I.- INDICE.

II.- PRESENTACIÓN.

El Plan de Contingencia Informático (PCI) implica un análisis de los posibles riesgos a cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información. Corresponde aplicar al Área de Informática, las medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

El alcance de este plan guarda relación con la Infraestructura Informática. La Infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan información.

El PCI está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

Al existir siempre la posibilidad de desastre, pese a todas nuestras medidas de seguridad, es necesario que el PCI incluya un Plan de Recuperación de Desastres(PRD), con el único objetivo de restaurar el Servicio o Servicios Informáticos en forma rápida, eficiente y con el menor costo y pérdidas posibles.

El PRD provee de mecanismos de recuperación para los registros vitales, sistemas alternativos de telecomunicaciones, evacuación de personal, fuente alternativa de provisión de servicios, etc., además, debe ser comprobado periódicamente para detectar y eliminar problemas. La manera más efectiva de comprobar si un PRD funciona correctamente, es programar simulaciones de desastres. Los resultados obtenidos deben ser cuidadosamente revisados, y son claves para identificar defectos en el PCI.

III.- CAPITULOS.

CAPÍTULO 1: ANÁLISIS DE LA SITUACIÓN ACTUAL INFORMÁTICA EN EPYSA.

1.1. Introducción.

Cualquier Sistema de Redes de computadoras (ordenadores, periféricos y accesorios), están expuestos a riesgo y puede ser fuente de problemas. El Hardware y el Software están expuestos a diversos factores de riesgo humano y físicos.

Frente a cualquier evento, la celeridad en la determinación de la gravedad del problema depende de la capacidad y la estrategia a seguir para señalar con precisión, por ejemplo: ¿Qué componente ha fallado?, ¿Cuál es el dato o archivo con información que se ha perdido, en qué día y hora se produjo el incidente, y, cuán rápido se descubrió? Estos problemas menores y mayores, sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información.

Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el Disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informáticos, etc.) que producen daño físico irreparable. Frente al mayor de los desastres sólo queda el tiempo de recuperación, lo que significa adicionalmente la fuerte inversión en recursos humanos y técnicos para reconstruir su Sistema de Red y su Sistema de Información.

1.2. Objetivos e Importancia del PCI.

Objetivos:

- ✓ Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- ✓ Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

Importancia:

- ✓ Garantiza la seguridad física, la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos.
- ✓ Permite realizar un conjunto de acciones con el fin de evitar el fallo, o en su caso, disminuir las consecuencias que de él se puedan derivar.
- ✓ Permite realizar un Análisis de Riesgos, Respaldo de los datos y su posterior Recuperación de los datos. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa. La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser grande que resultaría fatal para la institución.
- ✓ Permite definir contratos de seguros, que vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades.

1.3. Red Corporativa Institucional.

La Red Corporativa Institucional cuenta en la actualidad con Sistemas de Comunicación, Sistemas de Gestión Financiera y Administrativa, Sistemas de Información, Conectividad, Sistema de Servicios brindados por la institución hacia los Usuarios Externos, Usuarios Internos y diversas instituciones. Fig. 01.

Descripción	Año de Implementación	Operando/ Inoperativo o en Stand by.	Fecha de Culminación probable
SOFTWARE			
1.- Depósito Legal	2009 - 2010	Operando y buen estado	
2.- Proyecto Editorial	2009 - 2010	Operando y buen estado	Junio 2011.
3.- Página web institucional.	2006 Joomla Versión 1.4	Joomla. Operando y buen estado. Versión 1.5.	Soporte constante.
4.- Zimbra Collaboration Suite	2008 – 2009	Operando y buen estado.	No posee soporte.
5.- ISBN	2008	Stand by.	2012.
6.- Adquisiciones y Contrataciones.	2008	Stand by.	Ya está culminado.

7.- Sabini OPAC	2008	Operando	Soporte constante.
8.- SIAF	2006	Operando	Soporte constante.
9.- SIGA	2010	Operando	Soporte constante.
10.- SISTRA	2000	Operando	Soporte constante.
11.- INSCRIPCIONES	2009	Operando	Soporte constante.
12.- Firewall Sonicwall	2007	Operando.	No posee soporte por parte de la empresa.
13.- PREZENSA	2009	Operando.	No existe contrato de mantenimiento.
14.- SISPER	2009	Operando.	Soporte constante.
15.- Seguridad Cámaras.	2008	Operando.	Soporte.
16.- PC SISTEL	2010	Operando.	Soporte constante.
17.- SABINI	1988	Inoperativo.	
18.- AbsysNet v 1.6	2009	Stand by.	Caso por resolver
19.- SPIJ	2010 – 2011	Operando	Soporte constante.
20.- Call Manager	2010	Operando.	Soporte constante.
BASE DE DATOS.			
1.- Portal de Transparencia	2008	Operando.	B.D. Externa.
2.- Portal POI	2006	Operando.	B.D. Externa.
3.- FTP MEF	2010	Operando.	B.D. Externa.
4.- SIGA	2010	Operando.	Backup semanal.
5.- SIAF	2006	Operando.	Backup semanal.
6.- INSCRIPCIONES	2009	Operando.	Backup semanal.
7.- PREZENSA	2009	Operando.	Backup quincenal.
8.- ISBN	2008	Stand by.	Backup hasta 2010.
9.- REDELEG	2009	Operando.	Backup semanal.
10.- PROYECTO EDITORIAL	2009	Operando.	Backup semanal.
11.- SISTRA	2000	Operando.	Backup mensual.
12.- AbsysNet v 1.6	2009	Stand by.	Backup hasta 2010.
13.- SPIJ	2010-2011	Operando.	Backup semanal.
14.- Call Manager	2010	Operando.	Backup semanal.

Fig. 02. HARDWARE.

