe acerca de el estado del área u oficina, para que la Institución pueda informar a los medios respectivos la forma, fecha y lugar en el cual los servicios se prestaran nuevamente, ya sea temporal o de forma permanente.		

D. Procedimiento de Retorno a Operaciones Normales.

El procedimiento que se tendrá que seguir para volver a las operaciones normales será el siguiente:

1. Informe de daños del Comité de Contingencia.
2. Verificación del equipo dañado, y evaluación del alquiler o restitución del mismo.
3. Evaluación de la necesidad de alquilar un nuevo local, verificando la necesidad de contratar los servicios de comunicación de datos.
4. Verificación de la seguridad de lo dañado o recuperado y de todo lo nuevo adquirido.
5. Determinación de cuales servicios son prioritarios para los clientes.
6. Determinación del tiempo en el cual se volverá a normalizar las operaciones en su totalidad.
7. Informe final y de planificación para volver a las operaciones normales.

4.1.9.5 SUSPENSIÓN DE SERVICIO

4.1.9.5.1 ENERGÍA ELÉCTRICA

Plan de Contingencia del área: ENERGIA ELECTRICA
Ejecutivo Responsable: Jefe de Servicios Generales
Ejecutivo Suplente: Designado de Presidente Ejecutivo

.

A. Introducción.

La contingencia a cubrir será de suministro de energía eléctrica para la organización, indicando el procedimiento a aplicar y responsables de la implementación.

B. Objetivos.

1. Mantener el suministro de corriente normal y de emergencia en las unidades de la organización.
2. Restablecimiento del suministro de corriente eléctrica, a cada una de las unidades, ya sea este por medio de plantas eléctricas de emergencia o la resolución de la falla.

C. Plan de Contingencias

En caso de: ENERGIA ELECTRICA.

Realice las siguientes Actividades:

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
Falla en el suministro de energía eléctrica (En el caso de que no se tiene planta emergente de electricidad).	1. Apague todos lo equipos de su oficina o unidad. 2. Avise al Jefe de Servicios Generales y a los jefes relacionados con el área u oficina. 3. Identifique rápidamente las áreas y el tipo de servicios que se pueden brindar a los clientes manualmente. 4. Identifique si la falla ha causado algún daño en los equipos de la institución, en caso de ser así ejecute el “plan de contingencia daño de equipo”. 5. Para volver a operar normalmente, espere autorización de los ejecutivos .	Jefe de servicios generales y jefes de áreas u oficinas.	Lámparas de encendidos automáticos y recargables.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	encargados. 6. El Jefe de Servicios Generales, verificara el motivo de la falla, de ser la misma interna, solicitara la reparación inmediata, a la unidad encargada de ello. De ser la falla externa se comunicara con la empresa que brinda dicho servicio, para verificar el porque y el tiempo en que a esta le llevara la reparación. 7. Informar al Comité de contingencia de la falla del servicio, y el porque de la misma, para que este extienda un informe a las autoridades superiores de la organización. 8. El comité de contingencia será el encargado de informar el momento exacto en el que la falla será solucionada, y los procedimientos que se seguirán en caso de que se tengan que brindar los servicios de forma manual.		
Falla en el suministro de energía eléctrica (En el caso de que si se tiene planta emergente de electricidad).	1. Apague todos lo equipos de su oficina o unidad. 2. Avise al Jefe de Servicios Generales y a los jefes relacionados con el área u oficina o al encargado del encendido de la(s) planta(s) de emergencia. 3. Espere 30 segundos para que la planta pueda restablecer el suministro. 4. Identifique si la falla ha causado algún daño en los equipos de la institución, en caso de ser así ejecute el “plan de contingencia daño de equipo”. 5. El Jefe de Servicios Generales, verificara el motivo de la falla, de ser la misma interna, solicitara la reparación inmediata, a la unidad encargada de ello. De ser la falla externa se	Jefe de servicios generales y jefes de áreas u oficinas.	Planta(s) eléctrica(s) de emergencia. Lámparas de encendido automático y recargables. Combustible, según lo requiera las planta(s) eléctrica(s).

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	comunicara con la empresa que brinda dicho servicio, para verificar el porque y el tiempo en que a esta le llevara la reparación. 6. Informar al Comité de contingencia de la falla del servicio, y el porque de la misma, para que este extienda un informe a las autoridades superiores de la organización. 7. Verifique el restablecimiento de la energía eléctrica y el apagado automático de las planta(s) eléctrica(s). 8. El Jefe de Servicios Generales será el encargado en velar por que las planta(s) eléctrica(s), tengan combustible suficiente para su funcionamiento en todo momento.		

D. Procedimiento de Retorno a Operaciones Normales.

El procedimiento que se tendrá que seguir para volver a las operaciones normales será el siguiente:

1. Informe de daños del Comité de Contingencia.
2. Verificación del equipo dañado, y evaluación del alquiler o restitución del mismo.
3. Evaluación de la necesidad de alquilar un nuevo local, verificando la necesidad de contratar los servicios de comunicación de datos.
4. Verificación de la seguridad de lo dañado o recuperado y de todo lo nuevo adquirido.
5. Determinación de cuales servicios son prioritarios para los clientes.
6. Determinación del tiempo en el cual se volverá a normalizar las operaciones en su totalidad.
7. Informe final y de planificación para volver a las operaciones normales.

.

Al existir una falla en el servicio de energía eléctrica en la unidad u oficina, si se posee las planta(s) eléctrica(s) de encendido automático, la energía se reestablecerá en un máximo de 30 segundos o en el caso de ser manual el encendido, lo que tarde el personal capacitado para poder llevar a cabo el encendido de la misma.

En el caso de no tener planta eléctrica, será el Jefe de Servicios Generales el que deberá encargarse de reestablecer el servicio, en el menor tiempo posible. Será el Comité de Contingencia el que informara, previa evaluación de los técnicos del área, el momento en el cual se podrá contar con el servicio, a la administración superior y jefes de las áreas u oficinas.

4.1.9.5.2 COMUNICACIÓN DE DATOS

Plan de Contingencia del área:	COMUNICACIÓN DE DATOS
Ejecutivo Responsable:	Jefe de Informática
Ejecutivo Suplente:	Designado del Jefe de Informática

A. Introducción.

La infraestructura de comunicaciones de la organización, esta compuesta por una red de datos externa y otra interna. En el caso de la externa, esta es brindada por una empresa externa, por lo que es esta misma la responsable del mantenimiento de dicha red externa. En el caso de la interna, es el Jefe de Informática el encargado del buen funcionamiento de la misma.

Por lo anterior se orientara mayormente la contingencia a la red interna, tomando en cuenta algunas posibilidades de fallas externas, las cuales puedan ser tratadas internamente.

.

B. Objetivos.

1. Proveer alternativas de solución que eliminen o minimicen los eventos de riesgos de una contingencia en particular prevista o no prevista, de manera que se eviten paros de las actividades y servicios esenciales de la empresa.
2. Reducir al máximo el riesgo de errores de funcionamiento en los medios de comunicación y telecomunicación.

C. Plan de Contingencias

En caso de: COMUNICACIÓN DE DATOS.

Realice las siguientes Actividades:

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
Falla de Servidor (Principal).	1. Informe al Jefe del Departamento de Informática o al designado del mismo, acerca de lo sucedido. 2. El Jefe de Informática o el designado del mismo, removerá el Servidor principal y pondrá a funcionar el servidor secundario. 3. Los técnicos revisaran el servidor dañado y realizaran primeramente un back-up de toda la información almacenada en el disco duro del mismo, actualizando la información del servidor secundario o según el último back-up con el que se cuente. 4. Se evaluara el daño y el porque del mismo, realizando un informe, para dejar constancia. 5. Si la falla presentada no puede ser solventada por el departamento de informática, se le solicitara a la empresa encargada de realizar los mantenimientos de los equipo	Jefe de Informática.	Servidor Secundario. Back-up's recientes.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	informáticos, que se hagan presentes en la institución, para que estos puedan determinar el motivo de la falla. 6. En caso de poderse reparar, se procederá bajo autorización del Jefe del departamento de Informática, de no ser posible se procederá a solicitar las herramientas software o hardware necesarios. 7. Cuando se tenga reparado el servidor principal, se instalara de nuevo el mismo, no sin antes actualizar la información con la que se encuentra en el servidor secundario.		
Falla de Servidor Principal y Secundario.	1. Informe al Jefe del Departamento de Informática o al designado del mismo, acerca de lo sucedido. 2. El Jefe del departamento de Informática informara inmediatamente al Comité de Contingencia para que este pueda llevar a cabo las medidas necesarias para la prestación del servicio. 3. El Jefe de Informática o el designado del mismo, removerá el Servidor principal. 4. El jefe del departamento de Informática o designado del mismo, tendrá una maquina alternar con Sistemas operativos de forma opcional, para que se pueda elegir, con cual se quiere que funcione. Esta maquina se iniciara de tal manera que pueda funcionar como un servidor para poder reestablecer los servicios lo antes posible. 5. Los técnicos revisaran el o los servidor(es) dañado(s) y realizaran primeramente un back-up de toda la información almacenada en el disco duro del mismo y actualizaran el	Jefe de Informática. Técnicos Informáticos.	Una Pc, actualizada con Sistemas Operativos opcionales. Back-up's recientes.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	servidor provisional con la dicha información. 6. Se evaluara el daño y el porque del mismo, realizando un informe, para dejar constancia. 7. Si la falla presentada no puede ser solventada por el departamento de informática, se le solicitara a la empresa encargada de realizar los mantenimientos de los equipo informáticos, que se hagan presentes en la institución, para que estos puedan determinar el motivo de la falla. 8. En caso de poderse reparar, se procederá bajo autorización del Jefe del departamento de Informática, de no ser posible se procederá a solicitar las herramientas software o hardware necesarios. 9. Cuando se tenga reparado el servidor principal, se instalara, no sin antes actualizar la información con la que se encuentra en el servidor provisional, el cual pasara a ser servidor secundario hasta que este pueda volver a trabajar normalmente.		
Falla en la red interna de datos.	1. Informe al Jefe del Departamento de Informática o al designado del mismo, acerca de lo sucedido. 2. El Jefe de Informática o el designado del mismo, asignara a un técnico para que realice las evaluaciones que se realizaran según sea el caso. 3. El técnico proveerá de las posibles soluciones al Jefe del departamento de Informática, para que pueda ejecutar la más recomendable. 4. Si la falla se da por daño físico de un cable o conector, se procederá a hacer	Jefe de Departamento de Informática Jefe de áreas u oficinas	Cable para red de datos. Conectores RJ-45.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	el cambio del mismo. 5. Si el daño ha sido en la configuración de una maquina, se procederá a evaluar la falla y a repararla, de ser necesario configurando internamente la maquina, nuevamente.		
Falla externa de la red de datos.	1. Informar al Jefe del Departamento de Informática o designado del mismo. 2. Informar a la empresa que presta dicho servicio de lo acontecido para que se realice la evaluación del caso. 3. El Jefe de Informática o designado del mismo, realizara el cambio del servicio principal (cambio de cable físico), al secundario, o en su defecto se encenderá el MODEM, ya sea este en la oficina o cualquier regional. 4. Se realizara un informe de la falla y se documentara dentro del departamento de Informática. 5. En el caso de ser una oficina regional, donde se registro la falla será el encargado de la misma, el que tendrá que firmar el informe y la forma en que soluciono la falla, conjuntamente con el Jefe del departamento de Informática o designado del mismo.	Jefe del Departamento de Informática. Jefe del área u oficina.	Cable de servicio primario de red externa. Cable de servicio secundario de red externa. Línea telefónica y MODEM.
Falla de Equipo de Red (Propio).	1. Informar al Jefe del Departamento de Informática o designado del mismo. 2. El Jefe de Informática o designado del mismo, realizara el cambio del equipo de tal manera, que el servicio se interrumpa el menor tiempo posible (el nuevo hardware tendrá que haber sido configurado y actualizado con anterioridad, para que este al ponerlo pueda funcionar de la mejor manera posible). 3. Se realizara un informe de la falla y se	Jefe del Departamento de Informática.	Router, Hub o Swicth.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	documentara dentro del departamento de Informática. 4. En el caso de ser una oficina regional, donde se registro la falla será el encargado de la misma, el que tendrá que firmar el informe y la forma en que soluciono la falla, conjuntamente con el Jefe del departamento de Informática o designado del mismo.		
Falla de Equipo de Red (en calidad de préstamo, departe de la empresa que brinda el servicio).	1. Informar al Jefe del Departamento de Informática o designado del mismo. 2. Informar a la empresa que presta dicho servicio de lo acontecido para que se realice la evaluación del caso, e inmediatamente la misma proceda a realizar el cambio del equipo, el cual deberá estar previamente configurado por dicha empresa. 3. El Jefe de Informática o designado del mismo, realizara el cambio de equipo principal al secundario, de no tener otro equipo, se procederá conforme al Plan de contingencia de comunicación de datos, en su apartado de falla de red externa o interna, según sea el caso. 4. Se realizara un informe de la falla y se documentara dentro del departamento de Informática. 5. En el caso de ser una oficina regional, donde se registro la falla será el encargado de la misma, el que tendrá que firmar el informe y la forma en que soluciono la falla, conjuntamente con el Jefe del departamento de Informática o designado del mismo.	Jefe del Departamento de Informática.	Router o Hub.

.

D. Retorno a Operaciones Normales.

El procedimiento que se tendrá que seguir para volver a las operaciones normales será el siguiente:

1. Informe de daños del Comité de Contingencia.
2. Verificación del equipo dañado, y evaluación del alquiler o restitución del mismo.
3. Evaluación de la necesidad de alquilar un nuevo local, verificando la necesidad de contratar los servicios de comunicación de datos.
4. Verificación de la seguridad de lo dañado o recuperado y de todo lo nuevo adquirido.
5. Determinación de cuales servicios son prioritarios para los clientes.
6. Determinación del tiempo en el cual se volverá a normalizar las operaciones en su totalidad.
7. Informe final y de planificación para volver a las operaciones normales..

4.1.9.6 DAÑO DE EQUIPO INFORMATICO.

Plan de Contingencia del área:	DAÑO DE EQUIPO INFORMATICO
Ejecutivo Responsable:	Jefe de Informática
Ejecutivo Suplente:	Designado de Jefe de Informática.

A. Introducción.

El presente documento muestra los mecanismos preventivos y correctivos para hacer frente a este tipo de contingencia con variantes el tiempo y tipo de falla.

B. Objetivos.

1. Proporcionar una metodología eficaz de cómo asegurar la continuidad en la prestación de los servicios a los clientes externos o internos.

.

2. Proteger la información que se encuentra almacenada en los diferentes equipos que pertenecen a la institución y por medio de la cual se pueden brindar los servicios.

C. Plan de Contingencias

En caso de: DAÑO DE EQUIPO INFORMATICO

(Cualquier evento que afecte a los equipos informáticos, por medio de los cuales se brindan los servicios).

C.1 Prevención.

Observe las siguientes medidas preventivas de seguridad, para reducir eficazmente la exposición a cualquier tipo de desastres:

1. Ubicar impresoras de servicio común lejos de los CPU. Se reduce el número de personas que ingresan a los centros de cómputo, minimizando la posibilidad de accidentes o sabotajes.
2. Los centros de cómputo o PC, deben ubicarse en lugares lejanos a tuberías de agua o gas que pongan en peligro los equipos.
3. Los centros de computo no deben estar ubicados en sótanos un en áreas de fácil acceso para cualquier persona.
4. Sistemas automáticos contra incendios. Se activan automáticamente al detectar humo o fuego; no es necesario que haya personas presentes para que funcionen.
5. Usar extintores de Halon u otro químico que no cause daño al equipo eléctrico.
6. Realizar mantenimiento frecuente de los extintores para asegurarse que contiene carga y que funcionen bien.
7. Asegurar de contar con equipos ambientales, de protección eléctrica, alarmas, planta eléctrica de emergencia y prohibiciones visibles de comer, fumar, beber, etc.
8. Retirar todo el material inflamable de las cercanías a los CPU.

.

9. Utilizar amueblados de material no combustible dentro de los centros de cómputo.
10. Usar cableado estructurado para tener un mejor control sobre los enlaces de red. Los concentradores deben colocarse en zonas protegidas para evitar que queden accesibles a cualquier persona.
11. Diseñas procedimientos escritos de back-up y restauración. Realizar verificación de salvado.
12. Contratar bóvedas se seguridad externas al o los centros de computo para almacenar los back-up. También se recomiendan bóvedas para los materiales y equipos de respaldo.
13. Instruir a los empleados de nuevo ingreso acerca de las medias de seguridad del personal y para los equipos de computación dentro de la organización acerca del uso de equipos preventivos.
14. Realizar prácticas frecuentes de los procedimientos de seguridad durante un percance, y de las medidas de recuperación después de este.
15. En el caso del software, es conveniente mantener activa una bitácora de actividades en la cual se pueda reflejar la información estadística del desempeño de los equipos.
16. Ejecutar medidas de cambio de password periódico y diseñar estándares de manejo de estos password.
17. Nombrar un encargado por cada una de las oficinas regionales de la Institución, dentro del Departamento de Informática, y una persona que lo apoye al mismo perteneciente a estas oficinas, para que este lo pueda apoyar en emergencias. Ambos deben contar con medios de localización inmediata.
18. Aplicar medidas estándar en la compra de hardware en todas las instalaciones, coordinando con el responsable.
19. Cada unidad operativa y administrativa debe contar con un plan de recuperación.

