SERVICIO DE AGUA POTABLE Y ALCANTARILLADO DE AYACUCHO S.A.

SEDA AYACUCHO
Servicio de Agua Potable y Alcantarillado de Ayacucho S.A.
Llevamos vida a tu hogar

PROYECTO:
PLAN DE CONTINGENCIAS Y SEGURIDAD DE INFORMACIÓN 2023-2026

PARTICIPANTES:

FIRMA DIGITAL
Firmado digitalmente por MUNAYLLA ROJAS Ramiro FAU 20143079075 soft
Motivo: Soy el autor del documento
Fecha: 21.12.2023 16:50:53 -05:00

Ing. Ramiro Munaylla Rojas
Jefe del Departamento de Sistemas y TI

FIRMA DIGITAL
Firmado digitalmente por NAJARRO CARDENAS Skinner FAU 20143079075 soft
Motivo: Soy el autor del documento
Fecha: 21.12.2023 16:53:16 -05:00

Ing. Skinner Najarro Cárdenas
Especialista en Sistemas

AYACUCHO - PERÚ

2023

INDICE

PRESENTACIÓN

El Departamento de Sistemas y Tecnologías de Información, considera que la información es el patrimonio principal de la empresa, por lo que se deben de aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

A medida que la tecnología ha ido evolucionando y con ella, la envergadura de los sistemas de información de las empresas públicas y privadas, la seguridad del entorno informático (hardware, software, comunicaciones, etc.) se ha convertido en una de las grandes preocupaciones de los profesionales de esta actividad. Esta preocupación debe ser adecuadamente comprendida y compartida por los directivos, los cuales deben considerar a las inversiones en medidas de seguridad informática, como un gasto necesario, que contribuye a mantener la operatividad y rentabilidad de la Empresa.

Esto implica que los responsables del Servicio Informático, deban explicar con la suficiente claridad y con un lenguaje inteligible, las potenciales consecuencias de una política de seguridad insuficiente o incluso inexistente. El presente documento pretende ayudar a comprender mejor la contingencia en los sistemas de información que comprende: la identificación de riesgos, calificación de la probabilidad de que ocurra un riesgo, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias.

Los Planes de Contingencias permitirán mantener la continuidad de sus sistemas de información frente a eventos críticos, de nuestra entidad y minimizar el impacto negativo sobre la misma. Nuestros empleados y usuarios. Deben ser parte integral de su organización y servir para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

1. INTRODUCCIÓN

1.1. OBJETIVO DEL PLAN

1.1.1. Objetivo General

Establecer el marco necesario para garantizar la continuidad de los servicios y/o procesos frente a incidentes imprevistos, minimizando los riesgos, protegiendo los activos (servicios, datos e información, aplicaciones, equipos informáticos, personal, redes de comunicación, instalaciones) y facilitando la pronta recuperación.

1.1.2. Objetivos Específicos

- Indicar las acciones preventivas y correctivas que se deban ejecutar para asegurar la integridad de la información, la vida humana y equipos de la empresa, ante posibles causas como: Natural, Humano y Tecnológico.
- Identificar las aplicaciones consideradas críticas para la operatividad de SEDA AYACUCHO S.A.
- Desarrollar procedimientos y guías en caso de desastre para para los servicios críticos, vitales.
- Definir la funcionalidad mínima que se requiere en caso de contingencia.
- Desarrollar e impartir capacitación inicial para el correcto funcionamiento del Plan de Contingencia y Seguridad de la Información.
- Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan de Contingencia y Seguridad de la Información.

1.2. ALCANCE DEL PLAN

El alcance del Plan de Contingencia y Seguridad de la Información 2023-2026 comprende la restauración de los servicios críticos de tecnología de Información que dan soporte a los servicios de SEDA AYACUCHO S.A.

Todo el personal de SEDA AYACUCHO S.A. involucrado en el tratamiento de la Información.

1.3. REFERENCIAS NORMATIVAS Y LEGALES

- Ley Nº 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Legislativo N° 1412, aprueba la Ley de Gobierno Digital, y modificatorias.
- Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea al Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).

- Resolución Directoral N° 013-2016-INACAL-DN que aprueba las Normas Técnicas Peruanas entre otras sobre Ingeniería de software y sistemas. Resolución Ministerial N° 041-2017-PCM, que aprueba la Norma Técnica Peruana "NTP-ISO/IEC 12207:2016 Ingeniería de Software y Sistemas. Procesos del Ciclo de Vida del Software. 3a Edición.
- Reglamento de Organización y Funciones de SEDA AYACUCHO S.A.
- Ley N° 27658, Ley Marco de la Modernización de la Gestión del Estado y su modificatoria Decreto Legislativo N° 1446.
- Ley N°30096, Ley de Delitos Informáticos y su modificatoria Ley N°30171.
- Ley N°29773, Ley de protección de datos personales.
- Resolución Ministerial N.º 004-2016-PCM, Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática. Quedando derogada la Resolución Ministerial N° 129-2012-PCM.
- Decreto Supremo N° 066-2011-PCM que aprueba el "Plan de Desarrollo de la Sociedad de la información en el Perú.
- Resolución Ministerial N° 274-2006-PCM, que aprueba la "Estrategia Nacional de Gobierno Electrónico".
- Decreto Supremo N° 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.

1.4. DEFINICIONES

1.4.1. **Activos:** En términos informáticos se refiere a cualquier recurso de tecnología de información. Estos activos pueden incluir hardware, software, redes, datos, servicios en la nube y otros componentes relacionados con la tecnología

1.4.2. **Aplicación:** Es aquel programa informático que permite a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora y suelen ejecutarse sobre el sistema operativo

1.4.3. **Amenazas:** Es cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la institución.

1.4.4. **Base de Datos:** colección de información organizada de forma que un programa o aplicación pueda seleccionar rápidamente los fragmentos de datos que necesite.

1.4.5. **Centro de datos:** centro de procesamiento para obtener información, en el cual se albergan los sistemas de información, hardware, componentes asociados, como telecomunicaciones y sistemas de almacenamiento.

1.4.6. **Confidencial:** Información o asuntos que debe mantenerse protegida, restringida o privados.

1.4.7. **Firewall:** Dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios y pueden ser implementados en hardware o software, o en una combinación de ambos.

1.4.8. **Datos:** Son todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (base de datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colección de bits.

1.4.9. **Datos Personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

1.4.10. **Incidente:** En nuestro contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático en SEDA AYACUCHO S.A.

1.4.11. **Impacto:** Es el resultado o efecto de un evento, el impacto de un evento puede ser positivo o negativo sobre los objetivos relacionado de la institución.

1.4.12. **Plan de Recuperación:** Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

1.4.13. **Riesgo:** Posibilidad de que ocurran eventos no deseados o situaciones adversas relacionadas con la seguridad de la información y la tecnología de la información.

1.4.14. **Sistema de Información:** Es el conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso. Este involucra a personas, registro de datos, actividades que los procesan y los manuales de procesos o procesos automatizados.

2. PLANIFICACIÓN DE CONTINGENCIAS

La fase de planificación es la etapa donde se define y prepara el esfuerzo de planificación de contingencia/continuidad. Para asegurar que se consideran todas las posibles eventualidades, se ha de elaborar una lista de todos los riesgos conocidos, para lo cual se deberá realizar un análisis de riesgos.

2.1. DETERMINACIÓN DEL ESCENARIO CONSIDERADO

En esta primera instancia del Plan de Contingencia, se pone como objetivo identificar y delimitar el escenario que será objetivo de estudio para la realización del Plan.

La idea de este acercamiento inicial es conocer:

- Las condiciones físicas del entorno;
- Los servicios y aplicaciones existentes;
- Los equipos presentes;
- Los servidores;
- Los elementos de backup;
- Los elementos de almacenamiento de datos;
- Los elementos de comunicaciones.

2.2. DEFINICIÓN DE LOS TIPOS DE OPERACIÓN EN UNA CONTINGENCIA

Para elaborar el Plan de Contingencia, se consideran distintos estados de situación, que se definen a continuación, para establecer un marco claro que identifique y enumere las distintas instancias por las que puede atravesar la empresa en materia informática en estudio antes, durante y luego de una contingencia.

Los principales tipos de operaciones considerados ante una emergencia son:

a) Operación Normal Inicial:

Es la operación que se registra antes de ocurrir la contingencia. Asimismo, define las condiciones que se deben alcanzar como objetivo final mediante la ejecución del Plan de Contingencia Informática;

b) Operación Alternativa:

Mientras se trabaja en la recuperación de las prestaciones afectadas por la contingencia, los usuarios deberán utilizar una operación alternativa, constituida fundamentalmente por

procesos manuales, durante la cual se genera información. A partir del momento en que los servicios y aplicaciones estén disponibles, existe un tiempo de "catch up" o actualización de la información del sistema, en el cual se ingresan las novedades ocurridas desde la ocurrencia de la emergencia;

c) Operación Normal en Desastre:

Mediante la ejecución de los procedimientos que reciben el nombre de "Recuperación de las prestaciones", se llega a esta instancia en la cual todos los servicios y aplicaciones han sido recuperados, pero no se encuentran ejecutando en su lugar original o bajo las mismas condiciones en que se encontraban originalmente. Al finalizar el proceso de actualización de la información o "catch up", se considera que se ha llegado a la operación normal en desastre. El tiempo desde la declaración de la emergencia hasta que se alcanza la operación normal en desastre no debe ser superior a los tiempos máximos tolerables de suspensión definido para cada una de las prestaciones.

d) Operación Normal Reestablecida:

Mediante la ejecución de los procedimientos que reciben el nombre de "Reestablecimiento de las condiciones normales" se alcanza esta última instancia, en la cual todos los servicios y aplicaciones se encuentran ejecutando correctamente y bajo las mismas condiciones que presentaba antes de la contingencia.

Para alcanzar este tipo de operación, es posible que haya que considerar una suspensión programada de alcance total o parcial de las prestaciones, para lo cual es necesario acotar el tiempo de interrupción al mínimo indispensable, y que preferentemente sea imperceptible por los usuarios.

2.3. IDENTIFICACIÓN DE SISTEMAS DE INFORMACIÓN Y ACTIVOS CRÍTICOS

La idea es que en esta etapa se establezca la criticidad de las aplicaciones, de los equipos y los servicios que sostienen al negocio. En función del impacto producido por la suspensión de las prestaciones del entorno informatizado, se determina la criticidad y el tiempo máximo de tolerancia de corte de las mismas.