ITEM	DESCRIPCIÓN	CARACTERISTICAS	MARCA	MODELO/TIPO
1	Servidor	20 Gb HD	DiscServerVT	
2	Servidor	P I	Compaq	Proliant 2500
3	Servidor	P III, 1 Gb Ram, 8 Gb y 32 Gb HD	Dell	Power Edge 4400 SML
4	Servidor	Intel Xeon 2, 4 Ghz 1 Gb 73 Gb Licencia Windows 2000 Server + 5 clientes	IBM	Xseries 235, 8671 4AX
5	Servidor	Intel Xeon 2,66 Ghz, 512 Mb, 36 Gb		Xseries 225, 8647 42X
6	Servidor	Dual Core AMD Opteron 2,60 Ghz, 2 Gb Ram 73 Gb. Licencia Windows Server 2003 R2.		System X3655, 7985 5AU
7	Servidor	Dual Core AMD 64 Opteron, 2 Gb Ram, 72 Gb Licencia Windows Server 2003 OEM	HP	Proliant DL 385G2
8	Servidor	Dual Core AMD 64 Opteron, 2 Gb Ram, 72 Gb Licencia Windows Server 2003 OEM		Proliant DL 385G2
9	Servidor (06)	Intel Xeon Quad Core E5320 146 Gb Máquina virtual	IBM	Blade Center Chassis 8677-3RU
	BLADE 01	MV:1,83 Ghz, 3 Gb Ram, 20 Gb HD		
	BLADE 02	MV:1,83 Ghz, 3 Gb Ram, 60 Gb HD		
	BLADE 03	MV:1,83 Ghz, 2 Gb Ram, 40 Gb HD		
		MV:1,83 Ghz, 4 Gb Ram, 80 Gb HD		
	BLADE 04	Intel Xeon Quad Core E5320 1,86 Ghz, 4 Gb Ram, 146 Gb HD		
	BLADE 05	MV:1,83 Ghz, 2 Gb Ram, 40 Gb HD		
		MV:1,83 Ghz, 2 Gb Ram, 68 Gb HD		
	BLADE 06	Intel Xeon Quad Core E5320 1,86 Ghz, 4 Gb Ram, 146 Gb HD		
10	Servidor	Intel Xeon 2,66 Ghz, 2 Gb Ram, 140 Gb HD		System X3650, 7979-B4U
11	Servidor	Intel Xeon 2,66 Ghz 2 Gb Ram, 140 Gb HD		System X3650, 7979-B4U

12	Servidor	Intel Xeon 2,66 Ghz 2 Gb Ram, 140 Gb HD		System X3650, 797 – B4U
13	Servidor	Intel Xeon 2,66 Ghz 2 Gb Ram, 100 Gb HD		System X3550, 7978-B4U
14	Servidor	Intel 1,86 Ghz 2 Gb Ram, 146 Gb HD		System X3200, 4363-4DU
15	Servidor	P IV 3.2 Ghz, 2 Gb Ram, 36,4 Gb	HP	Proliant ML 110
16	Servidor	P IV 3,2 Ghz, 2 Gb Ram, 36 Gb HD	HP	Proliant ML 110
17	PC COMPATIBLE	P IV 3 Gb, 1 Gb Ram, 40 Gb	Compatible	
18	PC COMPATIBLE	P IV 2,4 Gb, 512 Mb Ram, 80 Gb	Compatible	
19	PC COMPATIBLE	Pentium D 2,8 Gb, 512 Mb Ram, 80 Gb	Compatible	

INVENTARIO DE EQUIPOS DE CÓMPUTO

DIRECCIÓN / ÁREA	NÚMERO DE PC ASIGNADAS
Administración	38
Desarrollo Técnico	32
CSBE	41
Módulos OPAC	11
Hemeroteca Nacional	18
Auditoría Interna	8
CIDB	10
CBN	45
Secretaria General	12
Dirección Nacional	03
Dirección Técnica	03
Asesoría Legal	07
Imagen Institucional	11
Bibliotecas Públicas Periféricas	09
GBPL (CCRBP + CCRBEE + SNB)	60
TOTAL PC	**308 Operando**

INVENTARIO DE TELÉFONOS IP CISCO

MODELO	NÚMERO TELEFONOS
7912	112
7940	26
7960	2
TOTAL Teléfonos	**140 operando**

INVENTARIO DE IMPRESORAS

IMPRESORAS	TOTAL
EPYSA + GBPL + BPP	**89 operando**

1.4. Sistemas de Información.

Los Sistemas de Información incluyen la totalidad del Software de aplicación, Software de Desarrollo, conjunto de Documentos electrónicos, Bases de Datos e Información histórica, registrada en medios magnéticos e impresos en papeles, documentación y bibliografía.

CAPÍTULO 2: PLAN DE REDUCCIÓN DE RIESGOS.

El presente documento implica la realización de un análisis de todas las posibles causas a los cuales pueden estar expuestos nuestros equipos conectados a la red de la EPYSA, así como la

información contenida en cada medio de almacenamiento. Se realizará un análisis de riesgo y el Plan de Operaciones, tanto para reducir la posibilidad de ocurrencia como para reconstruir el Sistema de Información y/o Sistema de Red de computadoras, en caso de desastres.

El presente incluye la formación de equipos de trabajo durante las actividades de establecimiento del Plan de Acción, tanto para la etapa preventiva y correctiva, como la de recuperación.

El Plan de Reducción de Riesgos es equivalente a un Plan de Seguridad, en la que se considera todos los riesgos conocidos, para lo cual se hará un Análisis de riesgos.

2.1. Análisis de Riesgos.

El presente realiza un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada, y que deben ser protegidos.

Bienes susceptibles de un daño.

Se puede identificar los siguientes bienes afectos a riesgos:

a) Personal.
b) Hardware.
c) Software y utilitarios.
d) Datos e información.
e) Documentación.
f) Suministro de energía eléctrica.
g) Suministro de telecomunicaciones.

Daños

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.

b) Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

c) Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la institución son:

* Acceso no autorizado.
* Ruptura de las claves de acceso a los sistemas computacionales.
* Desastres Naturales:
  a) Movimientos telúricos.
  b) Inundaciones.
  c) Fallas en los equipos de soporte (causadas por el ambiente, la red de energía eléctrica, no acondicionamiento atmosférico necesario).
* Fallas de Personal Clave: por los siguientes inconvenientes:
  a) Enfermedad.
  b) Accidentes.
  c) Renuncias.
  d) Abandono de sus puestos de trabajo.
  e) Otros.
* Fallas de Hardware:
  a) Falla en los Servidores.
  b) Falla en el hardware de Red. (Switch, cableado de la Red, Router, Firewall)
* Incendios.

Características

El Análisis de Riesgos tiene las siguientes características:

* Es posible calcular la probabilidad de que ocurran las cosas negativas.
* Se puede evaluar económicamente el impacto de eventos negativos.
*Se puede contrastar el Costo de Protección de la Informática y medios versus el Costo de volverla a producir.

Durante el estudio Análisis de Riesgo, se define claramente:

* Lo que intentamos proteger

* El valor relativo para la organización
* Los posibles eventos negativos que atentarían lo que intentamos proteger.
* La probabilidad de ataque.