.

En caso de daño de equipo informático realice las siguientes actividades:

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
Daño de equipo	1. Informe al Jefe del Departamento de Informática o al designado del mismo, acerca de lo sucedido. 2. El Jefe de Informática o el designado del mismo, removerá el equipo y pondrá a funcionar el equipo secundario. 3. Los técnicos revisaran el equipo dañado y realizaran primeramente un back-up de toda la información almacenada en el disco duro del mismo, actualizando la información del equipo secundario. 4. Se evaluara el daño y el porque del mismo, realizando un informe, para dejar constancia. 5. Si la falla presentada no puede ser solventada por el departamento de informática, se le solicitara a la empresa encargada de realizar los mantenimientos de los equipo informáticos, que se hagan presentes en la institución, para que estos puedan determinar el motivo de la falla. 6. En caso de poderse reparar, se procederá bajo autorización del Jefe del departamento de Informática, de no ser posible se procederá a solicitar las herramientas software o hardware necesarios. 7. Cuando se tenga reparado el equipo principal, se instalara de nuevo el mismo, no sin antes actualizar la información con la que se encuentra en el equipo secundario.	Jefe de Informática.	Equipo Secundario. Back-up's recientes.

.

D. Retorno a Operaciones Normales.

El procedimiento que se tendrá que seguir para volver a las operaciones normales será el siguiente:

1. Informe de daños del Comité de Contingencia.
2. Verificación del equipo dañado, y evaluación del alquiler o restitución del mismo.
3. Evaluación de la necesidad de alquilar un nuevo local, verificando la necesidad de contratar los servicios de comunicación de datos.
4. Verificación de la seguridad de lo dañado o recuperado y de todo lo nuevo adquirido.
5. Determinación de cuales servicios son prioritarios para los clientes.
6. Determinación del tiempo en el cual se volverá a normalizar las operaciones en su totalidad.
7. Informe final y de planificación para volver a las operaciones normales..

4.1.9.7 VIOLACION DE SEGURIDAD DE LA RED DE DATOS

Plan de Contingencia del área:	VIOLACION DE SEGURIDAD DE LA RED DE DATOS.
Ejecutivo Responsable:	Jefe de Informática
Ejecutivo Suplente:	Designado de Jefe de Informática

A. Introducción.

EL presente plan de contingencia, pretende minimizar el riesgo a consecuencia de la violación de seguridad, que se pueda dar específicamente en los sistemas informáticos u otros software relacionados al área.

.

B. Objetivos.

1. Prevenir la violación de seguridad que se pueda dar en los sistemas informáticos u otros software relacionados a esa área.
2. Proteger la información que se encuentra almacenada en los equipos informáticos de la institución.

C. Plan de Contingencias

En caso de: VIOLACION DE SEGURIDAD DE LA RED DE DATOS

Realice las siguientes Actividades:

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
Violación de Seguridad de los Sistemas o equipos Informáticos.	1. Informe al Jefe del Departamento de Informática o designado del mismo, de lo acontecido. 2. Evalué y examine el equipo donde se ha dado el suceso. Realice un back-up de la información que se encuentre en ese equipo, y proceda a revisar el mismo. 3. Establezca las posibles causas de la violación y describa el tipo de violación que se ha dado (interna o externa). La violación interna se realizaría por otro usuario al que no este asignado el equipo y la externa por un usuario no autorizado dentro de la institución. También revise en que sistema o sistemas se ha dado el suceso. 4. Realice un informe de todo lo acontecido, el tipo de violación, usuario, equipo y otros que puedan ayudar a que este tipo de sucesos no se vuelvan a repetir, enviándolo al Jefe de Informática y jefe del área u oficina.	Jefe del Departamento de Informática.	Programas de Antivirus. Programas de recuperación de información.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	5. Las contraseñas tendrán que ser cambiadas en término estipulado por el Jefe del Departamento de Informática, para que se minimice el riesgo de violaciones en los sistemas. Si la causa de la violación se debió a que descifraron o obtuvieron una contraseña, el Jefe del Departamento de Informática o designado del mismo, deberá cambiar inmediatamente todas las demás contraseñas de los usuarios dentro de la red interna.		

D. Retorno a Operaciones Normales.

El procedimiento que se tendrá que seguir para volver a las operaciones normales será el siguiente:

1. Informe de daños del Comité de Contingencia.
2. Verificación del equipo dañado, y evaluación del alquiler o restitución del mismo.
3. Evaluación de la necesidad de alquilar un nuevo local, verificando la necesidad de contratar los servicios de comunicación de datos.
4. Verificación de la seguridad de lo dañado o recuperado y de todo lo nuevo adquirido.
5. Determinación de cuales servicios son prioritarios para los clientes.
6. Determinación del tiempo en el cual se volverá a normalizar las operaciones en su totalidad.
7. Informe final y de planificación para volver a las operaciones normales.

.

4.1.9.8 ASALTOS Y ROBOS (EQUIPO INFORMÁTICO).

Plan de Contingencia del área:	ASALTOS Y ROBOS (Equipo Informático)
Ejecutivo Responsable:	Jefe de Informática
Ejecutivo Suplente:	Designado de Presidente Ejecutivo

A. Introducción.

Para contrarrestar y prevenir el aumento de la delincuencia se crearon instrucciones especiales al personal en general, designando pasos a seguir por el mismo, en cuanto a la protección de equipos informáticos que les haya sido asignado.

B. Objetivos.

1. Prevenir el impacto provocado por el asalto o robo de equipo informático de cualquier área u oficina.
2. Neutralizar las posibilidades de la suspensión del servicio por este tipo de contingencia, además de salvaguardar vidas humanas y la información con la que cuenta la Institución.

C. Plan de Contingencias

En caso de: ASALTO O ROBO DE EQUIPO INFORMÁTICO.

Realice las siguientes Actividades:

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
Robo o Asalto de equipo informático.	1. Activar las alarmas audibles, sin arriesgar la integridad física. 2. Avisar a las fuerzas de seguridad	Comité de Seguridad.	Alarmas Audibles.

.

Contingencia o Riesgo	Actividad a Realizar	Responsable	Recursos
	pública. 3. Avisar inmediatamente al Jefe de área u oficina, Jefe del Departamento de Informática y al Comité de Seguridad. 4. Avisar a la encargada de los seguros de los equipos. 5. Avise a la unidad de auditoria. 6. El jefe del área u oficina realizara un informe de todo lo acontecido y el equipo que ha sido extraído. 7. El departamento de Informática tendrá que instalar inmediatamente la situación se halla controlado, el equipo necesario para poder continuar con las operaciones normales, siempre que el daño no sea mayor al equipo secundario disponible. 8. Si no se tiene el equipo necesario para poder cubrir el robado, se tendrá que evaluar cuales son las áreas prioritarias para poder realizar la instalación del equipo secundario en dichas áreas.	Jefe de las áreas u oficinas. Jefe del Departamento de Informática. Comité de Contingencias.	Seguros de Equipos Informáticos. Equipos Informáticos Secundarios

D. Retorno a Operaciones Normales.

El procedimiento que se tendrá que seguir para volver a las operaciones normales será el siguiente:

1. Informe de daños del Comité de Contingencia.
2. Verificación del equipo dañado, y evaluación del alquiler o restitución del mismo.
3. Evaluación de la necesidad de alquilar un nuevo local, verificando la necesidad de contratar los servicios de comunicación de datos.
4. Verificación de la seguridad de lo dañado o recuperado y de todo lo nuevo adquirido.

.

5. Determinación de cuales servicios son prioritarios para los clientes.
6. Determinación del tiempo en el cual se volverá a normalizar las operaciones en su totalidad.
7. Informe final y de planificación para volver a las operaciones normales.

El comité de seguridad y el Jefe de Informática, evaluaran la situación y darán un informe al Comité de Contingencias, en relación de lo acontecido. En el momento que se considere que se haya superado en su totalidad la situación existente, se darán las instrucciones al personal, por parte del Comité de Contingencias, de volver a las operaciones normales.