En La Tabla de Criticidades por Equipo se deberá tener mayor foco al momento de definir la estrategia de recuperación a los tienen una criticidad alta y menor tiempo de tolerancia.

Tabla de Criticidades por Equipo

Nº	Equipo	Función	Sistema Operativo	Factor Crítico	Tolera	Impacto
01	PC usuario	Terminal	Windows 10/11 32/64bits	Media	1 día	Retrasos a nivel operativo
02	Servidor SIINCO	Servidor de Bases de Datos	Centos 7 / SyBASE 64bits	Alta	½ día	Pérdida de imagen pública/Paralización de Servicios Comercial
03	Servidor SGD	Servidor de Bases de Datos	Centos 7/ Oracle 64bits	Alta	½ día	Pérdida de imagen a nivel interno /Paralización de Servicios del Sistema de Gestión Documental
04	Servidor AVALON	Servidor de Base de Datos	Windows Server 2008/Visual FoxPro 64bits	Alta	½ día	Pérdida de imagen a nivel interno /Paralización de Servicios del Sistema AVALON
05	Servidor SIAF	Servidor de Base de Datos	Windows Server 2008/ Visual FoxPro 64bits	Alta	½ día	Pérdida de imagen a nivel interno /Paralización de Servicios del SIAF
	Servidor de Aplicaciones	Aplicaciones SIINCO, SGD	Centos 7/ PowerBuilder, PAYARA	Alta	1 día	Pérdida de imagen a nivel interno /Paralización de Servicios del SIINCO y SGD
06	Servidor GIS	Servidor de Base de Datos	Centos7/ PostGreeSQL 64bits	Alta	½ día	Pérdida de imagen a nivel interno /Paralización de Servicios del GIS
07	ServerWEB	Web/Correo/ FTP	CentOS 7 Linux 64bits 6.4	Media	1 día	Pérdida de imagen pública/Inconsistencia de Información
08	ServidorRemoto	Teminal Server MStsc 2008	Windows Server 2008 R2 64bits	Alta	½ día	Pérdida de imagen pública/Inconsistencia de Información
09	ServerVideoCam	Video Vigila Cámara	Windows Server 2008	Baja	2 día	Pérdida de Información

Tabla de Criticidades por Servicios

Nº	Servicio	Criticidad	Período crítico	Procedim. Alternat.	Parada Máxima	Plataf. S.O.	Usuarios
01	Web	Alta	Diario	Anexo 1	2 días	CentOS Linux 64bits 6.4	Internet
02	Correo	Alta	Diario	Anexo 1	½ días	CentOS Linux 64bits 6.4	Todos de SEDA AYACUCHO S.A.
03	Ftp	Baja	Semanal	Anexo 1	3 semanas	CentOS Linux 64bits 6.4	Unidad de Informática
04	Firewall	Alta	Diario	Anexo 1	½ días	CentOS Linux 32bits 5.3	Intranet
05	Archivos	Baja	Mensual	Guardar los archivos en PC locales	1 mes	Windows 7/8	Todos de SEDA AYACUCHO S.A.

2.4. ANÁLISIS DE RIESGOS

A la hora del análisis se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles con el fin de que se puedan priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado. Identificamos los objetos que deben ser protegidos, de daños que puedan sufrir, sus posibles fuentes de daño y oportunidad, su impacto en la empresa.

El análisis de riesgos supone responder a preguntas del tipo:

- ¿Qué puede ir mal?
- ¿Con qué frecuencia puede ocurrir?
- ¿Cuáles serían sus consecuencias?
- ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

2.5. EVALUACIÓN DE RIESGOS

Ya sabemos que es imposible medir con exactitud los riesgos, solo podemos basarnos en un análisis de los mismos. La idea de cuantificar el riesgo en esta etapa es poder reducir el mismo lo antes posible mediante el desarrollo del plan. Debemos determinar qué nivel de riesgo está dispuesto a tolerar la empresa y estar conscientes que como cada desastre puede llegar a ser único, es imposible definir estrategias para cada posibilidad.

En esta etapa comenzaremos contestando, con la mayor fiabilidad posible, a las siguientes preguntas:

- ¿Qué se intenta proteger?
- ¿Cuál es su valor para uno o para la organización?
- ¿Frente a qué se intenta proteger?
- ¿Cuál es la probabilidad de un ataque?

a) Riesgos en la seguridad informática a que se enfrenta la Empresa.

- Fallas del suministro eléctrico, que dañen los equipos.
- Incendio, que puede destruir los equipos y archivos.
- Robo común, llevándose los equipos.
- Fallas de hardware y software, que dañen los archivos.
- Errores del usuario, que dañen los archivos.
- Acción de virus, que dañen los equipos y archivos.
- Terremotos, que destruyen los equipos y archivos.
- Accesos no autorizados, filtrándose datos importantes.
- Robo de Datos: difundiéndose los datos.
- Fraude, desviando fondos merced a la computadora.

b) Probabilidad de efecto alguno de los riesgos mencionados

PREGUNTA	RESPUESTA
Fallas eléctricas, que dañen los equipos	
¿La Empresa cuenta con grupo electrógeno?	No
¿Se cuenta con Planos Eléctricos de la distribución del cableado?	No
¿Esta falla cuánto daño puede ocasionar?	10%
Incendio que destruyen los equipos y los archivos	
¿La Empresa cuenta con protección contra incendios?	No
¿Se cuenta con sistema de aspersión automática?	No
¿Diversos Extintores?	No
¿Detectores de Humo?	No
¿Los empleados están preparados para un posible incendio?	No
Robo común, llevándose los equipos	
¿En qué tipo de vecindario se encuentra la Empresa?	Medianamente seguro
¿Hay venta de drogas?	No
¿Las computadoras se ven desde la calle?	No
¿Hay personal de seguridad en la Empresa?	Si

¿Cuántos vigilantes hay?	2 turno día y 1 turno noche
Fallas de Hardware y Software, que dañen los archivos	
¿Los equipos tienen mantenimiento continuo por parte de personal calificado?	2 veces por año
¿Cuáles son las condiciones actuales de Hardware?	Regulares
¿Es posible predecir las fallas a que están expuestos los equipos?	Sí, es posible saberlo
¿Los softwares tienen actualización continua?	Si
Errores de los usuarios que dañen los archivos	
¿Cuánto saben los empleados de computadoras o redes?	Un nivel medio
Los que no conocen de manejo de computadoras, ¿Saben a quién pedir ayuda?	Si
Durante el tiempo de vacaciones de los empleados, ¿Qué tipo de personal los sustituye y que tanto saben del manejo de computadoras?	Un nivel medio
La acción de virus que dañen los archivos	
¿Se prueba software sin hacer un examen previo de virus?	No
¿Está permitido el uso de Medios de Almacenamiento Extraíbles (Discos externos, USBs, Memorias USB, CD, DVD) en la oficina?	Si
¿Todas las máquinas tienen algún Medio de Almacenamiento Extraíbles?	Si
¿Se cuenta con procedimientos contra virus?	Si
Terremotos que destruyan los equipos y archivos	
¿La Empresa se encuentra en zona sísmica?	Sismicidad media
¿El local cumple con las normas antisísmicas?	No
Un terremoto, ¿Cuánto daño podría causar?	60%
Accesos no autorizados, filtrando datos importantes	
¿Cuánta competencia hay para la Empresa?	Ninguna
¿Qué probabilidad hay que un competidor intente hacer un acceso no autorizado?	Ninguna
¿El Módem-Router se usa para comunicarse fuera y también se puede utilizar para comunicarse hacia dentro?	Si
¿Contamos con sistema de seguridad en el servidor?	Si
¿Contamos con seguridad en Internet?	Si
Robo de Datos: difundiéndose los datos	
¿Cuánto valor tiene actualmente las Bases de Datos?	Muy Importante (Factor crítico)
¿Cuánta pérdida podría causar en caso de que se hicieran públicas?	Media
¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?	No

c) Probabilidad de efecto en el Sistema de Información ante riesgos.

PREGUNTA	RESPUESTA
Fraude desviando fondos merced a la computadora.	
¿Cuántas personas se ocupan del Sistema Comercial?	45
¿Cuántas personas se ocupan del Sistema Administrativo?	18
Las personas que trabajan en los sistemas de información de la empresa ¿Qué tipo de antecedentes laborales tiene?	Bueno
¿Existe acceso a los sistemas de información de la empresa desde otros sistemas o personas?	No, únicamente los encargados, ya que está protegido por dominio
¿Existen sistemas que manejen cuentas corrientes?	Si
¿Existen posibles manipulaciones en los archivos de cuentas corrientes?	Si
¿Existen algún sistema de seguridad para evitar manipulaciones en determinados archivos?	No
¿Cuántas personas se ocupan de la contabilidad de la Empresa?	6
¿El sistema Comercial y Administrativo de la empresa es confiable?	Intermedia (SIINCO) Intermedia (Gestor)
Las personas que trabajan en el departamento de contabilidad ¿Qué tipo de antecedentes laborales tiene?	Bueno
¿Existe acceso al Sistema de Contabilidad desde otros sistemas o personas?	No
¿El sistema de contabilidad es confiable?	Intermedia (Gestor)

d) Probabilidad de Factor de Riesgo

RIESGOS	FACTOR DE RIESGO		
	ALTA	MEDIA	BAJA
A fallas eléctricas que dañen los equipos		X	
Incendio, que pueda destruir los equipos y archivos			X
Al robo común, llevándose los equipos y archivos			X
Fallas de Hardware y Software que dañen los archivos			X
A errores del usuario que dañen los archivos		X	
A la acción de virus que dañen los equipos y archivos		X	

A terremotos que destruyen el equipo y los archivos			X
A accesos no autorizados, filtrándose datos importantes			X
A robo de datos, difundiéndose los datos sin cobrarlos			X
Al fraude, desviando fondos merced a la computadora			X

2.6. EVALUACIÓN DE FALLAS

A continuación, se determina las potenciales fallas informáticas en la Empresa:

a. FALLAS FÍSICAS:

- Error Físico del Disco Duro: El dispositivo especificado, presenta fallas no salvables por ninguno de los programas de recuperación.
- Error de Memoria RAM: El equipo de cómputo presenta errores en mapas de direcciones hexadecimales o cuando no tiene una performance muy baja de tiempo de respuesta.
- Error de Tarjeta Controladora de Disco: Cuando ocurre esto no se tiene acceso al disco.
- Problemas en la Placa Madre: Producido por conexiones defectuosas entre componentes internos, condensadores hinchados o daños en los componentes integrados.
- Fallas en la tarjeta Gráfica: Pueden experimentar problemas como artefactos visuales, pantalla en blanco o negra, y en algunos casos el mal funcionamiento del ventilador de enfriamiento.
- Falla de la Fuente Interna del Computador: Por cambio de tensiones y tiempo de uso y mala conexión a tierra.
- Falla Física del Switch: No permite el acceso a la red, esto se produce por cambio de tensiones o por estar sin equipos de protección eléctrica.
- Ruptura de hilos de Cable de Conexión UTP: Corte de la conexión de red.

b. FALLAS LÓGICAS:

- Falla en el Software de red: Produce una caída del servidor o estaciones de trabajo no envían la información.
- Falla en el software del sistema operativo: Se produce una caída del servidor o equipos de cómputo.