Se debe tener en cuenta la probabilidad de suceso de cada uno de los problemas posibles, de tal manera de tabular los problemas y su costo potencial mediante un Plan adecuado.
Los criterios a tener en cuenta son:

Criterios	Escala
Grado de Negatividad	Leve / Moderado / Grave / Muy severo
Posible frecuencia	Nunca / Aleatorio / Periódico / Continuo
Grado de impacto o consecuencias	Leve / Moderado / Grave / Muy severo
Grado de Certidumbre	Nunca / Aleatorio / Probable / Continuo

Clases de Riesgos
El Factor de Probabilidad por Clase de Riesgo en función a la ubicación geográfica de la institución y a su entorno institucional; por ejemplo, si la institución:
* Se ubica en zona sísmica el factor de probabilidad de desastre por terremotos será alta.
* Se ubica en una zona marginal con alto índice de delincuencia, las probabilidades de robo, asalto o vandalismo será de un sesgo considerablemente alto.
* Se ubica en zona industrial las probabilidades de "Fallas en los equipos" será alto por la magnitud de variaciones en tensiones eléctricas que se generan en la zona.
* Cambia constantemente de personal, las probabilidades de equivocaciones y sabotaje será alto.

Identificación de Amenazas (Probabilidad de que ocurra la amenaza)

Amenaza	Factor (%) San Borja	Factor (%) GBPL
Incendio	20	45
Robo de equipos y archivos	35	55
Falla en equipos	15	25
Equivocaciones de personal	60	60
Virus informáticos	50	50
Inundaciones	10	40
Accesos no autorizados	15	30
Movimientos telúricos	70	70

Para identificar las clases de amenazas, se ha tenido en cuenta el historial de ocurrencias tanto de la sede San Borja y la sede de GBPL.

INCENDIO
Grado de negatividad: Muy severo.
Frecuencia de evento: Aleatorio.
Grado de impacto: Grave.
Grado de certidumbre: Probable.

Situación actual SAN BORJA	Acción correctiva
1.- Sala de Servidores cuenta con un extintor cargado. Está dentro del área de informática del 4to piso.	Se cumple.
2.- Sala de comunicaciones cuenta con aire acondicionado, debidamente regulado. Sin embargo no cuenta con extintor. Se encuentra en el sótano de la institución.	Se cumple aire acondicionado. Falta de extintores cerca a dicha sala. Se debe habilitar dos cerca de dicha sala.
3.- Sala de concentradores (sótano, 1 piso, 2 piso, 3 piso y 4 piso) no poseen extintores ni aire acondicionado.	No se cumple. En cada piso se debe colocar aire acondicionado en dicha sala de concentradores.
4.- En las diferentes áreas donde hay equipos de cómputo, no existen extintores. Falta mayor número de extintores.	No se cumple. Debe haber un mínimo de 2 extintores por cada 20 pc en un área.
5.- No se ejecuta un programa de capacitación sobre	No se cumple.

el uso de elementos de seguridad y primeros auxilios, lo que no es eficaz para enfrentar un incendio y sus efectos.	Defensa civil y el área de infraestructura deben coordinar para tener un plan de seguridad y capacitar al personal en casos de emergencia.
Situación actual GBPL	**Acción correctiva**
1.- Cuarto de Comunicaciones no posee aire acondicionado ni extintores.	Falta la adquisición de un equipo de aire acondicionado y extintores adecuados.
2.- Áreas o Salas de investigación, se encuentran con extintores.	Se cumple.

A continuación se describe gráficamente el procedimiento para el uso de extintores en caso de incendio:

ROBO

Grado de negatividad: Grave.
Frecuencia de evento: Aleatorio.
Grado de impacto: Moderado.
Grado de certidumbre: Aleatorio.

Situación actual SAN BORJA	**Acción correctiva**
1.- Sala de Servidores cuenta con seguridad electrónica.	Se cumple.
2.- Sala de comunicaciones cuenta con seguridad electrónica. Además de cámaras con circuito cerrado.	Se cumple.
3.- Sala de concentradores (sótano, 1 piso, 2 piso, 3 piso y 4 piso) no poseen seguridad electrónica ni videocámaras.	No se cumple. Se requiere colocar puertas imantadas y cámaras de seguridad.
4.- Diferentes áreas de la institución no cuenta con cámaras.	No se cumple. Debe haber un mínimo de 2 cámaras por cada 20 pc en un área.
Situación actual GBPL	**Acción correctiva**
1.- Sala de Comunicaciones no cuenta con seguridad electrónica.	No cumple. Se debe colocar puertas imantadas y cámaras de seguridad en todo el piso.
2.- Salas de investigación no cuenta con detectores ni puertas de accesos permitidos.	No cumple. Se debe priorizar la seguridad electrónica.

FALLA EN EQUIPOS

Grado de negatividad: Grave.
Frecuencia de evento: Aleatorio.
Grado de impacto: Grave.
Grado de certidumbre: Probable.

Situación actual SAN BORJA	**Acción correctiva**
1.- Red de Servidores cuenta con una Red Eléctrica Estabilizada.	Se cumple.
2.- Falla en hardware del equipo, requiere un rápido mantenimiento o reemplazo.	Se cumple. Contar con proveedores que tengan la rapidez de

	atención a nosotros.
Situación actual GBPL	**Acción correctiva**
1.- No existe un adecuado tendido eléctrico en Sala de Comunicaciones.	No cumple. Se debe gestionar la consultoría a empresas especializadas en corregir el tendido eléctrico.
2.- Sala de concentradores puede sufre caídas y oscilaciones de energía que ocasionan apagados inoportunos de equipos.	No cumple. Se debe gestionar la corrección del tendido eléctrico.

EQUIVOCACIONES DEL PERSONAL

Grado de negatividad: Moderado.
Frecuencia de evento: Periódico.
Grado de impacto: Moderado.
Grado de certidumbre: Probable.

Situación actual SAN BORJA	**Acción correctiva**
1.- Las equivocaciones son rutinarias y de carácter involuntario.	Capacitación de manejo de equipos informáticos, antes de iniciar labores y trabajos. Instruir al nuevo empleado con los procedimientos de seguridad.
2.- Cuando el usuario es practicante y tiene conocimientos de informática, tiene impulso de navegar por los sistemas.	Se debe cortar accesos y limitar el espacio de navegación, en modo básico.
3.- La falta de institucionalizar procedimientos, produce vacíos y errores en la toma de criterios para registrar información.	Se deben estandarizar y exigir que se realicen Acta de trabajo para fortalecer los procedimientos.
4.- La oficina de personal debe comunicar el reemplazo y el nuevo ingresante a Informática, para capacitar a éste.	Se debe capacitar al nuevo empleado previa coordinación entre el área de persona e informática.
Situación actual GBPL	**Acción correctiva**
1.- Las equivocaciones son rutinarias y de carácter involuntario.	Capacitación de manejo de equipos informáticos, antes de iniciar labores y trabajos. Instruir al nuevo empleado con los procedimientos de seguridad.
2.- La falta de institucionalizar procedimientos, produce vacíos y errores en la toma de criterios para registrar información.	Se deben estandarizar y exigir que se realicen Acta de trabajo para fortalecer los procedimientos.