.

MANUAL DE PROCEDIMIENTO Y POLÍTICAS DE ADMINISTRACIÓN DE RED.

.

4.2.1 INTRODUCCIÓN

“La información es uno de los activos más importantes de las entidades, y en algunos casos el giro principal de actividad”.

Es indudable que cada día las entidades dependen en mayor medida de la información y de la tecnología, y que los sistemas de información están más soportados por la tecnología, como soporte para la toma de las decisiones.

Por otra parte, hace unos años la protección era más fácil, con arquitecturas centralizadas y terminales no inteligentes, pero hoy en día los entornos son realmente complejos, con diversidad de plataformas y proliferación de redes, no solo internas sino también externas, incluso con enlaces internacionales como lo es Internet.

Es por esto que los administradores de IT deben de contar con procedimientos bien claros y políticas que ayuden a mantener un ambiente más seguro, implementando aplicaciones de seguridad, monitoreo y administración.

El presente manual de Procedimientos y Políticas de Administración de Red, esta sujeto a los cambios que con el crecimiento tecnológico se implementan nuevos servicios para la Institución.

4.2.2 OBJETIVOS

4.2.2.1 GENERAL

Establecer lineamientos de trabajo que normen de manera sistemática el buen funcionamiento operativo del Instituto Salvadoreño de Fomento Cooperativo, a través de la administración eficiente del área de Redes.

.

4.2.2.2 ESPECÍFICOS

1. Asegurar la correcta ejecución de las tareas de procesamientos.
2. Satisfacer las necesidades y el acceso de información a los diferentes usuarios de manera oportuna.
3. Definir normas y procedimientos que brinden seguridad a las instalaciones físicas del área y equipo Informático.

4.2.3 ALCANCES

El Manual se ha enfocado a desarrollar los procedimientos del Departamento de Informática del Instituto Salvadoreño de Fomento Cooperativo. Únicamente se documentarán los procedimientos, normas, guías rápidas y controles que tienen que ver con ésta.

4.2.4 RESPONSABLES DE REVISIÓN DEL MANUAL.

Jefe y personal del área de Informática.

4.2.5 AREA ADMINISTRACIÓN DE RED

Esta área se compone por dos grandes servicios:

1. La administración de recursos informáticos Internos.
2. El soporte técnico de recursos informáticos externos,

El primero tiene la responsabilidad de crear el ambiente de red necesario para el acceso de los usuarios (cuentas de acceso de usuarios, permisos de acceso a servicios y/o aplicaciones, etc), el segundo tiene la grande responsabilidad de garantizar el funcionamiento de las estaciones de trabajo, configuraciones de:

.

1. aplicaciones (software): correo electrónico, sistemas, base de datos, etc,
2. equipos (hardware): conectividad de red, Internet, correo electrónico, etc,
3. conectividades físicas de red: interruptores, repetidores, cableado estructurado, etc.

Para el buen funcionamiento de los servicios y uso de los recursos informáticos, como de la seguridad de los ambientes de usuarios, deben de establecerse políticas de uso y procedimientos, que ayudan a obtener una mejor administración de los usuarios y recursos tecnológicos como también el rendimiento de la red, la cual se puede degradar por el exceso de uso de los servicios, como por ejemplo Internet, correo electrónico (email), etc.

Para la administración de los recursos informáticos se hace necesario tener el universo tanto de los usuarios como de los recursos disponibles, es por ello que se detallan los pasos a seguir para la obtención de permisos y usos de los recursos tecnológicos existentes.

Por la estructura organizativa se presentan las siguientes clasificaciones de usuarios:

1. Ejecutivos
2. Jefes de Unidad
3. Colaboradores
4. Personal Técnico de Campo

Se le llamará usuario a todo aquel que posea una de cuenta de acceso a la red y haga uso de los servicios informáticos autorizados.

Se considera la diferenciación para efectos del alcance de los permisos de los que gozarán los agrupados bajo una misma clasificación, es decir, se estandarizarán los perfiles de usuario en una misma plantilla, tanto a nivel del Dominio como de los Sistemas, considerando estos últimos aquellos que realizan una tarea afín, por ejemplo : Fomento y Asistencia Técnica y Registro, etc.
Se consideran dentro de la clasificación los siguientes cargos:

.

Ejecutivos	**Presidente,** **Vicepresidente**.
Jefes de Unidad	**Los Jefes de cada una de las áreas u oficinas.**
Colaboradores	**Personal administrativo a las categorías anteriores**
Personal Técnico de Campo	**Personal de Campo que tiene como tarea principal el visitar a las Asociaciones Cooperativas.**

4.2.6 ALCANCES DE PROCEDIMIENTOS Y POLÍTICAS.

Se definirán en función de la siguiente forma, en la cual se representa las áreas de responsabilidad y los alcances.

1. Hardware: Servidores, Mantenimientos y Proveedores.
2. Software: Sistema Operativo, Aplicaciones, Antivirus, Detección de Intrusos, Base de datos, Licenciamiento y Proveedores.
3. Servicios: Red, Sistemas, Correo Electrónico, Internet y Antivirus.
4. Usuarios: Ejecutivos, jefes de unidad, colaboradores y Personal técnico de campo.
5. Otros: Copias de seguridad y proyectos.

4.2.7 PROCEDIMIENTOS Y POLÍTICAS DE USUARIOS DEL DOMINIO.

Las políticas de usuarios, ayudarán a conocer el universo de accesos y tipos usuarios que hacen uso de los recursos tecnológicos, adicionalmente servirá para crear y establecer plantillas en las que serán ubicados los usuarios.

La apertura de cuentas de red para los distintos usuarios, la realizara el Jefe del departamento de Informática, asignando los permisos según el grupo de usuario al que corresponda.

.

4.2.7.1 PROCEDIMIENTO

Para los usuarios que requieren hacer uso de las tecnologías, el procedimiento ha seguir es el siguiente:

4.2.7.1.1 SOLICITUD.

El Jefe del área deberá proporcionar toda la información que se requiere, considerando el alcance en el desarrollo de las actividades del usuario dentro de la institución.

Dicha información será remitida a Informática vía correo electrónico, solamente se recibirán los enviados por jefes de unidad.

4.2.7.1.2 AUTORIZACIÓN.

Informática verificara los datos con el jefe de Unidad indicado o en su defecto con Recursos Humanos, para su validación.

La autorización de los servicios requeridos, deberá estar relacionada con las funciones o tareas del puesto del usuario. Caso contrario solo aplicaran aquellas que cumplan con lo antes expuesto a criterio de Informática.

4.2.7.1.3 CONFIGURACIÓN

Aprobado el o los servicios del usuario, la configuración del perfil en la estación de trabajo estará bajo la responsabilidad del Técnico Asignado por el Jefe de Informática, quien contactará con el usuario y/o Jefe de Área y coordinar la visita técnica para realizar dicha tarea.

.

Adicionalmente, de ser necesario solicitar modificación de los servicios y aplicaciones otorgados o denegados al usuario, se hará de la misma manera solicitando al Jefe de Informática dichos cambios y verificando de la manera descrita anteriormente.

4.2.7.2 POLÍTICAS CUENTAS DE USUARIO

1. Las cuentas de usuario serán solicitadas únicamente por el Jefe de la unidad respectiva, enviando al Jefe de Informática la solicitud vía e-mail.
2. El usuario deberá ser empleado a tiempo completo o parcial de la Institución.
3. La creación de la cuenta de red es responsabilidad del Jefe de Informática o en su defecto el designado del mismo.
4. El logín de acceso al dominio (nombre de cuenta de red), estará compuesto por el primer nombre y el primer apellido, los cuales deberán ser únicos en el dominio. Esto estará sujeto a cambio cuando previamente exista una cuenta de usuario que coincida con la que se desea crear. Se hará una combinación entre su nombre y apellido.
5. Para los usuarios que se les permita el acceso a Internet se les proveerá de un nombre de usuario y palabra de acceso (password) para tales efectos. Previa autorización de los derechos de navegación dados por Informática o solicitadas por el Jefe de área del usuario.
6. El Jefe de Informática creara la cuenta de red del usuario con la palabra de acceso (password) respectiva, en blanco, y con la opción que al ingresar el usuario al dominio de la red por primera vez, le permita configurar dicha clave de acceso, a discreción del usuario, para efectos de seguridad.
7. El formato de la palabra de acceso (password) del usuario será alfanumérico, con una longitud mínima de 5 caracteres.
8. La cuenta de red y la palabra de acceso (password) esta bajo la responsabilidad del usuario a quien se le entrego en el momento de configurar, por lo que la seguridad y confidencialidad de la misma recae directamente en cada usuario.