- Incompatibilidades de software: Paralización o fallas de algunos servicios por existencia de conflictos entre diferentes componentes de software, versiones incompatibles.
- Falla en el Software de aplicaciones: Las aplicaciones instaladas en el computador no funcionan correctamente.
- Manipulación errada de información: Ingresos de virus en el sistema, error de digitación por parte de los usuarios.
- Configuración incorrecta: Mal funcionamiento del equipo.

c. FALLAS ELÉCTRICAS:

- Falla del UPS: Corte intempestivo de la corriente eléctrica.
- Falla de la red eléctrica: Corto circuito, picos en los equipos de cómputo, inestabilidad en calidad de la energía.
- Fallas en la toma de tierra: Aumenta el riesgo de daño a los dispositivos y representar un peligro para la seguridad eléctrica.

d. FALLAS DE AMBIENTACIÓN:

- Falla del aire acondicionado: Recalentamiento de los equipos, propensos a corto circuito.

FALLAS VS. IMPACTO

IMPACTO / FALLA	ALTO	MEDIO	BAJO
Error Físico del Disco Duro	X		
Error de Memoria RAM		X	
Error de Tarjeta Controladora de disco	X		
Fallas en la Placa Madre	X		
Fallas en la Tarjeta Gráfica		X	
Error de Fuente Interna del Computador	X		
Falla de la Tarjeta de Red		X	
Error físico de Switch	X		
Ruptura de Hilos de cable de conexión (UTP)	X		
Falla del Software de Red	X		
Falla del Software del Sistema Operativo	X		
Incompatibilidad de Software	X		
Falla de Software de Aplicativos	X		
Manipulación inadecuada de la Información	X		
Configuración incorrecta			

Falla de los UPS	X		
Falla de la Red Eléctrica	X		
Fallas en la Toma de Tierra		X	
Falla del Aire Acondicionado		X	

2.7. PLAN DE RECUPERACIÓN DE FALLAS Y/O DESASTRES

Es importante definir los procedimientos y planes de acción antes, durante y después de la ocurrencia de la falla, siniestro o desastre dentro de la Empresa SEDA AYACUCHO S.A. a fin de recuperar la total o mayor parte de información, archivos y equipos informáticos, evitando así la pérdida de tiempo y dinero. Las actividades a realizar en el Plan de Recuperación de fallas y/o desastres se pueden clasificar en tres etapas:

- Actividades previas a la contingencia.
- Actividades durante la contingencia.
- Actividades después de la contingencia.

2.7.1. ACTIVIDADES PREVIAS A LA CONTINGENCIA

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de información y equipos informáticos, que nos aseguren el proceso de recuperación de los mismos.

a. ESTABLECIMIENTO DE PLAN DE ACCIÓN

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a: Sistemas e Información, equipos de Cómputo, obtención y almacenamiento de los Respaldos de Información (BACKUPS), Políticas (Normas y Procedimientos de Backups).

- **SISTEMAS DE INFORMACIÓN.**

La Empresa tiene una relación de los Sistemas de Información con los que cuenta, tanto los realizados por Unidad de Informática como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

La relación de Sistemas de Información deberá detallar los siguientes datos:

- ✓ Nombre del Sistema.
- ✓ Lenguaje o Paquete con el que fue creado el Sistema, programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.)
- ✓ Las unidades que usan la información del Sistema.
- ✓ El volumen de los archivos que trabaja el Sistema.

- ✓ El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- ✓ El equipamiento necesario para un manejo óptimo del Sistema.
- ✓ La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- ✓ El nivel de importancia estratégica que tiene la información de este Sistema para la Empresa (medido en horas o días que la Empresa puede funcionar adecuadamente). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en dos turnos de trabajo, para que el equipamiento sea el mínimo posible).
- ✓ Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

➢ **EQUIPOS DE CÓMPUTO:**

Se tendrá en cuenta:

- ✓ Inventario actualizado de los equipos de manejo de información (computadoras, impresoras, etc.) especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso en la empresa.
- ✓ Pólizas de Seguros Comerciales. Como parte de la protección de los activos institucionales, pero haciendo la salvedad en el contrato que, en casos de siniestros, la restitución del computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.
- ✓ Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo, etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC's con información importante o estratégica y color verde a las PC's de contenidos normales.

➢ **OBTENCIÓN Y ALMACENAMIENTO DE LOS RESPALDOS DE INFORMACIÓN (BACKUPS):**

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la empresa, para lo cual se debe contar con:

Backups del Sistema Operativo, Backups del Software Base, Backups del Software Aplicativo, Backups de los Datos, Backups del Hardware (Externa, Interna).

- **POLÍTICAS (NORMAS Y PROCEDIMIENTOS DE BACKUPS):**

Se debe establecer los procedimientos, normas y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente.

- ✓ Respaldo de Información de movimiento entre los períodos que no se cuenta con Backups (backups incrementales).
- ✓ Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del dispositivo de almacenamiento empleado.
- ✓ Reemplazo de los Backups, en forma periódica, antes que el dispositivo de almacenamiento de soporte se pueda deteriorar (reciclaje o refresco).
- ✓ Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.
- ✓ Las copias de seguridad deberá realizarse en forma diaria en el disco duro de una estación de trabajo, en la nube; mensualmente la copia que se encuentra en la estación de trabajo se deberá grabar en un dispositivo de almacenamiento en tres copias (03 copias) de las cuales una copia son entregados al Gerente General para su resguardo, una copia deber ser almacenado fuera del local institucional en un lugar protegido de polvo, humedad y sismo, etc. y una copia que permanecerá a la oficina de El Departamento de Sistemas y Tecnologías de Información.
- ✓ Los archivos de las estaciones de trabajo son de absoluta responsabilidad del operador de dicho equipo, el usuario del equipo debe coordinar con El Departamento de Sistemas y Tecnologías de Información para realizar las copias de seguridad de sus archivos personales de trabajo.

b. FORMACIÓN DE EQUIPOS OPERATIVOS

Todas las áreas u oficinas de la SEDA AYACUCHO S.A., que almacenen información y sirva para la operatividad institucional, deberán designar un responsable de la seguridad de dicha información. Pudiendo ser el Jefe del Departamento o el trabajador que maneje directamente la información. Entre las acciones a tomar por el Área de Informática conjuntamente con las oficinas serán:

- ✓ Ponerse en contacto con los desarrolladores y/o propietarios de las aplicaciones y trabajar con ellos.
- ✓ Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.

- ✓ Supervisar procedimientos de respaldo y restauración.
- ✓ Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.

2.7.2. ACTIVIDADES DURANTE EL DESASTRE

Una vez presentada la Contingencia, se deberá ejecutar las siguientes actividades:

a. PLAN DE EMERGENCIAS

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre la contingencia. Si bien es cierto la integridad de las personas es lo primordial, se deben adoptar medidas con el fin de asegurar la información:

- ✓ Apagar los equipos inmediatamente después de haber detectado el siniestro.
- ✓ Desconexión del equipo para su retiro del lugar del siniestro.
- ✓ Salir rápidamente a través de las vías de escape.
- ✓ Proteger y cubrir los equipos.
- ✓ Enseñanza del manejo de extintores.

En caso de contingencias como fallas en equipos de cómputo, fallas humanas, acción de virus, etc.; lo más recomendable es solicitar la ayuda del personal informático, si es que en el área no existe una persona capacitada para resolver el problema.

b. ENTRENAMIENTO

El personal de la SEDA AYACUCHO S.A. tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos. Para el cual se comunicará al personal los días de las charlas de Seguridad Institucional.

2.7.3. ACTIVIDAD DESPUÉS DE LA CONTINGENCIA

a. EVALUACIÓN DE DAÑOS.

Inmediatamente después que la contingencia ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

b. PRIORIZACIÓN DE ACTIVIDADES DEL PLAN DE ACCIÓN.

La evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Empresa. Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignamiento temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

Prioridad de Atención	Descripción
1	**Atención Prioritaria:** Servicio de Internet, correo electrónico, Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información: Servidores de base de datos, SIINCO, Portal Web institucional, Sistema de pago on-line, Call-Center, entre otros.
2	**Atención Normal:** Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información: Avalon, SIAF, GIS, Servidor de correo, Servicio de Video Vigilancia, etc.
3	**Atención Baja:** Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Asimismo, equipos apoyo: SGD y equipos terminales.

c. EJECUCIÓN DE ACTIVIDADES.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de

los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

d. EVALUACIÓN DE RESULTADOS.

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por la contingencia, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

e. RETROALIMENTACIÓN DEL PLAN DE ACCIÓN.

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

3. ORGANIZACIÓN PARA EL PLAN DE CONTINGENCIAS

3.1. ROLES Y RESPONSABILIDADES

El Departamento de Sistemas y tecnologías de Información tiene dentro de sus funciones desarrollar e implementar la políticas de seguridad promoviendo la privacidad y control de datos en el acceso de la base de datos institucional, así como, establecer mecanismos de registro histórico de modificaciones, autenticación de los usuarios, auditoría y control de accesos a la base de datos; además de diseñar, construir, implantar, mantener los sistemas informáticos e infraestructura tecnológica necesaria para el cumplimiento de los objetivos de SEDA AYACUCHO S.A., así como, asegurar la disponibilidad y brindar soporte a los servicios.