VIRUS INFORMÁTICO

Grado de negatividad: Muy severo.
Frecuencia de evento: Continuo.
Grado de impacto: Grave.
Grado de certidumbre: Probable.

Situación actual SAN BORJA	**Acción correctiva**
1.- Se cuenta con un Antivirus corporativo y con licencia por un año para todos los equipos informáticos.	Se cumple.
2.- Todo software debe ser manejado por el área de informática.	Se cumple en 95 %. Faltan dos servicios que deben ser administrados por el área de informática.
3.- Se cuenta con un Firewall del tipo SONICWALL 5060 Pro. Sin embargo la licencia ha expirado desde el año pasado.	La adquisición de esta licencia es imperativa y urgente.
4.- La oficina de personal debe comunicar el reemplazo y el nuevo ingresante a Informática, para capacitar a éste.	Se debe capacitar al nuevo empleado previa coordinación entre el área de persona e informática.
Situación actual GBPL	**Acción correctiva**
1.- Se cuenta con un Antivirus corporativo y con licencia por un año para todos los equipos informáticos.	Se cumple.
2.- Todo software debe ser manejado por el área de	Se cumple en 95 %. Faltan dos servicios que deben

informática.	ser administrados por el área de informática.

INUNDACIONES

Grado de negatividad: Moderado.
Frecuencia de evento: Aleatorio.
Grado de impacto: Grave.
Grado de certidumbre: Aleatorio.

Situación actual SAN BORJA	Acción correctiva
1.- La ubicación geográfica y el clima, son factores que influyen de que no existan estos problemas.	Se cumple con infraestructura adecuada en caso de inundaciones y/o lluvias torrenciales.
2.- En época del Fenómeno del Niño, se han establecido maneras de atacar el problema.	Se cumple.
3.- El ambiente de las Salas de Servidores, está alejada del suelo y de filtraciones.	Se cumple.
4.- El ambiente del Cuarto de comunicaciones, esta propenso a inundaciones por estar en el sótano de la EPYSA.	Debe haber una distribución nueva en el tema de comunicaciones.
Situación actual GBPL	**Acción correctiva**
1.- La ubicación geográfica y el clima, son factores que influyen de que no existan estos problemas.	Se cumple. Sin embargo, la infraestructura de la sede debe tener mantenimiento, sobretodo en temas de conexiones sanitarias.
2.- El ambiente del Cuarto de comunicaciones, esta propenso a inundaciones por estar a lado de los baños.	Debe ser cambiado el cuarto de comunicaciones a un área de mayor seguridad.

ACCESOS NO AUTORIZADOS

Grado de negatividad: Grave.
Frecuencia de evento: Aleatorio.
Grado de impacto: Grave.
Grado de certidumbre: Probable.

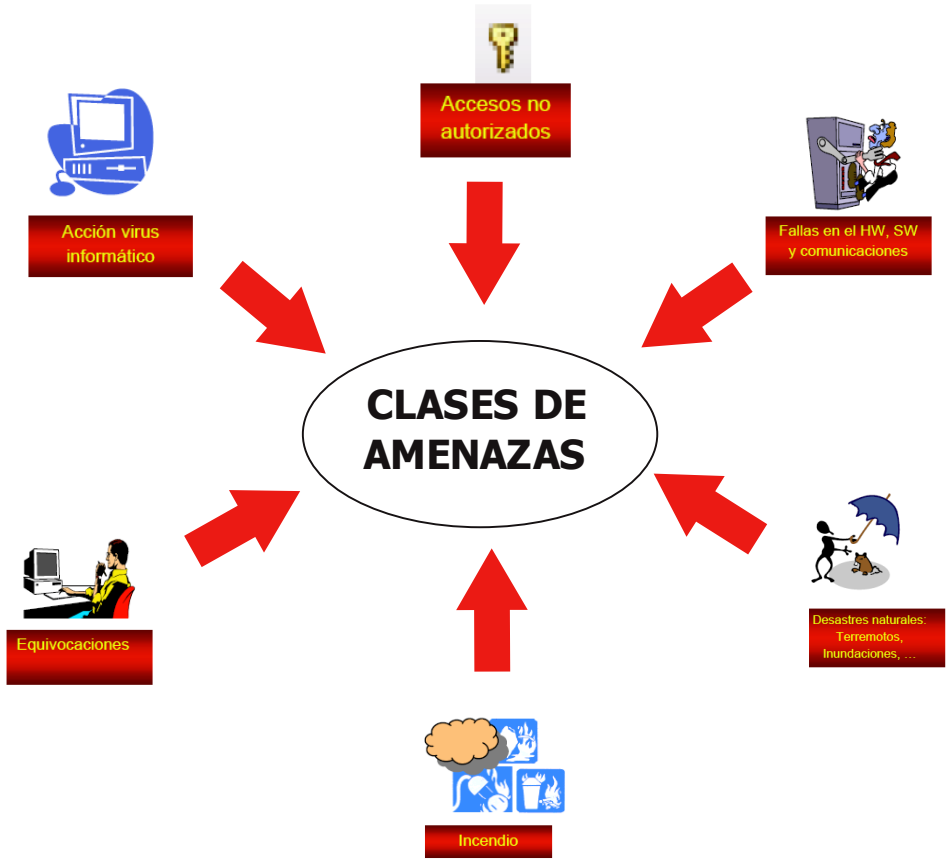
Situación actual SAN BORJA	Acción correctiva
1.- Se controla el acceso al Sistema Operativo de cada PC mediante usuario y Password.	Se cumple. Sin embargo, en algunos casos, los usuarios dan a conocer sus claves a amistades, lo que no asegura 100 % de efectividad.
2.- En caso de los Sistemas o aplicativos, se les asigna atributos y accesos autorizados, dependiendo del requerimiento.	Se cumple.
3.- Cuando el personal cesa sus funciones, el área de personal indica que se deben deshabilitar cuentas y/o accesos a los sistemas.	Se cumple.
4.- No se tiene un registro electrónico de los usuarios, dando a conocer las ocurrencias y problemas.	No existe. Se debe crear un Sistema especial de toma de datos respecto a ocurrencias y problemas de usuarios.
Situación actual GBPL	**Acción correctiva**
1.- Se controla el acceso al Sistema Operativo de cada PC mediante usuario y Password.	Se cumple. Sin embargo, en algunos casos, los usuarios dan a conocer sus claves a amistades, lo que no asegura 100 % de efectividad.
2.- Cuando el personal cesa sus funciones, el área de personal indica que se deben deshabilitar cuentas y/o accesos a los sistemas.	Se cumple.