.

9. La palabra de acceso (password) tendrá vigencia de 60 días, la cual automáticamente se le solicitará cambiar al usuario el cual tiene la obligación de ingresarle una nueva contraseña según políticas.
10. Las cuentas de red serán inhabilitadas en periodos de vacaciones, especialmente: Semana Santa, Agosto y Diciembre.
11. El horario de ingreso al dominio será de las 8:00 a.m. a las 5:00 p.m., salvo aquellos usuarios que tienen un horario distinto el cual deberá reportar Recursos Humanos.
12. El usuario esta en la obligación de usar el acceso a la red o servicios destinados exclusivamente con el fin para lo cual se le permitió acceso.

4.2.7.3 POLÍTICAS CUENTAS DE CORREO ELECTRÓNICO

1. Las cuentas de usuario de correo electrónico serán solicitadas únicamente por el Jefe de la unidad respectiva, al Jefe del Departamento de Informática.
2. El jefe de área que solicita, determinara el derecho del usuario de correo electrónico, bajo su responsabilidad, dependiendo de sus funciones o cargo asignado el cual deberá ser:
    - Cuenta de correo solo interno.
    - Cuenta de correo solo con salida a Internet.
    - Las dos anteriores.
3. El usuario deberá ser empleado a tiempo completo o parcial de la Institución.
4. La creación de la cuenta de correo electrónico es responsabilidad del Jefe de Informática y en su defecto el designado del mismo.
5. El formato de la cuenta de correo electrónico del usuario por razones del dominio, será: **nombre.apellido@insafocoop.gob.sv**

4.2.7.4 POLÍTICAS DEL PERSONAL DE INSTITUTO.

1. Las cuentas de usuario administrativos tendrán vigencia a partir de la notificación de su contratación por Recursos Humanos.

2. La cuenta será dada de baja por notificación del Departamento de Recursos Humanos o en su defecto el Jefe del área u oficina, a la cual pertenece el usuario, una vez que dicho personal no labore mas en la Institución, dicha cuenta será inhabilitada por 2 meses y posteriormente será eliminada.
3. Para las cuenta de usuarios temporales se crearán alias, los cuales podrán ser utilizados por contrataciones rotativas y con los mínimos de permisos para el desarrollo de las tareas para las cuales fueron contratados.
4. Se tomará el mismo nombre de la cuenta de red para efectos de acceso a la información compartida dentro de la red.
5. Se utilizarán la misma cuenta de red para el acceso a la base de datos y el sistema, con la misma contraseña (de preferencia) o si el usuario lo desea podrá cambiarla.
6. Para efectos de poder accesar los archivos o correos de los usuarios, cuidando la confidencialidad de la información, se procederá previa autorización del Presidente Ejecutivo, Vicepresidenta o Encargado del despacho, responsables de la unidad a donde pertenece el usuario.

4.2.8 SERVICIOS

Los servicios son aquellas facilidades tecnológicas, de los cuales el usuario podrá hacer uso como apoyo de sus actividades o funciones, y es en relación a esto que el Jefe de Unidad a la cual pertenece el usuario, solicitara dichos servicios disponibles, el cual evaluara el puesto del usuario para considerar el requerimiento de los derechos de uso de los servicios.

Los servicios de los que podrán hacer uso los usuarios son:

1. Servicios de Red.
2. Aplicaciones
3. Correo electrónico
4. Navegación Internet
5. Antivirus

.

A continuación se presenta una breve descripción de los servicios implementados en la Institución, para una mejor comprensión.

4.2.8.1 SERVICIO DE RED

Será la configuración realizada por el Departamento de Informática, en la que se le permitirá al usuario hacer uso de los recursos compartidos, como por ejemplo las impresoras y carpetas.

4.2.8.2 SERVICIO DE SISTEMAS

Para la configuración del servicio de aplicaciones, se tomarán como base lo especificado por el Jefe de Área u Oficina en la solicitud efectuada al Departamento de Informática y si se requiere ampliar las opciones de acceso al o los sistemas, tendrá que hacerlo de la misma manera, solicitándolo el Jefe del área u oficina al Departamento de Informática.

Así como también la instalación y configuración de alguna herramienta o software, que dependiendo de su puesto o funciones se autorice para apoyar su trabajo.

4.2.8.3 SERVICIO DE CORREO ELECTRÓNICO

El Jefe de Área u Oficina evaluará si el usuario debe o no tener habilitado el servicio de correo, para lo que se le propondrá especificar el alcance del servicio en la solicitud realizada al Departamento de Informática, donde especificará si el servicio será solamente interno o interno-externo.

4.2.8.4 SERVICIO DE INTERNET

Para efectos de una mejor utilización del ancho de banda contratado se considerará de uso prioritario para los ejecutivos, jefes de área u oficina y

.

colaboradores según la necesidad, tomándose como base la solicitud hecha al departamento de Informática, en el momento de crear la cuenta**.**

Al personal técnico de campo se le asignaran cuentas de forma general, dependiendo al área u oficina que pertenezcan, para que puedan hacer uso de este servicio.

4.2.8.5 SERVICIO DE ANTIVIRUS

Por protección de los datos, todos los equipos dentro de la institución tendrán instalado y ejecutando el antivirus, con el propósito de proteger tanto los equipos de trabajo (PC´s) como la red institucional de cualquier amenaza de virus informático que atente contra la información y los servicios implementados

4.2.9 POLÍTICAS Y PROCEDIMIENTOS DE SERVICIOS TECNOLOGICOS

Para la utilización de cada uno de los servicios el Jefe del Área u Oficina procederá a hacer la solicitud al Jefe del departamento de Informática, detallando los servicios tecnológicos que quieren ser accedidos.

4.2.9.1 POLÍTICAS DE LOS SERVICIOS TECNOLOGICOS

4.2.9.1.1 SERVICIO DE RED

1. El usuario es responsable del uso y acceso a los recursos compartidos o periféricos a los cuales se le ha dado acceso, como por ejemplo los impresores, scaners, etc.
2. El usuario tendrá terminantemente prohibido almacenar archivos en el que no estén relacionados con su área de trabajo, particularmente en las carpetas que tuviere acceso para dichos fines.

.

3. Informática realizara monitoreos de la red en las que asegurará la conexión de un usuario en la red, esto para efectos del reporte de navegación y otros.
4. Para efectos de compartir la información en grupos de trabajo o usuarios de la red, se deberá hacer el requerimiento, por parte de las Jefaturas para la creación de carpetas compartidas y derechos de acceso al Jefe de Informática.
5. Los impresores o cualquier periférico que requiera el usuario para realizar sus funciones o tareas de su puesto, deberá ser requerido a Informática para su evaluación, configuración e instalación

4.2.9.1.2 SERVICIO DE APLICACIONES Y/O SISTEMAS

1. Las configuraciones de acceso serán responsabilidad de Departamento de Informática, en cuanto la asignación al Rol dentro de la Base de Datos y a los permisos, opciones y configuración de conectividad a la Base de Datos (Fuente ODBC).
2. Las cuentas de usuario serán independiente de las cuentas de dominio, pero se utilizará el mismo nombre de usuario de red (login) para el acceso al sistema y Base de Datos. Cualquier cambio a esta política en relación a la configuración de la cuenta, deberá ser autorizada por Informática y debidamente documentada.
3. Las opciones habilitadas a los usuarios serán de responsabilidad del Jefe de Área u Oficina, quien verificará que soporte técnico halla realizado las configuraciones de acceso según halla solicitado.
4. Para la creación de las cuentas de este servicio, es imperativo que tenga la aprobación del Jefe de Informática.

4.2.9.1.3 SERVICIO DE CORREO ELECTRONICO

.