3.2. RESPONSABLES DE LA EJECUCIÓN DEL PLAN

- Gerente General
- Jefe del Departamento de Sistemas y TI
- Especialista en Sistemas
- Especialista en Informática
- Analista en Informática

RESPONSABILIDADES

- **Del Gerente General:**
  - Brindar apoyo mediante coordinaciones del nivel que le compete (convenios, solicitudes de apoyo externo, etc.)
  - Supervisar en coordinación con el Jefe del Dpto. de Sistemas y TI la Ejecución del Plan.
  - Ordenar el Apoyo Logístico necesario para la ejecución del Plan.

- **Del Jefe del Departamento de Sistemas y TI**
  - Dirección Técnica de la Ejecución del Plan.
  - Coordinación con la Gerencia General, áreas usuarias y el personal bajo su responsabilidad.
  - Brindar Apoyo Técnico Operativo.
  - Coordinar y mantener actualizado el Plan de Contingencias.

- **Del Especialista en Sistemas**
  - Apoyo total en la Ejecución del Plan.

- Dirección del Plan en Contingencias Menores.
- Coordinar con la Jefatura del Departamento de Sistemas y TI los requerimientos mínimos y/o detalles concernientes a la Ejecución del Plan.
- Coordinar al Apoyo Logístico.
- Mantener al día los "backups" del Sistema, de los aplicativos y otros. Llevar al día la documentación de éstos en caso se requiera desplegar y/o reinstalar los aplicativos informáticos y sistemas.
- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones, así como el servidor de base de datos.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los aplicativos informáticos y sistemas de información de SEDA AYACUCHO S.A.

➢ **Del Especialista en Informática**

- Apoyo total en la Ejecución del Plan.
- Coordinar con la Jefatura del Departamento de Sistemas y TI los requerimientos mínimos y/o detalles concernientes a la Ejecución del Plan.
- Debe iniciar el proceso de recuperación de los servicios tecnológicos de la información, realizando las pruebas de funcionamiento en los equipos componentes del Centro de Datos.
- Restaurar la Información de los equipos afectados de la infraestructura informática que afectan los servicios TI.
- Notificar al Jefe del Dpto. de Sistemas y TI las acciones de recuperación realizadas.
- Elaborar un informe técnico que incluya las acciones de recuperación de los equipos de comunicaciones y los equipos componentes del Centro de Datos.
- Supervisar la restauración de los servicios de TI
- Validar la información documentada de los procedimientos de restauración utilizados.

➢ **Del Analista en Informática**

- Apoyo total en la Ejecución del Plan.
- Iniciar con el proceso de recuperación con el servicio relacionado a la red de comunicaciones.

- Realizar la evaluación de las redes de comunicación, así como de equipos terminales y su operatividad.
- Elaborar un informe técnico que incluya las acciones de recuperación de equipos de comunicación, equipos terminales, etc.

4. PROCESOS Y PROCEDIMIENTOS PARA EL PLAN DE CONTINGENCIAS

Tiene como objetivo identificar aquellos procesos que sin los cuales la empresa no podría operar y que tienen prioridad para ser restaurados en caso de pérdida de información.

4.1. PROCESOS CRÍTICOS DENTRO DE LAS FUNCIONES ORGANIZACIONALES

4.1.1. COMERCIAL

- Función
  - Comercialización
  - Catastro de Clientes y Ventas
  - Medición y Facturación
  - Cobranzas
  - Atención al Cliente

- Procesos Críticos
  - Atención al cliente
    - Reclamos
  - Facturación
    - Lecturas
    - Cargar la Base de Datos
    - Emisión de recibos
    - Distribución de recibos
  - Cobranzas
    - Recaudación, Cortes y Reconexiones

4.1.2. ADMINISTRATIVA

- Función
  - Contabilidad
  - Tesorería
  - Personal
  - Logística

- Procesos Críticos
  - Contabilidad (Base de Datos de Débitos y Créditos)

4.1.3. TECNICO

- Función
  - Producción
  - Distribución
  - Ingeniería
  - Mantenimiento

- Procesos Críticos
  - Distribución
    - Instalaciones nuevas

4.1.4. RESPONSBLES

Proceso	Responsable
Comercialización	Jefe de la Gerencia Comercial
Facturación	Jefe del Departamento de Facturación
Cobranza	Jefe del Departamento de Cobranzas
Catastro	Jefe del Departamento de Catastro
Medición	Jefe del Departamento de Medición
Contabilidad General	Jefe del Departamento de Contabilidad
Distribución	Jefe del Departamento de Distribución

5. RECURSOS E INFRAESTRUCTURA

- **RECURSOS HUMANOS**

  Los recursos humanos a utilizarse estarán constituidos por el personal del Departamento de Sistemas y Tecnologías de Información y el responsable del proceso.

- **SUMINISTROS**

  Los suministros básicos a emplearse serán aquellos dispositivos de almacenamiento en los que se contengan las copias de respaldo; es decir CD/DVD,. USBs, cintas de tape backup o disco duro extraíbles o de una estación de trabajo, etiquetas, formularios para impresión en cantidad suficiente.

- **ENERGÍA ELÉCTRICA**

  Se contará como fuente de suministro de energía eléctrica a las fuentes convencionales de electricidad y también la posibilidad de contar con un grupo electrógeno (Se recomienda que el grupo electrógeno sea de honda Sinusoidal-No cuadrática).

- **EQUIPOS**

  Se deberá considerar la posibilidad de utilizar otro computador de SEDA AYACUCHO S.A. como servidor o en su defecto la posibilidad de obtener otro de fuente externa; también es necesario determinar que estaciones de trabajo puedan reemplazar a las que se encuentran en los puntos críticos.

- **DETERMINACIÓN DE UNA LOCALIDAD EXTERNA**

  SEDA AYACUCHO S.A. buscará una empresa de características similares a fin de establecer un convenio recíproco, para poder seguir operando en caso de pérdida total de información y equipos.

6. PLAN DE PRUEBAS Y MANTENIMEINTO

Tiene por objetivo probar que el Plan de Contingencias funcionan, pues "Probar es convertir el Plan de Contingencias de la Empresa, de un concepto planeado a una realidad".

➢ GENERALIDADES DE LA PRUEBA

La prueba simulará una "Caída" total del servidor de la Red y algunos periféricos, de tal manera que en nuestro desastre supuesto quedarán inutilizados los siguientes equipos:

- Servidores de Red.
- Estaciones de Facturación.
- Estaciones de Cobranzas.
- Estaciones de Contabilidad.
- Se verificará que el tiempo de los procesos está dentro de lo esperado por el área usuaria.

➢ RECURSOS

- Para ejecutar la prueba se deberá seleccionar aquellos computadores que tengan las características más posibles a los computadores supuestamente inutilizados.
- Se contará con los dispositivos de almacenamiento de las copias de respaldo; es decir disco duro de una estación de trabajo, usb, tarjetas de memoria, CD/DVD.

➢ ACTIVIDADES

- Anotación de tiempos de inicio y final de la prueba.
- Instalación del Servidor Windows 2008.
- Conexiones de Estaciones de Trabajo.
- Instalación del Software, Aplicativos y Bases de Datos.
- Estimación del tiempo de digitación de la data supuestamente perdida.
- Prueba que lo instalado funciona.
- Conclusiones y Recomendaciones para mejorar / actualizar el Plan.
- Generar un documento con el resultado de la prueba.

7. ANEXO

7.1. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona, de ahí que resulte obvio el interés creciente que día a día se evidencia sobre este aspecto de la nueva sociedad informática. La seguridad de la información tiene dos aspectos importantes como:

7.1.1. PROTECCIÓN CONTRA VIRUS

Tiene por objetivo evitar la infección de la Red con virus informático, tomándose en cuenta las siguientes consideraciones:

✓ Solo los computadores de El Departamento de Sistemas y Tecnologías de Información contarán grabador de CD/DVD.

✓ Todo archivo contenido en disco externo, USB y CD/DVD de procedencia externa deberá ser revisado por el usuario con un antivirus actualizado antes de ser copiada la información a la Red o pc del trabador.

✓ Las estaciones que tengan Puerto USB y lectora de CD/DVD deberán contar necesariamente con antivirus residentes.

✓ Los usuarios de las estaciones que tengan acceso a Internet son responsables de bajar (download en inglés) programas, archivos, etc. de sitios web (pudiendo ser estos confiables o no confiables). Los programas, archivos, etc. bajados desde Internet pueden contener virus informático, código informático malicioso, etc. que pueden dañar los archivos del equipo o la red. Estos equipos deberán contar necesariamente con antivirus residente actualizado.

✓ Los antivirus deberán ser actualizados cada vez que sale una nueva versión; por razones de orden económico y la periodicidad de la compra, los antivirus a adquirirse serán de licencia corporativa.

7.1.2. ACCESO NO AUTORIZADO

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a: Área de Sistemas, Computadoras personales y/o terminales de la red, Información Confidencial.

✓ Control de Acceso al Área de Sistemas: El acceso normal debe ser dado solamente a la gente que regularmente trabaja en esta área. Cualquier otra persona, de otro modo

debe tener acceso únicamente bajo control. Es necesario considerar alarmas como prevención frente a cualquier contingencia no prevista. Como un detector de humo.

✓ Acceso limitado a los terminales: Los terminales que son dejados sin protección pueden ser mal usados. Cualquier terminal que puede ser utilizado como acceso a los datos del sistema controlado, debe ser encerrado en un área segura o guardado, de tal manera que no sean usados, excepto por aquellos que tengan autorización para ello. Igualmente, se deberá considerar la mejor manera de identificar a los operadores de los terminales del sistema, y el uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5-10 Min). Restricciones que pueden ser aplicadas: Determinación de los periodos de tiempo para los usuarios o las terminales. Designación del usuario por terminal o del terminal por usuario. Limitación del uso de programas para usuarios o terminales. Límite de tentativas para la verificación del usuario. Tiempo de validez de las señas.

✓ Control de acceso a la Información: Deben existir programas protegidos que mantengan y controlen a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente. Debe existir autenticación por password. El sistema de computación debe cerrarse después que un individuo no autorizado falle dos veces al intentar ingresar una clave de acceso. En todo proceso corporativo es recomendable que el responsable de cada área asigne y actualice en forma periódica el password a los usuarios.