MOVIMIENTOS TELÚRICOS

Grado de negatividad: Grave.
Frecuencia de evento: Periódico.
Grado de impacto: Grave.
Grado de certidumbre: Probable.

Situación actual SAN BORJA	Acción correctiva
1.- Zona geográfica sísmica muy alta.	Se cumple con infraestructura adecuada.
2.- Sala de Servidores ubicada en cuarto piso, hecha con concreto armado.	Se cumple. Bajas menores.
3.- Sala de comunicaciones, ubicada en sótano, hecha de concreto armado.	Se cumple. Bajas menores.
4.- Ambientes donde se encuentran las PC o equipos de todas las dependencias hechos de concreto armado.	Se cumple. Sin embargo se recomienda un espacio considerable entre PC y PC.
Situación actual GBPL	**Acción correctiva**
1.- Zona geográfica sísmica muy alta.	Infraestructura muy antigua, debe hacer mantenimiento periódicamente.
2.- Sala de comunicaciones, ubicada en 3er piso, hecha de material noble antiguo.	Se debe reforzar ciertos sectores o cambiar la ubicación de esta sala.

Resumen de las principales amenazas en las dos sedes que conforman la EPYSA y GBPL. Fig. 03.



2.2. Análisis en las fallas de la Seguridad.

Esto implica el estudio del hardware, software, la ubicación física de la estación su utilización, con el objeto de identificar los posibles resquicios en la seguridad que pudieran suponer un peligro.

Las fallas en 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 sobre este aspecto. La seguridad de la información tiene dos aspectos importantes como:

* Negar el acceso a los datos a aquellas personas que no tengan derecho a ellos.
* Garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

Por ejemplo, en el uso del Servicio Virtual Público de Red (VPN), implica una vía de acceso a la Red Central de EPYSA, la seguridad en este servicio es la validación de la clave de acceso.

2.3. Protecciones actuales.

Se realizan las siguientes acciones:

* Se hace copias de los archivos que son vitales para la institución.
* Al robo común se cierran las puertas de entrada y ventanas de todos los ambientes.
* Al vandalismo, se cierra la puerta de entrada.
* A la falla de los equipos, se realiza el mantenimiento de forma regular.

* Al daño por virus, todo el software que llega se analiza en un sistema utilizando software antivirus, sin embargo, debemos contar con el Firewall licenciado, para obtener mejores resultados en materia de seguridad perimetral.

* A las equivocaciones, los empleados tienen regular formación computacional. Cuando se requiere personal temporal se intenta conseguir a empleados debidamente preparados.
* A terremotos, no es posible proteger la instalación frente a estos fenómenos. El presente Plan de contingencias da pautas al respecto.
* Al acceso no autorizado. Varias computadoras disponen de llave de bloqueo del teclado.
* Al fuego, en la actualidad se encuentran instalados extintores, en sitios estratégicos y se brindara entrenamiento en el manejo de los extintores al personal, en forma periódica.

Para la realización de las Copias de Seguridad se tiene que tomar algunas decisiones previas como:

¿Qué soporte de copias de seguridad se va utilizar?
¿Se van a usar dispositivos especializados para copia de seguridad?
¿Con qué frecuencia se deben realizar las copias de seguridad?
¿Cuáles son los archivos a los que se le sacara copia de seguridad y donde se almacenara?

El Área de Informática establecerá Directivas y/o Reglamentos en estas materias, para que los usuarios tomen conocimiento de sus responsabilidades. Tales reglas y normativas deben incorporarse en una campaña de capacitación educativa.

La institución debe tener en cuenta los siguientes puntos para la protección de los datos de una posible contingencia:

* Hacer de la copia de seguridad una política, no una opción.
* Hacer de la copia de seguridad resulte deseable.
* Facilitar la ejecución de la copia de seguridad (equipos adecuados, disponibilidad, suministros).
* Hacer de la copia de seguridad obligatoria.

CAPÍTULO 3: PLAN DE RECUPERACIÓN DE DESASTRE Y RESPALDO DE LA INFORMACIÓN.

El costo de la Recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros.

El Costo de Recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior a 07 o un incendio de controlable, estará dado por el valor no asegurado de equipos informáticos e información más el Costo de Oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones. Típicamente las personas pueden ser: personal del Área de Informática, personal de Seguridad.

Las actividades a realizar en un Plan de Recuperación de Desastres se clasifican en tres etapas:

- ✓ Actividades previas al desastre.
- ✓ Actividades durante el desastre.
- ✓ Actividades después del desastre.

3.1. Actividades previas al desastre.

Se considera las actividades de planteamiento, preparación, entrenamiento y ejecución de actividades de resguardo de la información, que aseguraran un proceso de recuperación con el menor costo posible para la institución.

ESTABLECIMIENTOS DE PLAN DE ACCIÓN

En esta fase de planeamiento se establece los procedimientos relativos a:

a. Sistemas e Información.

La institución cuenta con los siguientes Sistemas: Fig. 01.

b. Equipos de Cómputo.

Se debe tener en cuenta el catastro de Hardware, impresoras, lectoras, scanner, ploters, modems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- ✓ Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
- ✓ Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación. Por ejemplo etiquetar de color rojo los servidores, color amarillo a los PC con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso).
- ✓ Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

Verificación de datos en la Fig. 02.

c. Obtención y almacenamiento de los Respaldos de Información (BACKUP).

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución. Las copias de seguridad son las siguientes:

- ✓ Backup del Sistema Operativo: o de todas las versiones de sistema operativo instalados en la Red.
- ✓ Backup de Software Base: (Lenguajes de Programación utilizados en el desarrollo de los aplicativos institucionales).
- ✓ Backup del software aplicativo: backup de los programas fuente y los programas ejecutables.
- ✓ Backups de los datos (Base de datos, password y todo archivo necesario para la correcta ejecución del software aplicativos de la institución).
- ✓ Backups del Hardware, se puede implementar bajo dos modalidades:

Modalidad Externa: mediante el convenio con otra institución que tenga equipos similares o mejores y que brinden la capacidad y seguridad de procesar nuestra información y ser puestos a nuestra disposición al ocurrir una continencia mientras se busca una solución definitiva al siniestro producido.