1. El usuario utilizará como software cliente Microsoft Outlook, queda terminantemente prohibido la utilización de cualquier otro cliente de correo como por ejemplo: lotus Notes, Outlook express, etc.
2. El Jefe del Área u Oficina a donde pertenece el usuario, determinara el tipo de acceso de la cuenta de correo: para uso interno, para uso externo o ambas, eso dependerá del puesto, sus funciones o tareas del usuario que demande el servicio, esto se hará a través de la solicitud hecha al Departamento de Informática, en el momento de crear la cuenta.
3. Los tamaños de los buzones para las cuentas de correo serán los siguientes:

    - Ejecutivos: 50 MB
    - Jefes de Área u Oficina: 10 MB
    - Colaboradores : 6 MB

4. El tamaño máximo de envió y recepción de mensajes será de 2.5 MB.
5. Se prohíbe terminantemente las cadenas de correo no productivas o cualquier otra información que interfiera con el uso normal del servicio.
6. Los usuarios son responsables de mantenimiento del buzón asignado a su persona, ya que en caso de no hacerlo, el Jefe de Informática le notificará automáticamente el tamaño actual y el establecido, solicitándole eliminar correos, de lo contrario le advierte que no podrá recibir o enviar mensajes.
7. Por seguridad se establece que no existirán archivos PST (carpetas personales) para que todos los correos o e-mails residan en el servidor y puedan ser respaldados (Backups), salvo en los casos que el usuario lo solicite, con las indicaciones respectivas, previamente autorizadas por el jefe de unidad y el jefe de Informática.
8. En caso de existir en archivo PST, no se garantiza el buen funcionamiento del cliente Microsoft Outlook, en caso de que tal archivo exceda o alcance 1 GB.
9. El servicio de correo es para uso exclusivo de la comunicación electrónica interna o externa de la Institución con las demás áreas u oficinas descentralizadas o instituciones con las cuales se tenga relaciones laborales.

.

10. Se establece como herramienta de comunicación interna el uso del servicio de mensajería electrónica, evitando hacer uso del tradicional memorando.
11. Informática tiene la responsabilidad de efectuar procesos de Backup, al servidor de correos, los cuales serán utilizados en casos de desastre, por lo que se establece realizar el proceso de backup cada viernes.
12. El acceso a los buzones de correo es de uso exclusivo de los usuario, salvo que el Jefe de Área u Oficina, lo requiera se le concederá acceso para realizar una auditoria, lo cual será autorizado por el Jefe de Informática y el Presidente de la Institución o designado del mismo.
13. Informática se reserva el derecho de privacidad sobre los buzones de los usuarios.

4.2.9.1.4 SERVICIOS DE NAVEGACIÓN INTERNET

1. El Jefe del Área u Oficina, evaluará el puesto del colaborador para efectos de evaluar la navegación en Internet, solicitándolo de manera formal al Jefe del Departamento de Informática, quedando bajo la responsabilidad de Jefe de Informática la aprobación del acceso requerido.
2. Para los usuarios que tengan acceso a Internet es prohibitivo la descarga de archivos de Música y video los cuales originan saturación el ancho de banda contratado.
3. El Departamento de Informática, emitirá un reporte de navegación, el cual se le presentará al Presidente y Vicepresidente o designados de los mismos, como garante del uso racional del recurso.
4. Los accesos de navegación y restricción a sitios específicos, se establecerán por medio de la aplicación ID para seguridad de accesos o Firewall y/o el Sistema de Detección de Intrusos, bajo la responsabilidad de el Jefe de Informática.
5. El Jefe de Informática realizara monitoreos aleatorios del enlace, para determinar un mejor uso del enlace o ancho de banda contratado para tal servicio.

.

4.2.9.1.5 SERVICIO DE ANTIVIRUS

1. Es responsabilidad de Informática la actualización de los programas de antivirus en los servidores y clientes.
2. El Departamento de Informática, instalara y configurara los equipos para todo el Dominio INSAFOCOOP.
3. Se prohíbe terminantemente que los usuarios utilicen otra solución Antivirus que no sea la proveída por informática a excepción de los antivirus usados en prueba, instalados por Informática.

4.2.9.1.6 PROCEDIMIENTO CONFIGURACIÓN DE SERVICIOS DE USUARIO

1. Jefe del Área u Oficina solicita de manera escrita a través del correo interno al Departamento de Informática.
2. El Jefe de Informática autoriza la solicitud efectuada por el Jefe del Área u Oficina.
3. El Jefe de Informática, configura el ambiente de acceso a los servicios, según la solicitud presentada por el Jefe del área u oficina, a la que pertenece el usurario.
4. Informática coordina la visita de configuración de servicios autorizados con el usuario.
5. El departamento de Informática realiza la configuración y pruebas de los servicios solicitados y autorizados en el equipo del usuario.
6. El Usuario es configurado tomando como referencia a lo requerido por el Jefe del Área u Oficina.

4.2.10 POLÍTICAS Y PROCEDIMIENTOS DE APLICACIONES (SOFTWARE)

.

Dentro de la administración de las aplicaciones están comprendidas todas aquellas que son exclusivamente para la configuración de la plataforma de servidores los cuales son:

1. BackOffice
    - Windows 2000 Server
    - Exchange 2000 Server
    - SQL 2000 Server
2. Windows NT 4.0
3. Norton Antivirus 10.0

La autorización del acceso a cualquier servidor que compone la plataforma de servidores, será autorizado exclusivamente al personal del Departamento de Informática.

4.2.10.1 POLÍTICAS DE APLICACIONES

1. Los productos (cd´s originales y licencias) estarán bajo la responsabilidad del Jefe de Informática.
2. Los productos estarán resguardados en una caja de seguridad para su protección.
3. Solamente el Jefe de Informática tendrá acceso a la caja de seguridad donde se encuentre los productos.
4. Por motivos de auditoria interna, se llevará bitácora de acceso a la caja de seguridad en la que se especificará el producto a utilizar y el motivo de uso.
5. En los casos que lo requiera se considerará la contratación de servicios especializados. Por ejemplo: nuevas configuraciones o topologías de seguridad.
6. Los productos de aplicaciones (software) originales serán de responsabilidad del Jefe de Informática o en quien le delegue la custodia.
7. Por cuestiones de seguridad se elaborara copias de respaldo de los productos originales, para su uso en la instalación y configuración de los equipos. Dichas copias serán responsabilidad del Jefe de Informática.

.

4.2.10.2 PROCEDIMIENTO INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES

A continuación se presentan los pasos a seguir por el Jefe de Informática o Técnico designado para la instalación y configuración de las aplicaciones en casos de la creación o actualización de un nuevo servidor o en casos de desastre:

1. El Jefe de Informática, extraerá de la caja fuerte, las licencias de los programas a utilizar para habilitar un nuevo servidor o reinstalar todos los programas del servidor, llenando la bitácora, en el que especificará el fin y los programas a utilizar.
2. Una vez concluida el proceso de instalación y/o configuración de las aplicaciones en los equipos, el Jefe de Informática verificara y certificara el buen funcionamiento de los mismos.
3. El Jefe de Informática devolverá a la caja fuerte, los discos de instalación prestados, dejándolo por escrito en la bitácora.
4. Se elaborara un informe de la falla y la forma de resolver el problema, detallando tiempos y recursos utilizados. Dicho reporte será competencia del Jefe de Informática.

4.2.10.3 PROVEEDORES

4.2.10.3.1 POLÍTICAS

1. Las cotizaciones para la evaluación de los posibles proveedores y opciones tecnológicas, se realizarán por parte de Informática por ser propietario de las soluciones a implementar, caso contrario se le delegará a la Unidad de Contrataciones y Adquisiciones Institucional.
2. Informática negociará la cobertura o alcance de los productos comprados y servicios contratados.
3. Informática evaluara las diferentes opciones recibidas para determinar la mejor solución tecnológica.

.

4.2.10.3.2 PROCESO ADQUISICIÓN DE SOFTWARE

Para la adquisición de nuevos productos de software se ejecutara el siguiente procedimiento:

1. Recepción y evaluación del requerimiento de software del usuario o área.
2. Cotizar y contar con una terna de proveedores de tecnología, la cual es entregada por la UACI.
3. Solicitar dentro de la cotización la instalación de los productos con sus respectivos manuales del usuario, capacitación y garantía, esto aplica dependiendo del producto que se desea adquirir.
4. Solicitar tiempo mínimo y máximo de soporte técnico (consultas y visitas), si el producto lo requiere.
5. Informática evaluara el precio, calidad, soporte técnico, garantía, tiempos de entrega, características técnicas del producto.
6. Informática elaborara un cuadro de precios comparativos por proveedor, resaltando las características del producto que mas convengan a la Institución.

4.2.11 POLÍTICAS Y PROCEDIMIENTOS DE HARDWARE

La administración del hardware dentro de la Red de Datos, obedece a la evaluación y desempeño que cada equipo realiza según el software instalado para una función especifica destinada. A continuación se presenta en términos generales los servidores, las funciones y procedimientos que realizan entre los servidores.

4.2.11.1 POLÍTICA GENERAL

.

El Jefe de Informática tiene la responsabilidad de documentar las configuraciones de cada uno de los servidores y servicios que se prestan por medio de los mismos.