✓ No se puede depender de que la ausencia de un operador o responsable de un computador trabe la operatividad normal de una Empresa, por lo que es necesario el establecer la cuenta de Administrador cuya clave es conocida solo por los administradores de sistemas de El Departamento de Sistemas y Tecnologías de Información. Además, se debe contar con el password del usuario, lacrado en un sobre el cual debe estar entregado al Jefe inmediato superior tendrá en un sobre lacrado, los passwords de su personal, debiendo utilizar un cuaderno de control, cuando exista la necesidad de romper el sobre lacrado (anotando fecha, hora, motivo, etc.), así como un procedimiento de cambio de password periódicos y por dichas eventualidades.

7.1.3. NIVELES DE ACCESO.

Se tienen los siguientes niveles de acceso a la información:

✓ Nivel de consulta de la información con autorización de lectura permite leer, pero no modificar la base de datos.

✓ Nivel de mantenimiento de la información, el concepto de mantenimiento de la información consiste en: Ingreso: Permite insertar datos nuevos, pero no se modifica los ya existentes. Actualización: Permite modificar la información, pero no la eliminación de datos. Borrado: Permite la eliminación de datos. Un usuario puede tener asignados todos, ninguno o una combinación de los tipos de autorización anteriores. Además de las formas de autorización de acceso de datos antes mencionados, es posible autorizar al usuario para que modifique el esquema de la base de datos, pero es preferible que esta función sea de responsabilidad de El Departamento de Sistemas y Tecnologías de Información.

✓ Nivel de Administrador, la forma fundamental de autoridad es la que se le da al administrador del sistema, que entre otras cosas puede autorizar nuevos usuarios, reestructurar la base de datos, etc. Esta forma de autorización es análoga a la que se provee a un "super usuario" o al operador para un sistema operativo.

7.1.4. PROTECCIÓN ESPECIAL DE LA INFORMACIÓN

La protección de información reservada en un canal de comunicación, es esencial. Uno de los principales métodos para ofrecer protección es hacer que la información del mensaje sea ilegible por medio de técnicas criptográficas, sin intentar ocultar la existencia del mensaje.

✓ Encriptación, Es una técnica mediante la cual se transforman los datos de forma que no proporcionen información al ser interceptados, puesto que tal como están almacenados o transmitidos son completamente ilegibles. Las técnicas de cifrado pueden ser Criptografía de clave simétrica o Criptografía de clave asimétrica.

7.2. INTEGRIDAD DE LA INFORMACIÓN

La integridad de la información objetivo que sólo se almacena la información correcta, contenida en una base de datos.

7.2.1. CONCURRENCIA

En un sistema de gestión de base de datos existen problemas conocidos como concurrencia, que se generan cuando existen procesos en los que dos o más usuarios deben acceder y/o actualizar la misma información de una base de datos, para lo cual deben prevenirse los errores semánticos, que resultan de la interacción de dos o más procesos que operan simultáneamente en una base de datos. Existen mecanismos

como: sistema de gestión de base de datos centralizado, el mecanismo consiste en bloquear la porción de los datos durante la actualización, para prevenir resultados inconsistentes que puedan generarse. Cuando una transacción accede a un registro bloqueado, espera hasta que el bloqueo sea eliminado y el registro esté nuevamente en un estado consistente. Una base de datos es coherente si después de ejecutar varias transacciones concurrentes, su estado es idéntico al que hubiera tenido, si es que éstas se hubiesen ejecutado consecutivamente en cualquier orden.

7.2.2. AUDITORIA DE SISTEMAS

La auditoría informática es una función cuya misión es garantizar la seguridad, eficacia y rentabilidad del Sistema de Información. Esto es de gran importancia y se ve amenazada por factores intrínsecos de alto riesgo ya que, fallas en los sistemas informáticos pueden generar graves daños, materializados en pérdidas de patrimonio y operatividad, distorsiones en el servicio, inconsistencia en la gestión y deterioro de la imagen.

Los objetivos de la auditoria de sistemas son: implementar los controles necesarios en el ámbito global de los sistemas y establecer las especificaciones necesarias para la verificación y adecuación de éstos, de modo tal que se asegure la exactitud, seguridad e integridad de los sistemas y sus resultados.

7.2.3. CALIDAD DE UN SISTEMA DE INFORMACIÓN

La calidad de un sistema de información no sólo se logra con un buen diseño del sistema o con un bajo nivel de riesgo. Para asegurar la calidad es necesario, además, revisar la documentación asociada al software con el objetivo de verificar su cobertura, corrección, confiabilidad y facilidad de mantenimiento. Para obtener la calidad mencionada anteriormente, en el análisis y diseño de los sistemas debe contemplarse los siguientes niveles:

✓ Nivel de Prueba. Debido a que en el desarrollo de un sistema no puede demostrarse que esté exento de errores, el concepto de prueba puede definirse como el proceso de ejecutar un programa con la finalidad de encontrar errores o fallas, los mismos que deben corregirse para dar mayor confiabilidad a un sistema.

✓ Nivel Verificación y Validación. De manera similar al anterior, la verificación permite hallar errores y se realiza al ejecutar un programa en un ambiente simulado. La validación consiste en un proceso hacer trabajar al sistema en un ambiente real, en el

cual se procesan las transacciones en directo, emitiendo las salidas normales. No puede establecerse un periodo de validación que puede ser corto o prolongado. Mientras dure, el sistema puede fallar y se tiene que proceder a su modificación.

✓ Certificación. La certificación consiste en garantizar que un sistema de información o software determinado esté correcto. Existen normas internacionales que tratan sobre este punto (Ver ISO 9000).

Las Pruebas de sistemas persigue la integración de cada módulo en el sistema, así como, buscar las discrepancias entre el sistema y sus especificaciones y documentación del mismo. Entre las pruebas especiales de sistemas se pueden considerar las siguientes:

✓ Prueba de Carga Máxima. Se basa en la existencia de tiempos críticos en los sistemas en línea, es decir, la respuesta de un sistema en prueba cuando varios usuarios quieren acceder a ella. Por ejemplo, cuando se prenden todas las terminales en un sistema comercial.

✓ Prueba de Almacenamiento. Mediante esta prueba se determina si el sistema realmente soporta la capacidad (número de registros que un archivo puede almacenar en disco) considerada en su diseño, la misma que debe ser verificada antes de la implantación.

✓ Prueba del Tiempo de Ejecución. Permite conocer qué tan rápido o lento es el sistema y debe realizarse antes de la implantación del mismo, para primero determinar el tiempo que toma recibir una respuesta a una consulta, hacer una copia de respaldo de un archivo o mandar una transmisión y recibir una respuesta, así como, indexar grandes archivos o preparar reportes, y segundo, realizar los ajustes necesarios.

✓ Prueba de Recuperación. La prueba de recuperación consiste en crear un evento de fallas o pérdida de datos, para que los usuarios vuelvan a cargar y recuperar a partir de una copia de respaldo. Con ello, se determina si los procedimientos de recuperación, son los más adecuados para cuando el sistema falle y no se pierdan los datos.

✓ Prueba de Procedimientos. Con esta prueba se determina si los manuales de documentación y ejecución contienen una descripción detallada y si refleja realmente las acciones que se llevan a cabo para el funcionamiento del sistema. Para ello, el usuario debe seguir las instrucciones en forma exacta, como se indica en el manual de procedimientos.

✓ Prueba de Factores Humanos. Esta prueba consiste en hallar repuestas sobre la reacción de los usuarios, cuando interactúen con el sistema y sucedan imprevistos. Como: Los mensajes que deben aparecer en la pantalla cuando un usuario esté procesando una transacción. Observar a las personas si tienen facilidad de manejo del teclado para el ingreso de datos. Comodidad de los usuarios frente a lo mostrado en la pantalla (color, resplandor, mucho detalle, etc.).

7.3. MEDIDAS PREVENTIVAS CONTRA AMENAZAS

7.3.1. EXTINGUIDORES MANUALES

El personal designado para usar extinguidores de fuego debe ser entrenado en su uso, recibir algunas lecciones de instrucciones en el mecanismo de lucha contra el fuego, examinar el potencial del problema y tomar las medidas apropiadas para impedir la entrada de humo. Colocando adecuadas cubiertas plásticas para todo el equipo, escritorios y cabinas, puede ayudar a reducir el daño ocasionado por el humo y/o agua.

Cuando no se cuenta con sistemas automáticos antifuego y se vea o perciba señales de fuego, entonces se debe actuar con rapidez para poder sofocar el incendio. Para cada tipo de situación hay un agente antifuego ideal, así tenemos:

TIPO	GAS CARBONICO (CO_2)	ESPUMA	AGUA
PAPEL, MADERA	Apaga solamente la Superficie.	Sofoca	Ideal: Enfría y empapa, apaga totalmente.
EQUIPAMIENTO ELECTRICO	Ideal: No deja residuos, no daña el equipamiento y no es conductor de electricidad.	Conduce electricidad y además daña el equipo.	Conductora de Electricidad.
LIQUIDOS INFLAMABLES	No deja residuos y es inofensivo.	Ideal: Produce una sábana de espuma que sofoca y enfría.	

7.3.2. MEJORAMIENTO DE INFRAESTRUCTURA

7.3.2.1. INSTALACIONES ELÉCTRICAS

Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible. En nuestro medio se han podido identificar siete problemas de energía más frecuente: Fallas de energía, Transistores y pulsos, Bajo voltaje, Ruido electromagnético, Distorsión, Alto voltaje, Variación de frecuencia.

Existen dispositivos que protegen de estas consecuencias negativas, los cuales tienen nombres como: Supresores de picos, Estabilizadores, Sistemas de alimentación ininterrumpida (SAI o UPS: UNINTERRRUPTIBLE POWER SYSTEM).

Como Prever las Fallas que Generan Altas Temperaturas:

✓ Tomas de Tierra. En la actualidad la empresa SEDA AYACUCHO S.A., cuenta con dos sistemas de pozo a tierra para el sistema de negocio. Se ha considerado un mantenimiento preventivo de una vez al año para los dos sistemas, con el fin de comprobar la resistencia y las conexiones. Es recomendable que esta labor se efectúe en los meses de verano o en tiempo de sequía, con el fin de evaluarlas en el momento más crítico del año por falta de humedad.