En este caso se debe definir claramente las condiciones del convenio a efectos de determinar la cantidad de equipos, periodos de tiempo, ambientes, etc., que se puede realizar con la entidad que cuente con equipo u mantenga un Plan de Seguridad de Hardware.

Modalidad Interna: si se dispone de más de un local, en ambos se debe tener señalado los equipos, que por sus capacidades técnicas son susceptibles de ser usados como equipos de emergencia.

d. Políticas (Normas y Procedimientos de Backups).

Se debe establecer procedimientos, normas y determinación de responsabilidades en la obtención de los "Backups" o Copias de Seguridad. Se debe considerar:

- ✓ Periodicidad de cada tipo de Backup: los Backups de los sistemas informáticos se realizan de manera diferente.
- ✓ Respaldo de información de movimiento entre los periodos que no se sacan backups: días no laborales, feriados, etc. en estos días es posible programar un Backup automático.
- ✓ Uso obligatorio de un formulario de control de ejecución del programa de Backups diarios, semanales y mensuales: es un control a implementar, de tal manera de llevar un registro diario de los resultados de las operaciones del Backups realizados y su respectivo almacenamiento.
- ✓ Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleando.
- ✓ Reemplazo de los backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar. No se realiza reemplazos pero se realiza copias de las mismas, considerando que no se puede determinar exactamente el periodo de vida útil del dispositivo donde se ha realizado el backup.
- ✓ Almacenamiento de los backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local). Esta norma se cumple con la información histórica, es decir se tiene distribuidos los backups de la siguiente manera: una copia reside en las instalaciones del Área de Informática, y una segunda copia reside en la Oficina que genera la información (Dirección o Áreas).
- ✓ Pruebas periódicas de los backups (Restore), verificando su funcionalidad, a través de los sistemas comparando contra resultados anteriormente confiables.

3.2. Actividades durante el desastre.

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:

a. Plan de Emergencias.

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe 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 el siniestro. Solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas.

Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que la acción del siniestro causen más daños o destrucciones. Se debe tener en toda Oficina los números de teléfono y direcciones de organismos e instituciones de ayuda. Todo el personal debe conocer lo siguiente:

- ✓ Localización de vías de Escape o Salida: Las vías de escape o salida para solicitar apoyo o enviar mensajes de alerta, a cada oficina debe señalizar las vías de escape.
- ✓ Plan de Evaluación Personal: el personal ha recibido periódicamente instrucciones para evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por Defensa Civil a nivel local. Esa actividad se realizara utilizando las vías de escape mencionadas en el punto anterior.
- ✓ Ubicación y señalización de los elementos contra el siniestro: tales como los extintores, las zonas de seguridad que se encuentran señalizadas (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde. De existir un repintado de paredes deberá contemplarse la reposición de estas señales.

- ✓ Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.

b. Formación de Equipos.

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

c. Entrenamiento.

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc.

Es importante lograr que el personal 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 Directivos y Ejecutivos, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

3.3. Actividades después del desastre.

a. Evaluación de daños.

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo.

En el caso de la EPYSA se debe atender los procesos de contabilidad, tesorería, administrativo-académicos, documentarios; que son las actividades que no podrían dejar de funcionar, por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

b. Priorizar Actividades del Plan de Acción.

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

c. Ejecución de actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar actividades previamente planificadas en el Plan de Acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar el avance de los trabajos de recuperación y, en caso de producirse un problema, reportarlo de inmediato a la Jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas:

- ✓ La primera la restauración del servicio usando los recursos de la institución o local de respaldo.
- ✓ La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

d. Evaluación de Resultados.

Una vez concluidas las labores de Recuperación de los sistemas que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia 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.

De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones: una la retroalimentación del Plan de Contingencias y Seguridad de Información, y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

e. Retroalimentación del Plan de Acción.

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

El otro elemento es evaluar cual hubiera sido el costo de no contar con el Plan de Contingencias en la institución.

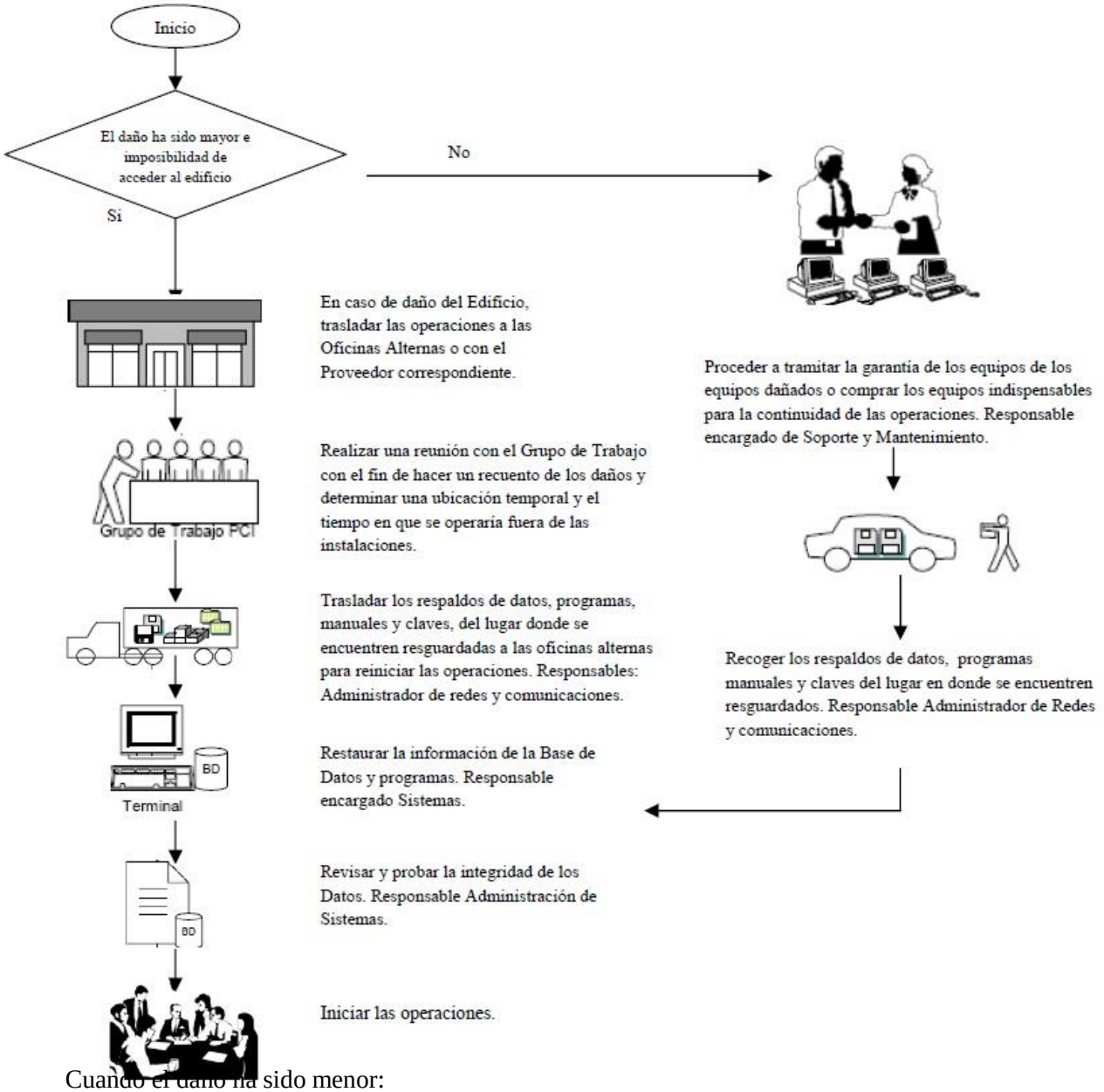
ACCIONES FRENTE A LOS TIPOS DE RIESGO.