4.2.11.2 POLÍTICAS

4.2.11.2.1 SERVIDOR BASE DE DATOS.

1. Este equipo alojará únicamente la Base de Datos Institucional y será responsabilidad del Jefe de Informática.
2. A la Base de Datos se conectarán los usuarios únicamente por la fuente ODBC configurada y el Sistema que utilizaren.
3. Es responsabilidad del Jefe de Informática efectuar procesos de respaldo, como en casos de desastre habilitar nuevamente la Base de Datos.
4. Deberán existir partes en stock en calidad de redundancia para ser utilizadas en caso de desastre por ejemplo: Discos Duros, Memoria RAM, etc.

4.2.11.2.2 SERVIDOR DE WEB

1. La publicación del sitio web de la Institución será responsabilidad del webmaster, el cual es un técnico del departamento de Informática.
2. La administración de dicho servidor será de responsabilidad del Jefe de Informática.
3. El webmaster será el responsable de actualizar la información que se presenta en la página web a los clientes de la Institución.
4. La configuración del sitio web (IIS, Internet Information Service), será proporcionada por el Webmaster y el Jefe de Informática.
5. El Jefe de Informática realizará las configuraciones para enrutar las consulta http y hará las pruebas haciendo uso de otro enlace distinto para su verificación.

.

4.2.11.2.3 SERVIDOR DE CORREO

1. La administración del Servidor de Correo será responsabilidad del Jefe de Informática.
2. El Jefe de Informática será responsable de realizar Backup de los buzones de los usuarios.

4.2.12 POLÍTICAS Y PROCEDIMIENTOS DE MANTENIMIENTO

Los mantenimientos son parte del cuidado físico de los equipos, con los que se pretende evitar daños por acumulación de polvo, como por ejemplo, atascamiento de ventiladores de enfriamiento, acumulación de polvo en las superficies electrónicas, etc.

4.2.12.1 POLÍTICAS

1. Los mantenimientos preventivos se realizarán cada dos meses según el plan de mantenimientos descrito en el Plan Contingencial.
2. Los mantenimientos se realizarán en horas de oficina, preferiblemente, previa programación.
3. Informática destinará sus esfuerzos en instalar y habilitar los servicios afectados en el menor tiempo posible en casos de desastre.
4. Si existiera dificultades en la instalación y configuración de algún servicio, se solicitará soporte externo, alquilando los servicios necesarios para el restablecimiento de las operaciones normales.

4.2.12.2 PROCEDIMIENTOS

4.2.12.2.1 MANTENIMIENTO PREVENTIVO

.

1. El Jefe de Informática le solicitará autorización de acceso a las áreas u oficinas donde se realice el mantenimiento, haciendo del conocimiento que se realizará mantenimiento preventivo a los Equipos.
2. Los equipos serán desinstalados y llevados a otra área para el respectivo aspirado, por ejemplo : el Pasillo, etc.
3. Los equipos serán abiertos y aspirados usando el equipo apropiado, aspiradora / sopladora.
4. Se aspirarán el teclado y Mouse, este último se destapará para limpiar los contactos que hacen girar la bolita.
5. El monitor se limpiara superficialmente con limpiadores de exteriores de equipos de cómputo, por ejemplo : Desk en Office Cleaner.
6. Una vez aspirados los equipos, se instalarán nuevamente en el área del cual fueron tomados se conectarán sus dispositivos.
7. Se harán prueba de comunicación y de servicio (funcionamiento).

4.2.12.2.2 MANTENIMIENTO CORRECTIVOS

1. Dependiendo del equipo que requiere atención técnica, se les notificará a los usuarios que dichos servicios, que se esta en labores de mantenimiento.
2. Una vez habilitado el equipo atendido se harán pruebas internas de comunicación y Servicio.
3. Una vez realizadas las pruebas se les hará del conocimiento al o los usuarios.

4.2.13 POLÍTICAS Y PROCEDIMIENTOS DE COPIAS DE SEGURIDAD (BACKUPS)

4.2.13.1 POLITICAS

.

1. Las copias de seguridad servirán para garantizar, en casos de desastre como por ejemplo: terremotos, incendios, daños en los equipos, etc., que las pérdidas de información sean mínimas.
2. El proceso de Backup se hará de los siguientes Aplicaciones y archivos :

    - Aplicación de cada uno de las áreas u oficinas.
    - Base de Datos que contiene información básica de Asociaciones Cooperativas.
    - Archivos con extensiones *.doc, *.xls, *.ppt y otros de importancia para la Institución.
    - WebSite.
    - Correo.

    Además de estos también se harán respaldos de:

    - Archivos fuentes de Programas desarrollados
    - Proyectos y otros documentos que la Presidencia considera indispensable para el buen funcionamiento de la Institución.
3. Los Backup se realizarán semanalmente a excepción de la información de los servidores, los cuales se realizaran cada dos semanas.
4. El proceso de Backup será responsabilidad del Jefe de informática o designado del mismo.
5. Los backups se almacenarán en CD´s o DVD's.
6. Los backups se resguardarán en la caja de seguridad del INSAFOCOOP.
7. Los Desarrolladores copiarán los archivos fuentes en una carpeta destinada de donde el Jefe de informática tomará para realizar el proceso de backup en CD o DVD.

4.2.14 POLÍTICAS Y PROCEDIMIENTOS DE OFICINAS REGIONALES.

Las Oficinas Regionales tendrán la finalidad de brindar servicios especializados, algunos de estos propiamente para las áreas de Fomento y Asistencia técnica y

.

Vigilancia y Fiscalización, estas oficinas tendrán acceso a internet, haciendo uso del enlace contratado.

4.2.14.1 PROCEDIMIENTOS

1. La implementación de los equipos de la Oficina Regional estará a cargo del Jefe de Informática, pero el responsable de los mismos será el Jefe de la Oficina.
2. El equipo informático, así como el cableado de red de la Oficina lo instalara el departamento de Informática.

4.2.14.2 POLITICAS

1. El Jefe de la Oficina es la entidad responsable de la administración del equipo de Cómputo, con la finalidad de realizar y brindar todos lo servicios.
2. La evaluación, análisis y determinación de la tecnología o soluciones tecnológicas a implementarse en las Oficinas Regionales, es competencia del Departamento de Informática.
3. El Departamento de Informática proporcionara la solución tecnológica más conveniente, para que la Oficina pueda brindar los servicios de la mejor manera.
4. Informática dará todo el soporte técnico en lo relacionado al mantenimiento preventivo y correctivo, garantías, configuración de software, etc., de los equipos de cómputo y periféricos que integran las Oficinas Regionales.
5. En las Oficinas Regionales no se harán consulta de correo personal como por ejemplo Hotmail, Yahoo mail, latinmail, etc., o visitas a sitios no productivos como sitios de entretenimiento diversos, esto por seguridad de no permitir que virus que se descargan automáticamente desde estos sitios entren en las maquinas.
6. Las necesidades de capacitación informática para el buen uso del equipo se solicitarán directamente a Informática, con el fin de poder determinar el soporte tecnológico, técnico, recurso humano para atender a la solicitud.

.

4.2.15 PROCESO DE DIVULGACION

Los responsables de la divulgación de este manual se realizara a través de los departamentos de Recursos Humanos y de Informática, para lo cual se seguirán los siguientes pasos:

1. El Departamento de Recursos Humanos establecerá la lista de personas y la cantidad de las mismas que se capacitaran en cada reunión.
2. El Departamento de Informática diseñara el material audiovisual por medio del cual se presentara este manual, explicando cada uno de sus apartados, a los nuevos personeros de la Institución.
3. Los Departamentos de Recursos Humanos y de Informática, se reunirán para establecer un cronograma, en el que se refleje los días y las horas, en los que se desarrollaran las capacitaciones.

.

RECOMENDACIONES.

Después de realizado el presente trabajo de graduación y de haber estudiado el caso en particular de la red de datos de la Institución de Gobierno, se recomienda lo siguiente:

1. La Institución tendrá que velar por el cumplimiento y el conocimiento de este Plan Contingencial y el Manual de Procedimientos y Políticas para la Administración de la Red de Datos, por parte de cada uno de los empleados.
2. La Institución a través del Depto. de Recursos Humanos, tendrá que crear el Plan de Evacuación, que se menciona en este trabajo, con el propósito de fortalecer la aplicación del Plan Contingencial.
3. La Institución deberá diseñar un plan de capacitaciones periódicas dirigido al personal que formara los Comités de Contingencia y Grupos de Apoyo que la institución creare para atender las emergencias.
4. La Institución es la garante de proveer a cada uno de los Comités de Contingencia y grupos de apoyo, los recursos necesarios para poder dar atención a las respectivas emergencias.
5. La Institución, a través del Coordinador del Comité de Contingencias será el responsable de la implementación y el mantenimiento del Plan Contingencial y el Manual de Procedimientos y Políticas de Administración de Red; en la búsqueda de la mejora continua de los procesos y la calidad de los servicios que presta la Institución a sus clientes, tanto internos como externos.
6. La revisión y/o actualización del Plan Contingencial y el Manual de Procedimientos y Manual de Procedimientos y Políticas de Administración de Red, tendrá que realizarse al menos una vez cada año.