✓ Fusibles. Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo. A continuación, debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible. Entre las causas menos problemáticas para que se fundan los fusibles o salten los diferenciales se encuentra la sobrecarga de un circuito eléctrico. Para corregir esto se necesita reorganizar la distribución de enchufes sobre las placas, distribuyendo la carga de forma más uniforme. Entre las fallas más serias, se incluyen los cables dañados de forma que el aislante entre los conductores se ha roto. En los aparatos, los aislantes pueden decaer o fundirse, dando lugar a cortocircuitos. Al sustituir los fusibles de una computadora, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el fusible.

✓ Extensiones Eléctricas y capacidades. Deben estar fuera de las zonas de paso, siempre que sea posible. Se debe utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso. Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esta cifra el amperaje total de todos los aparatos conectados a ellas. Tanto los toma corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

7.3.2.2. CAÍDAS Y SUBIDAS DE TENSIÓN

Las caídas y subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras personales, los monitores, las impresoras y los demás periféricos. Lo que causa problemas en las computadoras personales son las grandes oscilaciones en el voltaje. Por ejemplo, una

caída por debajo de los 200V y una subida por encima de los 240V. Si la lectura del voltaje continúa fluctuando, anote la medida más alta y la más baja. Si se encuentran dentro de un margen del 5 por 100, alrededor del voltaje esperado, probablemente no causará ningún problema. Si las oscilaciones se encuentran fuera de este margen, puede ser recomendable pedir que un electricista revise el cableado e invertir en algún equipo de acondicionamiento de corriente (Estabilizadores de Voltaje).

✓ **Supresores de Subidas de Tensión**. Una protección relativamente barata ante las subidas de tensión es un supresor de subidas. Este es un dispositivo eléctrico situado entre la computadora personal y la fuente de corriente. Incluye circuitos que recorta el voltaje cuando éste comienza a subir por encima de un nivel aceptable. El supresor de subidas evita que las subidas de la corriente de alimentación peligrosas lleguen al equipo. Cualquier buen supresor de subidas de tensión debe contar con las siguientes características:

- Ruptor de circuito.- Cualquier supresor de sobretensiones debe incluir un ruptor del circuito, un conmutador rearmable que corta la alimentación si se sobrecargan los circuitos (normalmente un switch). Este es el mínimo nivel de protección para cualquier dispositivo, debiendo incluso la extensión eléctrica múltiple más sencilla, de incluir uno.

- Protección separada.- Muchos supresores de subidas de tensión ofrecen varios puntos de conexión para conectar el sistema. El diseño de la unidad debe proteger cada punto de conexión de forma separada. Con este diseño es fácil que pueda hacer frente a subidas más grandes que con otro en que simplemente se protege la línea que va al múltiple.

✓ **Picos.** Una variación en la corriente más peligrosa y difícil de medir son los picos. Estos consisten en una súbita subida de tensión a niveles muy altos. Muchos de estos picos son causados por la conexión y desconexión de grandes aparatos eléctricos. Los picos son de dos tipos distintos: Modo Normal y Modo Común. Los sucesos de modo normal se pueden medir entre los hilos activo y neutro del circuito eléctrico del edificio. Los de modo común se miden entre el neutro y la tierra. Un pico en modo normal de gran magnitud puede dañar la fuente de alimentación de la microcomputadora. Sin embargo, un pico en modo común de sólo unas pocas docenas de voltios puede dañar los circuitos lógicos o producir errores entre las computadoras.

- Protección frente a Picos.- Los criterios de adquisición de un protector ante picos son en gran parte los mismos que los de los protectores ante sobretensiones, siendo normal y deseable que una misma unidad ofrezca protección ante ambos, aunque se debe comprobar sus especificaciones para asegurarse.

7.3.2.3. GARANTIZAR EL SUMINISTRO ELÉCTRICO

Las caídas, subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras, monitores, las impresoras y los demás periféricos. Un corte de la alimentación de la unidad principal puede:

- Hacer que desaparezca la información que hay en la RAM. Los datos recién introducidos o recién editados que no se hayan grabado, se pierden.

- Se interrumpe el proceso de escritura en el disco. Se puede perder información de importancia que necesita el sistema operativo, como puede ser la localización de un archivo, dando como resultado que pierdan o desorganicen archivos.

- Puede "aterrizar" un disco fijo. La cabeza de lectura - escritura de la mayor parte de los discos fijos se separa automáticamente del disco cuando se desconecta la unidad, pero puede ocurrir en algunos sistemas que la cabeza "aterrice" sobre la superficie del disco y la dañe, dando lugar a que se pierdan datos e incluso, resulte dañado físicamente el disco.

- Interrumpir impresión. Cuando vuelva la tensión se han de continuar los procesos de impresión. En algunos casos se ha de volver a comenzar el proceso de impresión.

- Se interrumpen las comunicaciones. Cuando vuelve la corriente, los datos que se estaban transfiriendo entre las computadoras deben de ser comprobados para tener exactitud, y los archivos que se estaban transmitiendo puede que haya que volver a transmitirlos.

- El sistema queda expuesto a picos y subidas de tensión cuando vuelve la tensión. Normalmente se desconectan los equipos cuando se va la corriente, pero esto no siempre es posible.

✓ **U.P.S o S.A.I.** (SISTEMA DE ENERGÍA ININTERRUMPIBLE). El UPS suministra electricidad a una PC (estación o servidor) cuando falla el fluido eléctrico, es energía de seguridad para un sistema de computación, ya sea cuando la energía eléctrica de la línea se interrumpe o baja a un nivel de tensión inaceptable. Los sistemas UPS también proveen protección contra sobrecarga y pueden proveer asimismo regulación de tensión. Selección de un UPS.- Al seleccionar un UPS se debe tener en cuenta los siguientes factores principales:

- Requerimientos de Potencia (actuales y futuros)
- Requerimiento de frecuencia
- Tiempo de respaldo requerido
- Futuras Expansiones
- Picos por corriente de arranque
- Servicio de Mantenimiento
- Soporte Técnico (antes, durante y después de la instalación)

✓ **Grupo Electrógeno**. Para obtener el rendimiento y la confiabilidad adecuada, se recomienda que se declare las especificaciones en términos de rendimiento deseado, en vez de intentar especificar un determinado tamaño, tipo o marca de equipo.

7.3.3. ANTE ACCIONES HOSTILES

7.3.3.1. EL ROBO

- Mantener el servidor y los equipos asociados en el armario del cableado hay que asegurarse de que el armario se refrigere adecuadamente.
- Asegurarse que el personal es de confianza, competente y conoce los procedimientos de seguridad.

✓ **Cómo prevenir los robos con computadora.**

- Creación de un equipo con misión especial que establezca y compruebe técnicas de seguridad para la computadora. Este equipo deberá incluir representantes de los departamentos de procesamiento de datos, seguridad, auditoría y usuario.

- Ejecución de un análisis de riesgos en los sistemas que abarquen pérdidas potenciales por accidentes, así como por delitos intencionados.

- Compilación de una lista con las aplicaciones de la computadora identificando posibles oportunidades para delinquir y estableciendo un sistema de defensas.

✓ **Evitar**

- Depender de una sola persona para las funciones vitales.
- Repetición periódica de comprobaciones de seguridad. Emplear inspecciones ad-hoc.
- Trabajo no supervisado, especialmente durante el turno de noche, malas técnicas de contratación, evaluación y de despido de personal.

7.3.3.2. EL FRAUDE

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, los computadores han sido utilizados en dicho propósito. Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones. Las tres principales áreas donde se produce el fraude son:

1) Manipulación de información de entrada, fácil de realizar y muy difícil de detectar, al ser los métodos de validación de entrada simples y, en general, conocidos por un gran número de personas de la empresa.

2) Alteración o creación de archivos de información. Se alteran los datos directamente del fichero o se modifica algún programa para que realice la operación deseada.

3) Transmisión ilegal. Interceptar o transferir información de teleproceso.

4.3.2. EL SABOTAJE

El peligro más temido por los centros de Procesamiento de Datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia Empresa.

La protección contra el sabotaje requiere:

- Una selección rigurosa del personal.
- Buena administración y controles de los recursos humanos.
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

Se menciona a continuación algunas medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles:

- Tener información de contacto con el departamento de policía local.
- Mantener adecuados archivos de reserva (backups).
- No confiarse en una pequeña fuerza de Vigilancia.
- Planear para probar los respaldos (backups) de los servicios de procesamiento de datos.
- Identificar y establecer operaciones criticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Montar procedimientos para remitir registros de almacenamiento de archivos y recuperarlos.
- Usar rastros de auditorías o registros cronológicos (logs) de transacción como medida de seguridad.

7.4. MEDIDAS DE PRECAUCIÓN Y RECOMENDACIONES

7.4.1. EN RELACIÓN AL CENTRO DE CÓMPUTO

- Es recomendable que el Centro de Cómputo no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.

- Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad del Centro de Cómputo.
- Otra precaución que se debe tener en la construcción del Centro de Cómputo, es que no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.
- El acceso al Centro de Cómputo debe estar restringido al personal autorizado. El personal de la Empresa deberá tener su carné de identificación siempre en un lugar visible. Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.
- Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médico y tener muy en cuenta sus antecedentes de trabajo, ya que un Centro de Cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.
- El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.
- Deben establecerse controles para una efectiva disuasión y detección, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contienen.
- Se recomienda establecer políticas para la creación de los password y establecer periodicidad de cambios de los mismos.
- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
- Establecer políticas de control de entrada y salida del personal, así como de los paquetes u objetos que portan.
- La seguridad de los terminales de un sistema en red podrá ser controlados anulando las Puerto USB y grabador de CD/DVD, cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.
- Los controles de acceso, el acceso en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de Cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.

- Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Dirección.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.
- El modelo de seguridad a implementar, estará basado en el entorno y en la política y estrategias de la instalación.

7.4.1.1. RESPECTO A LA ADMINISTRACIÓN DE LA CINTOTECA

- Debe ser administrada bajo la lógica de un almacén. Esto implica ingreso y salida de medios magnéticos (sean cintas, USBs, cartuchos, Discos removibles, CD's, etc.), obviamente teniendo más cuidado con las salidas.

- La cintoteca, que es el almacén de los medios magnéticos (sean cintas, USBs, cartuchos, Discos removibles, CD's, etc.) y de la información que contienen, se debe controlar para que siempre haya determinado grado de temperatura y de la humedad.

- Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.

- El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

7.4.1.2. RESPECTO A LA ADMINISTRACIÓN DE IMPRESORAS

- Todo listado que especialmente contenga información confidencial, debe ser destruido, así como el papel carbón de los formatos de impresión especiales.
- Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.
- Establecer controles respecto a los procesos remotos de impresión.

7.4.1.3. NIVELES DE CONTROL

Existen dos tipos de activos en un Centro de Cómputo. Los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de robo o daño del equipo, revelación o destrucción no autorizada de la información clasificada, o interrupción del soporte a los procesos del negocio, etc.

El valor de los activos a proteger, está determinado por el nivel de clasificación de la información y por el impacto en el negocio, causado por pérdida o destrucción del Equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será

necesario el control. Cualquier control debe basarse únicamente en el valor del equipo y servicios que ellos prestan.

En cambio, tratándose de nivel clasificado, deben observarse además todas las medidas de seguridad de la información que estos equipos contengan.

7.4.2. MEDIOS DE ALMACENAMIENTO

7.4.2.1. RECOMENDACIONES PARA EL MANTENIMIENTO DE CD/DVD

El CD/DVD es un dispositivo más común de almacenamiento óptico, con la finalidad de garantizar una adecuada conservación de la información almacenada.

- El ambiente debe contar con aire acondicionado.
- Los CD/DVD's deben guardarse en estantes o armarios adecuados.
- Se les debe dar un mantenimiento preventivo en forma periódica a fin de quitar impurezas que se hayan registrado sobre ellas.

7.4.2.2. RECOMENDACIONES PARA EL MANTENIMIENTO DE CINTAS MAGNÉTICAS Y CARTUCHOS

Las cintas magnéticas y cartuchos deben guardarse bajo ciertas condiciones, con la finalidad de garantizar una adecuada conservación de la información almacenada.

➢ **Cintas Magnéticas.**

- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:

Temperatura : 4ºC a 32ºC
Humedad Relativa : 20 % a 80 %

- El ambiente debe contar con aire acondicionado.
- Las cintas deben colocarse en estantes o armarios adecuados.
- Deberá mantenerse alejados de los campos magnéticos.
- Se les debe dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas que se hayan registrado sobre ellas.

➢ **Cartuchos**

- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:

Temperatura : 16ºC a más
Humedad Relativa : 20 % a 80 %

- La temperatura interna del Drive puede oscilar entre: 5ºC a 45ºC.
- Deben ser guardados dentro de su caja de plástico.
- Deben mantenerse alejados de campos magnéticos.

7.4.2.3. RECOMENDACIONES PARA EL MANTENIMIENTO DE DISCOS MAGNÉTICOS

Las recomendaciones para el buen mantenimiento de los discos magnéticos son:

- En general los discos magnéticos son medios de almacenamiento "delicados", pues si sufren un pequeño golpe puede ocasionar que la información se dañe o producir un CRASH al sistema.
- El cabezal de lectura-escritura debe estar lubricado para evitar daños al entrar en contacto con la superficie del disco.
- Se debe evitar que el equipo sea colocado en una zona donde se acumule calor, ya que el calor interfiere en los discos cuando algunas piezas se dilatan más que otras, o se secan los lubricantes. Con ello se modifican la alineación entre el disco y los cabezales de lectura-escritura, pudiéndose destruir la información.
- Las ranuras de los ventiladores de refrigeración deben estar libres.
- Se debe evitar, en lo posible, la introducción de partículas de polvo que pueden originar serios problemas.

7.4.2.4. RECOMENDACIONES PARA EL MANTENIMIENTO DE LOS DISCOS DUROS

Las recomendaciones para HDD:

- Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.
- El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.
- Se debe evitar que la microcomputadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras. No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.
- Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un microcomputador.

Las recomendaciones para SDD:

- Evitar golpes y vibraciones, aunque los SDD son más resistentes a lso golpes que los SDD, aún es importante tratarlos con cuidado para evitar daños.
- Temperatura controlada, los SDD son más resistentes a los HDD, aun así es recomendable mantenerlos en un rango de temperatura moderada, evitando la exposición a temperaturas extremas de calor o frio extremos.
- Mantener los SDD en un entorno con niveles de humedad moderada.
- Fuente de alimentación estable para prevenir variaciones en la alimentación eléctrica.
- Actualizaciones de firmware, realizar las actualizaciones de firmware disponibles mejorará el rendimiento y compatibilidad.
- Uso eficiente del espacio, evitando llenar el SSD hasta su máxima capacidad permitirá una operación más eficiente y el rendimiento no se vea afectado.
- Evitar escrituras excesivas, los SDD tienen un número limitado de ciclos de escritura, evitar escribir en exceso para prologar su vida útil, especialmente tareas que implican grandes cantidades de escrituras, como la edición frecuente de archivos grandes.

7.4.2.5. RECOMENDACIONES PARA EL MANTENIMIENTO DE USBS

Las recomendaciones que a continuación se sugieren se aplican en general para los diferentes tipos de USBs: de v3 o v2 de alta y baja densidad.

- Debe mantenerse a una temperatura normal, en un rango comprendido entre los 10ºC y 52ºC, con la finalidad de evitar que se deteriore el material del cual está hecho.
- Para coger el USB debe hacerse por la parte plástica y nunca por la parte física interna, debido a que, por su tecnología, el proceso de almacenamiento es magnético y el cuerpo humano ejerce cierta fuerza magnética y puede desmagnetizarse.
- De manera similar, no debe acercarse a los USBs ningún cuerpo con propiedades magnéticas (como los imanes), ya que podrían provocar la pérdida irrecuperable de los datos ya almacenados.
- Cuando se esté grabando o borrando información no se debe presionar el botón (USB de v3 o v2), porque puede ocurrir que no sólo se dañe la información

restante, sino también el formato lógico, tomándolos como bloques de sectores dañados.

- Los USBs deben mantenerse en sus respectivas fundas y en su manipuleo se debe evitar: Doblar los USBs, Colocar un peso sobre ellos, debiendo mantenerse en zonas libres, Tratarlos como una placa simple de plástico, es decir, no se debe usar clips o grapas para unirlos con otros materiales (hojas u otros USBs).

7.4.2.6. RESPECTO A LOS MONITORES

- La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección.
- Generalmente éstos vienen en forma de una pantalla con un terminado áspero o algún tipo de capa contra brillo con una base de sílice, sobre la superficie de la pantalla del monitor.
- Se recomienda sentarse por lo menos a 60 cm. (2 pies) de la pantalla. No sólo esto reducirá su exposición a las emisiones (que se disipan a una razón proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual.
- También manténgase por lo menos a 1 m. o 1.20 m. (3 o 4 pies) del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.
- Finalmente apague su monitor cuando no lo esté usando.

7.4.2.7. RECOMENDACIONES PARA EL CUIDADO DEL EQUIPO DE CÓMPUTO

- **Teclado:** Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.
- **Cpu:** Mantener la parte posterior del cpu liberado en por lo menos 10cm. Para asegurar así una ventilación mínima adecuada.
- **Mouse:** Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste.
- **Protectores de pantalla:** Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.
- **Impresora:** El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel. Caso de impresora de rodillo, no usar rodillo cuando esté prendido. Caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.

7.5. SEGURIDAD EN REDES

7.5.1. CONTROL DE ACCESO A LA RED

- Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Restringir la posibilidad de conectar estaciones mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Identificación para la red con clave de acceso.
- Protección con clave de todas las áreas sensitivas de datos y restricción de acceso a los programas, según su uso.
- Registro de toda la actividad de la estación de trabajo.
- Protección con clave de acceso o bloqueo de todas las operaciones de copia a USB en las estaciones de trabajo.
- Monitorización de todas las operaciones de copia en USB y CD/DVD en las estaciones de trabajo.

7.5.2. PROTECCIÓN DEL SERVIDOR

- La parte más importante de la red es el servidor. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlo de todas las eventualidades.
- La dependencia en que esté el servidor no debe ser accesible para nadie, excepto para el administrador de la red. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él. Las impresoras y otros periféricos deben mantenerse alejados de ojos fisgones.
- Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local) o en su defecto almacenadas en alguna cuenta pagada de la nube.

7.5.3. PROTEGIENDO LA RED

Estaciones de trabajo sin Puerto USB activado y sin grabador de CD/DVD. Una posible solución para poder impedir la copia de programas y datos fuera de la red en USBs y CD/DVD, y que a través de los USBs ingresen virus y otros programas dañinos a la red, es dotar a los usuarios vulnerables con estaciones de trabajo sin puerto USB y sin grabador de CD/DVD.

7.5.4. TECNOLOGÍA RAID

- **RAID (Arreglo Redundante de Discos Asequibles)** reemplaza los sistemas de almacenamiento, grandes y costosos, con múltiples unidades de disco duro, pequeñas e idénticas. Potencialmente la tecnología RAID puede reducir el costo del almacenamiento, aumentar la velocidad y mejorar la confiabilidad del sistema.
- El **Arreglo RAID** sólo responde como un disco duro grande, en lugar de varios discos identificados por letras (en el caso de múltiples discos duros conectados a una computadora estándar). Más importante aún, el contenido de un archivo no está concentrado en un solo disco duro, sino que está esparcido a lo largo del arreglo, aumentando la seguridad de la información. La redundancia en el diseño de RAID significa que una parte de los datos almacenados se duplica para ayudar a detectar errores y corregirlos. Este método de almacenamiento pone fin a los errores de lectura y escritura y ofrece una verdadera tolerancia a fallas. Además, los sistemas RAID pueden ofrecer a los usuarios de las redes, acceso a todos los datos, aunque un disco duro en el arreglo, falle catastróficamente. Esta tecnología va más allá de los asuntos de confiabilidad para mejorar el rendimiento. Los múltiples discos en el arreglo pueden leer y escribir los datos en paralelo, dividiendo la información entre los discos a nivel de bit, byte o bloque, usando un proceso llamado la división de datos (data striping), y potencialmente pueden multiplicar la transferencia de información máxima por el número de discos en el arreglo.
- **NIVELES DE RAID. RAID 5:** "Acceso independiente con paridad distribuida". Este array ofrece tolerancia al fallo, pero, además, optimiza la capacidad del sistema permitiendo una utilización de hasta el 80% de la capacidad del conjunto de discos. Esto lo consigue mediante el cálculo de información de paridad y su almacenamiento alternativo por bloques en todos los discos del conjunto. La información del usuario se graba por bloques y de forma alternativa en todos ellos. De esta manera, si cualquiera de las unidades de disco falla, se puede recuperar la información en tiempo real, sobre

la marcha, mediante una simple operación de lógica de O exclusivo, sin que el servidor deje de funcionar. RAID 5 es el nivel de RAID más eficaz y el de uso preferente para las aplicaciones de servidor básicas para la empresa. Comparado con otros niveles RAID con tolerancia a fallos, RAID 5 ofrece la mejor relación rendimiento-coste en un entorno con varias unidades. Gracias a la combinación del fraccionamiento de datos y la paridad como método para recuperar los datos en caso de fallo, constituye una solución ideal para los entornos de servidores en los que gran parte del E/S es aleatoria, la protección y disponibilidad de los datos es fundamental y el coste es un factor importante. Este nivel de array es especialmente indicado para trabajar con sistemas operativos multiusuarios.