En caso de: Incendio.

Cuando el daño del edificio ha sido mayor:

Evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado. El procedimiento de respuesta a esta emergencia se ve en la figura 04.

Fig. 04.



Cuando el daño ha sido menor:

a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento

b) Se recoge los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.

c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento

d) Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.

e) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

¿QUE HACER? Antes, Durante y Después de un INCENDIO.

ANTES:

* Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.
* No concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.
* Verificar las condiciones de extintores e hidratantes y capacitar para su manejo.
* Si se fuma, procurar no arrojar las colillas a los cestos de basura, verificar que se hayan apagado bien los cigarrillos y no dejarlos en cualquier sitio, utilizar ceniceros.
* No almacenar sustancias y productos inflamables.
* No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.
* Por ningún motivo mojar las instalaciones eléctricas, recordar que el agua es un buen conductor de la electricidad.
* Si se detecta cualquier anomalía en los equipos de seguridad (extintores, hidratantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, reportar de inmediato a Seguridad.
* Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.
* Tener a la mano los números telefónicos de emergencia.
* Portar siempre el Fotocheck de identificación.

DURANTE

* Ante todo se recomienda 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 (si el tiempo lo permite) "Salir de Red y Apagar Computador": Down en el (los) servidor(es), apagar (OFF) en la caja principal de corriente del Área de Informática o Sala de Servidores.
* Si se conoce sobre el manejo de extintores, intenta sofocar el fuego, si este es considerable no trates de extinguirlo con los propios medios, solicitar ayuda.
* Si el fuego está fuera de control, realizar evacuación del inmueble, siguiendo las indicaciones del Personal de bomberos.
* No utilizar elevadores, descender por las escaleras pegado a la pared que es donde posee mayor resistencia, recuerda: No gritar, No empujar, No correr y dirigirse a la zona de seguridad.
* Si hay humo donde nos encontramos y no podemos salir, mantenernos al ras del piso, cubriendo tu boca y nariz con un pañuelo bien mojado y respira a través de él, intenta el traslado a pisos superiores.
* Las personas que se encuentren en los últimos pisos, deberán abrir ventanas para que el humo tenga una vía de salida y se descongestionen las escaleras.
* Si es posible mojar la ropa.
* Verifica si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

DESPUES

* Retirarse inmediatamente del área incendiada y ubícate en la zona de seguridad externa que te corresponda.
* No obstruir las labores del personal especializado, dejar que los profesionales se encarguen de sofocar el incendio.
* El personal calificado realizara una verificación física del inmueble y definirá si esa en condiciones de ser utilizado normalmente.
* Colaborar con las autoridades.

En caso de: Robo.

Analizar las siguientes situaciones:

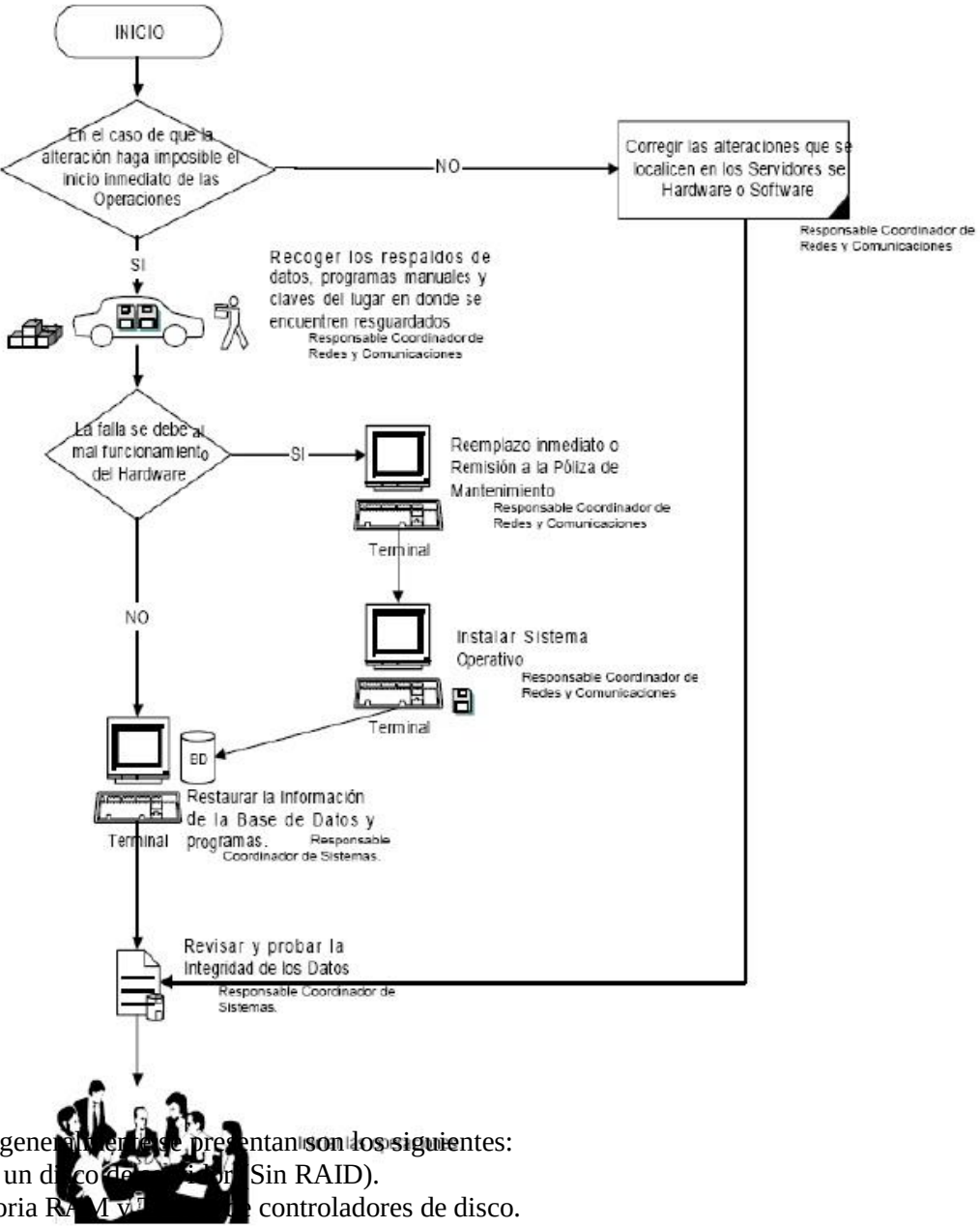
* En qué tipo de vecindario se encuentra la Institución
* Las computadoras se ven desde la calle
* Hay personal de seguridad en la Institución y están ubicados en zonas estratégicas
* Cuánto valor tienen actualmente las Bases de Datos
* Cuánta pérdida podría causar en caso de que se hicieran públicas