.

CONCLUSIONES.

En la actualidad uno de los factores que afectan tanto a las personas jurídicas como a las personas naturales es la “seguridad”. Esto nos ha enseñado a que debemos estar listos en cualquier momento para poder reaccionar ante las distintas problemáticas que se nos planteen. El equilibrio entre lo que puede pasar y el espectro de lo que se puede cubrir es amplio, existiendo entre estos un espacio grande, a esto se le suma que es un campo de trabajo intangible.

No obstante se hace necesario desarrollar herramientas que permitan minimizar los riesgos a los cuales nos podemos enfrentar, contando con las soluciones antes de conocer la problemática. También es importante mencionar que las soluciones no deben de ser aisladas, sino más bien integrado para que contribuyan a la solución general de la problemática que se plantee.

Es por ello que el Plan de Contingencias que se presenta, minimiza todos los riesgos a los cuales se puede enfrentar la Institución, aunque se sabe que “la seguridad perfecta requiere de un nivel de perfección que no existe”.

El Plan de Contingencias, así como el Manual de Procedimientos y Políticas de Administración de Red, funcionara en la Institución en razón que cada uno los siguientes factores cumplan con su parte:

1. Personal de la Institución.
2. Implementación de los mismos.
3. Dotar de las herramientas necesarias.
4. Capacitaciones.

Es importante mencionar además, que cada una de las problemáticas planteadas mostrara según sea el caso que a medida acontecen, evolucionan, es por ello que será necesario la revisión y actualización del Plan Contingencial y el Manual de Procedimientos y Políticas de Administración de Red, para que estos también puedan evolucionar y fortalecer a la institución.

.

GLOSARIO

Cookie: Procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para sus posterior recuperación. En la práctica la información es proporcionada desde el visualizador al servidor del Word Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

Clave secreta: Es el código básico utilizado para encriptar y desencriptar un mensaje. Cuando se utiliza la misma para las dos funciones, estamos ante un sistema simétrico.

Cliente: Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que solicita el contenido de un archivo a un servidor es un cliente de este servidor.

Cracker (intruso): Un "cracker" es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los "hackers", y suelen disponer de muchos medios para introducirse en un sistema.

Dominio: Conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios.

Firewall: un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente uilizados para evitar el acceso no autorizado de usuarios de internet a redes privadas conectadas a la misma, especialmente intranets.Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

.

Existen varias técnicas de firewall:

- Filtrado de paquetes: Examinar a cada paquete que deje o entre a la red, y aceptarlo o rechazarlo basado en reglas definidas por el usuario. El filtrado de paquetes es efectivo y transparente a los usuarios, pero es difícil de configurar. Adicionalmente, es suceptible a IP spoofing.
- Gateway de aplicación: Aplica mecanismos de seguridad a aplicaciones específicas como FTP y Telnet. Es muy efectivo, pero puede provocar degradaciones de perfomance.
- Gateway a nivel de circuito: Aplica mecanismos de seguridad cuando una conexión TCP es establecida. Una vez establecida los paquetes circulan sin más inspección.
- Proxy server: Intercepta todos los mensajes que entran y dejan la red. Un Proxy server oculta en forma efectiva las direcciones reales de red. Ver proxy, Proxy server.

En la práctica, un firewall utiliza alguna o varias de estas técnicas en conjunto.

Firewall Router: Filtro de paquetes que filtra el tráfico en base a la dirección destino y fuente.

Hacker: Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

HTML Lenguaje de marcado de hipertexto, (Hiper-Text Markup Languaje) es el lenguaje con que se escriben los documentos en el World Wide Web. A la fecha existen tres versiones de HTML. HTML 1, se sientan las bases para la disposición del texto y las gráficas, HTML 2 donde se agregan formas y HTML 3 (llamado también extensiones Netscape) donde se añaden tablas, mapas, etc.

HTTP. Protocolo de Transferencia de Hipertextos (Hiper-Text Transfer Protocol). Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

.

Hub Un punto común de conexión de dispositivos en una red. Los hubs son usados comúnmente para conectar segmentos de una LAN. Un hub contiene múltiples ports. Cuando un paquete llega al port, es copiado a los otros ports, de esta manera los otros segmentos de la LAN pueden ver todos los paquetes. Un hub pasivo simplemente sirve de conductor de datos entre los diferentes ports. Los llamados hubs inteligentes incluyen servicios adicionales como permitir a un administrador monitorear el tráfico y configurar cada port del hub. Estos hubs se conocen generalmente como hubs administrables (manageable hubs). Un tercer tipo de hub, llamado switching hub, lee la dirección de destino en cada paquete y lo envía al port correcto.

Intranet. Una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno.

IP address (Dirección IP) Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

Local Area Network (LAN) (Red de Area Local) Red de datos para dar servicio a un área geográfica pequeña, un edificio por ejemplo, por lo cual mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

Navegador: Aplicado normalmente a programas usados para conectarse al servicio WWW. Protocolo Descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.

Router (direccionador) Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento. El router se necesita cuando las dos redes utilizan la misma capa de transporte y tienen diferentes capas de red. Por ejemplo, para una conexión entre una red local ethernet y una red pública X.25, se necesitaría un router para convertir las tramas ethernet a la forma que exige la red X.25. De esta manera la definición teórica del router es la de un dispositivo que cubre hasta la capa 3 del modelo OSI, aunque en la práctica, cubren hasta la 4 (transporte) ya queinspeccionan las sesiones y los ports utilizados, para filtrar tráfico mediante

.

access-lists, por ejemplo. Los Routers tienen amplio soporte para protocolos LAN y WAN, y además cuentan con diferentes interfaces de esos tipos. Son equipos con un tiempo medio de falla muy alto, confiables, y que una vez configurados requieren muy poco mantenimiento. Poseen características que hacen que rara vez deban ser detenidos, por ejemplo, mantenimiento del software y actualización del mismo sin disrupción del servicio, y desde el punto de vista del hardware, los modelos “high end” poseen características tales como placas “hot swap”, esto es, pueden ser cambiadas sin detener el equipo, y fuentes de alimentación redundantes.

TCP: Transmission Control Protocol. Protocolo de control de Transmision. Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

TCP/IP (Transmission Control Protocol/Internet Protocol) Arquitectura de red desarrollada por la "Defense Advanced Research Projects Agency" en USA, es el conjunto de protocolos básicos de Internet o de una Intranet.

Telnet Telnet es el protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto. Está definido en STD 8, RFC 854 y tiene opciones adicionales descritas en muchos otros RFCs

Trojan Horse (Caballo de troya) programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

URL. Localizador Uniforme de recursos (Uniform Resorce Locator). Sistema de direccionamiento estandar para archivos y funciones de Internet, especialmente en el Word Wide Web. El url esta conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.sfp.gov.sv) más el directorio y el archivo referido.

WAN: Wide Area Network. Red de Area Extensa.

WWW, WEB o W3: World Wide Web. Estrictamente que la WEB es la parte de Internet a la que accedemos a través del protocolo HTTP y en consecuencia gracias a browsers normalmente gráficos como Netscape.

.

BIBLIOGRAFIA

Manual de Políticas para la Implementación de las Tecnologías de la Información y la Comunicación de la Universidad Mayor de San Andrés.

Manual de Seguridad en Redes. ArCERT**.** Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina. Subsecretaría de Tecnologías Informáticas Secretaría de la Función Pública.

http://www.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5010/presenta.htm
http://www.monografias.com/trabajos16/seguridad-informatica/seguridad-informatica.shtml#ataques
http://www.monografias.com/trabajos12/fichagr/fichagr.shtml
http://www.monografias.com/trabajos30/mantenimiento-computador/mantenimiento-computador.shtml
http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/es/security-guide/s1-netprot-hardware.html
http://www.improven-consultores.com/
http://www.unellez.edu.ve/otros/ctsi/paginas/soporteman.php
http://www.idrc.ca/es/ev-28257-201-1-DO_TOPIC
http://www.auditoriasistemas.com/politicas_de_seguridad.htm
http://www.solomantenimiento.com/
http://www.terra.es/tecnologia/seguridad/
http://www.jevansa.com.pe

.