Se necesita un mínimo de tres unidades para implementar una solución RAID 5.

- LOS NIVELES 4 Y 5 de RAID pueden utilizarse si se disponen de tres o más unidades de disco en la configuración, aunque su resultado óptimo de capacidad se obtiene con siete o más unidades. RAID 5 es la solución más económica por megabyte, que ofrece la mejor relación de precio, rendimiento y disponibilidad para la mayoría de los servidores.

7.6. CASOS DE EMERGENCIAS PARA EQUIPOS DE CÓMPUTO

7.6.1. DE LAS EMERGENCIA FÍSICAS

CASO A: ERROR FÍSICO DE DISCO DE UN SERVIDOR (SIN RAID)

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

- Ubicar el disco malogrado.
- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de Departamento.
- Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
- Bajar el sistema y apagar el equipo.
- Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
- Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
- Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
- Habilitar las entradas al sistema para los usuarios.

CASO B: ERROR DE MEMORIA RAM

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.
- Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto, si hubiese un error de paridad, el servidor se autocorregirá.
- Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la empresa, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a Jefes de Departamento.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar las memorias malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Deshabilitar a los grupos de usuarios el acceso al servidor, ello evitará que al encender el sistema los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente, luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: ERROR DE TARJETA(S) CONTROLADORA(S) DE DISCO

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a Jefes de Departamento.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar la posición de la tarjeta controladora.

4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

CASO D: CASO DE INCENDIO TOTAL

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos en los dispositivos de almacenamiento.

- Ante todo, se recomienda conservar la serenidad. Es obvio que, en una situación de este tipo, impera el desorden, sin embargo, es muy recomendable tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).
- Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas
- Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

CASO E: CASO DE INUNDACIÓN

- Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.
- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.
- Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.

- Proveer cubiertas protectoras para cuando el equipo esté apagado.

CASO F: CASO DE FALLAS DE FLUIDO ELÉCTRICO

Se puede presentar lo siguiente:

- Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.
- Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.
- Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS).

7.6.2. DE LAS EMERGENCIAS LÓGICAS DE DATOS

CASO A: ERROR LÓGICO DE DATOS

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.
- Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de red.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.

PASO 4: Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de

datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.
Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

CASO B: CASO DE VIRUS

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

- Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación.
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Estos archivos (exe, com, ovl, nlm, dll, etc.) serán reemplazados del CD original de instalación o del backup
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

Se revisará las computadoras que no estén en red con antivirus libre de virus.
De suceder que una computadora se haya infectado con uno o varios virus ya sea en la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

- Utilizar un USB que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado. Reiniciar el computador con dicho USB.
- Retirar el USB con el que arrancó el computador e insertar el USB antivirus, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables.

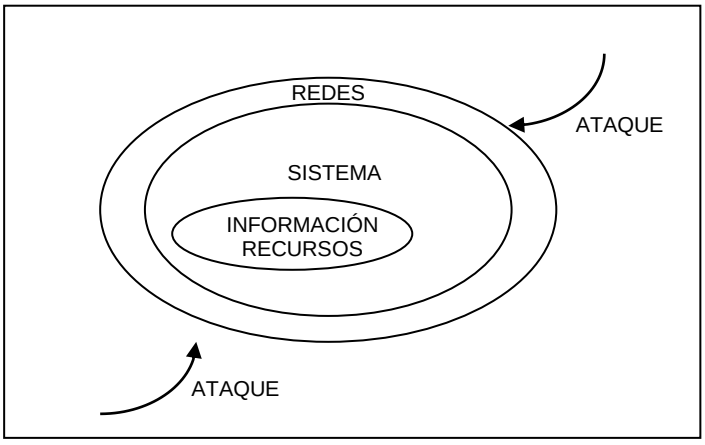
De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del escaneado. Finalizado el escaneado, reconstruir el Master Boot del disco duro.

7.7. CRITERIOS SOBRE SISTEMAS DE INFORMACION EN INTERNET

La seguridad es uno de los aspectos más conflictivos del uso de las tecnologías de la información. Es suficiente comprobar cómo la falta de una política de seguridad global está frenando el desarrollo de Internet en áreas tan interesantes y prometedoras, como el comercio electrónico o la interacción con las administraciones públicas.

Los recientes avances en las telecomunicaciones y en la computación en red han proporcionado la aparición de canales rápidos para la propagación de datos a través de sistemas digitales. Las redes abiertas están siendo utilizadas cada vez más como una plataforma para la comunicación en nuestra sociedad, pues permiten rápidos y eficientes intercambios de información con un bajo coste económico asociado y con una fácil accesibilidad.

El desarrollo actual y las perspectivas de futuro de las "superautopistas de datos" y de una infraestructura global de información, es decir, de Internet y de la World Wide Web (WWW), crean toda una variedad de nuevas posibilidades. Sin embargo, la realización efectiva de tales posibilidades está influidas por las inseguridades típicas de las redes abiertas: los mensajes pueden ser interceptados y manipulados, la validez de los documentos se puede negar, o los datos personales pueden ser recolectados de forma ilícita. Como resultado, el atractivo y ventajas ofrecidas por la comunicación electrónica, tanto en el desarrollo de oportunidades comerciales entre organizaciones privadas como en las interrelaciones entre las organizaciones públicas y los ciudadanos, no pueden ser explotadas en su totalidad.



Es por esto tener en cuenta dentro de nuestro plan de contingencia la operatividad de un firewall (cortafuego) para impedir el acceso a usuarios del exterior que no tengan autorización, ya que esto podría ser perjudicial para el servicio de nuestros servidores de red.

7.8. CASOS DE MIGRACIÓN DE SERVIDORES

Cualquier proyecto de migración debe constituirse, en términos generales, de:

1. Una fase de colecta de datos y definiciones de proyecto, incluyendo:
   - Una descripción de las condiciones iniciales relevantes que consisten, por ejemplo: arquitectura de sistemas, aplicativos y los datos a ellos asociados, protocolos y padrones usados, hardware, ambiente físico, como ancho de banda de la red, localización, requisitos sociales tales como idioma(s) y conjunto de habilidades de personal.
   - Una serie de condiciones objetivo detalladas de la misma forma; una descripción de como pasar de las condiciones existentes para las planeadas;
2. Una justificativa para la migración, incluyendo los beneficios y el costo a ella asociado.
3. Una o más fases pilotos, proyectadas para testar el plan y las justificativas. Los datos de esos pilotos pueden ser realimentados en el modelo de costo usado en el plan.
4. Acompañamiento del plan.
5. Acompañar la experiencia actual junto al plan hecho.

Siempre que instalemos un servidor tenemos que estar conscientes que tarde o temprano tendemos que reemplazarlo, ya sea por daño o por obsolescencia, por esta razón tenemos que estar preparados para estos casos, en este caso señalamos algunas medidas que se toman para restaurar servidores o bien estar listos para reemplazarlos.

Se cuenta con un Servidor de bases de datos sobre la Plataforma Oracle Linux 6U4, estos son muy importantes ya que están en constante cambio y es el más importante de la empresa ya constituye información del sistema de negocio, tanto Comercial y Administrativo. Por lo que se debe tener un respaldo semanal del directorio activo, así como las backups diarios de todo el sistema de negocio, de igual forma estos se hacen en las utilidades de respaldo del propio servidor, también tenemos las estructuras de los discos duros las cuales son indispensables para reparar un daño en el sistema.

Este mismo servidor es usado como servidor de aplicación, es necesario que se posean respaldos de los programas cargados y respaldos de los programas ya configurados y

en operación, de esta forma garantizamos que en caso de un daño podemos restaurar la operación en un tiempo más óptimo.

Los servidores de correo, Web, FTP y Firrewall, están sobre la plataforma Oracle Linux/GNU 6U4 que además de estar en constante cambio son bastante más delicados, la información de éstos está fluyendo y cambiando con bastante frecuencia. En el caso de estos equipos es bueno contar con un espejo de los datos, y además con discos en arreglos RAID seguros, de esta forma podemos tener cierta seguridad de restaurar estos equipos tan delicados, los respaldos a tener de estos equipos son:

- Las estructuras de los discos duros,
- Las estructuras del sistema,
- Respaldos del servidor en operación,
- Respaldo de la tabla de arranque de los discos,
- Respaldo de las cuentas de correo y de las estructuras de los directorios.

Pasos Para La Instalación de los Servidor:

1. Previamente se ejecuta los procedimientos de respaldo y backups de todo el sistema de negocio verificando la integridad de la información.
2. Con el utilitario del servidor se efectúa el Borrado del RAID.
3. Para el caso del Servidor IBM series M 3500 se selecciona Start and Installation.
4. Seleccionar el Sistema Operativo soportado y por el servidor y de acuerdo a las necesidades del sistema de negocio.
5. Configurar la Hora y Fecha del Sistema (24 hrs).
6. Configurar el RAID5.
7. En la configuración del RAID5, Seleccionar los discos a ser convertir a RAID5.
8. Asignar el Nombre por defecto el nombre del RAID5.
9. Aplicar la configuración efectuada.
10. Instalar el Sistema Operativo.
    - Para el Caso del Servidor de Aplicaciones y Bases de Datos, Seleccionar el S.O. MS Windows Server 2008 R2.
    - Para el Caso de los Servicios WEB, Seleccionar el S.O. Linux/GNU.