* Asegurarse que el personal es de confianza, competente y conoce los procedimientos de seguridad.
* Trabajo no supervisado, especialmente durante el turno de noche, malas técnicas de contratación, evaluación y de despido de personal.

En caso de: Falla de Equipos.

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos ó a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo ó de la pérdida de su configuración. El procedimiento de respuesta a esta emergencia se ve en la figura 05

Fig. 05.



Los casos que generalmente se presentan son los siguientes:
Error físico de un disco de [illegible] (Sin RAID).
Error en Memoria RAM y [illegible] controladores de disco.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, 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 área.
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. Retirar la conexión del servidor con el concentrador, 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.

En caso de: Equivocaciones.

* Cuánto saben los empleados de computadoras o redes.
* Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?
* Difusión de Manuales de Usuario y operación del correcto uso del software y el hardware a todo el personal que labora de manera directa con los equipos informáticos.

En caso de: Virus Informáticos.

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; aislar el virus para su futura investigación.
* El antivirus muestra el nombre del archivo infectado y quién lo usó.
* 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:

* Utilizar los discos de instalación que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado.
* Insertar el disco de instalación antivirus, luego instalar el sistema operativo, 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.

***** TENER EN CUENTA QUE LA LICENCIA DEL FIREWALL PERMITIRÍA OBTENER EL 100 % DE SEGURIDAD PERIMETRAL EN CASO DE VIRUS O INTRUSIONES.**

En caso de: Terremotos o Inundaciones.

* Para evitar problemas con inundaciones ubicar los servidores a un promedio de 50 cm de altura.
* En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.

* Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado.
* Cuando el daño ha sido menor se procede:

a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento

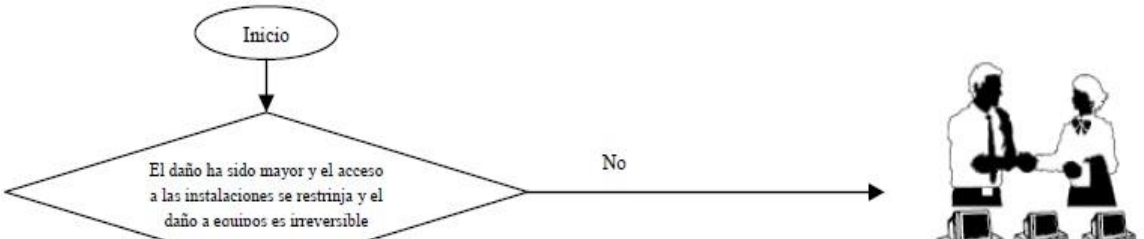
b) Recoger los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.

c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento

d) Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.

e) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

Fig. 06.



En caso de: Accesos no autorizados.

Enfatiza los temas de:

* Contraseñas. Las contraseñas son a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse un número máximo (3) de intentos infructuosos. El Área de Informática implementa la complejidad en sus contraseñas de tal forma que sean más de siete caracteres y consistentes en números y letras.

* Entrampamiento al intruso. Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

* Privilegio. En los sistemas informáticos de la EPYSA, cada usuario se le presenta la información que le corresponde. Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. En este punto el administrador de la red ha clasificado a los usuarios de la red en "Grupos" con el objeto de adjudicarles el nivel de seguridad y perfil adecuado.

IV.- CONCLUSIONES.

- ✓ El presente Plan de contingencias y Seguridad en Información de la EPYSA, tiene como fundamental objetivo salvaguardar la infraestructura de la Red y Sistemas de Información extremando las medidas de seguridad para protegernos y estar preparados a una contingencia de cualquier tipo.

- ✓ Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de riesgos, Evaluación de riesgos, Asignación de prioridades a las aplicaciones, Establecimiento de los requerimientos de recuperación, Elaboración de la documentación, Verificación e implementación del plan, Distribución y mantenimiento del plan.

- ✓ Un Plan de Contingencia es la herramienta que la institución debe tener, para desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones. Las políticas con respecto a la recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

- ✓ No existe un plan único para todas las organizaciones, esto depende de la infraestructura física y las funciones que realiza en Centro de Procesamiento de Datos más conocido como Centro de Cómputo.

- ✓ Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia, por lo cual debe estar plasmado dentro del Plano Primordial de capacitaciones anuales al personal.

V.- RECOMENDACIONES.

- ✓ Programar las actividades propuestas en el presente Plan de Contingencias y Seguridad de Información.

- ✓ Hacer de conocimiento general el contenido del presente Plan de Contingencias y Seguridad de Información, con la finalidad de instruir adecuadamente al personal de la EPYSA.

- ✓ Adicionalmente al plan de contingencias se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.

- ✓ Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la empresa.

- ✓ Urgente se debe tener en cuenta que la Seguridad perimetral de la institución es un factor importante que si no se realiza la adquisición de la licencia, pueden haber muchos ataques informáticos a futuro que tendrían un impacto demasiado infructuoso para la EPYSA.

V.- BIBLIOGRAFÍA.

1.- ARCHIVOS DE DEFENSA CIVIL.
2.- ONGEI.
3.- ANTECEDENTES E HISTORIAL DE LA EPYSA y GBPL.