SERPAR LIMA
Servicio de Parques de Lima

SERVICIO DE PARQUES DE LIMA
OF. PLANIFICACION
24 ENE 2012
Hora ..... Firma .....

RESOLUCION DE GERENCIA GENERAL Nº 030 - 2012

20 ENE 2012

LA GERENCIA GENERAL DEL SERVICIO DE PARQUES DE LIMA HA DICTADO LA SIGUIENTE RESOLUCION:

Visto el Informe N° 008-2012/SERPAR-LIMA/GG/GA/MML de fecha 18 de enero de 2012 suscrito por el Gerente Administrativo de SERPAR-LIMA, solicitando la aprobación del Plan de Contingencia Informático y Seguridad de Información 2011.

CONSIDERANDO:

Que, mediante Informe Nº 059-2010/SERPAR-LIMA//GA/UI/MML, de fecha 16 de agosto de 2010, la Unidad de Informática presentó a la Gerencia Administrativa, el Proyecto de del Plan de Contingencia y Seguridad de la Información, para su revisión y aprobación;

Que, el citado Plan fue elaborado e base a cuatro factores importantes que son: seguridad eléctrica, seguridad de la información, seguridad de equipamiento de los servidores y seguridad de las comunicaciones;

Que, mediante Informe Nº 084-2010/SERPAR-LIMA/GA/UI/MML, de fecha 17 de diciembre de 2010, el Jefe de la Unidad de Informática, señala a la Gerencia Administrativa que se efectuaron modificaciones al Plan;

Que, mediante Informe Nº 073-2011/SERPAR-LIMA/GA/UI/MML, de fecha 25 de julio de 2011, el Jefe de la Unidad de Informática presentó, a la Gerencia Administrativa, el Plan de Contingencia Informático y Seguridad de la Información 2011;

Que, por las facultades que me otorga la Ordenanza Nº 758, que aprueba el Estatuto del Servicio de Parque Lima y en virtud de la Resolución de Consejo Administrativo Nº 004-2011 de fecha 01 de marzo de 2011;

SE RESUELVE:

ARTICULO PRIMERO.- Aprobar el Plan de Contingencia Informático y Seguridad de la Información 2011.

ARTICULO SEGUNDO.- Remitir copia de la siguiente Resolución a la Unidad de Informática para la ejecución del citado Plan.

REGISTRESE, COMUNIQUESE Y CUMPLASE.

SERVICIO DE PARQUES - LIMA
MUNICIPALIDAD METROPOLITANA DE LIMA
Transcripción Nº.....
A:.....UDI.....
Para Conocimiento y fines cumplo con
Transcribir.....
Nº ..... de fecha 20 ENE 2011
Atentamente.
Lic. Adm. ELVIRA CARDENAS PAJUELO
Directora Administración Documentaria

GONZALO LLOSA TALAVERA
GERENTE GENERAL
SERVICIO DE PARQUES
MUNICIPALIDAD METROPOLITANA DE LIMA

SERVICIO DE PARQUES DE LIMA
OF. AUDITORIA INTERNA
24 ENE 2012

NATALIO SANCHEZ 220 OF. 801 – JESUS MARIA Telf.: 433-1535 - 433-1546 Fax: 433-1550

2012 ENE 27

ASC
Hora .....

26 ENE 2012

Municipalidad Metropolitana de Lima

SERVICIO DE PARQUES DE LIMA
OFICINA DE ADMINISTRACION DOCUMENTARIA

HOJA DE TRAMITE

REF: Inf. 08 12 REG:

NOMBRE O RAZON SOCIAL 614

ASUNTO Plan contingencia informática y seguridad de la información 2011

FOLIOS 25

DESTINO	INDICACIONES	FECHA	FOLIOS	HORA	FIRMA
Gc		19.12.2012	25	14.50	

SERVICIO DE PARQUES DE LIMA - GERENCIA JEFATURA ZONAL - V° B° GERENTE GENERAL

☞ INDICACIONES:

☐ URGENTE ☐ MUY URGENTE ☐ ATENCION INMEDIATA

01	Trámite	10	Revisar e Informar
02	Opinión e Informe	11	Aprobarlo
03	Pago Apoyes	12	Coordinar con este Despacho
04	Para su conocimiento y fines	13	Denegar lo Solicitado
05	Adjuntar antecedentes	14	Proyectar Respuesta o Resolución
06	Transcribir	15	Preparar Convenio o Contrato
07	Apoyar lo solicitado	16	Firma o Visación
08	Tratar conmigo sobre el tema	17	Archivo
09	Agradecere sus Comentar os al Respecto	18	

MAYORES DETALLES:

SERPAR – LIMA
Servicios de Parques de Lima
GERENCIA ADMINISTRATIVA

"Decenio de las Personas con Discapacidad en el Perú"
"Año del Centenario de Machu Picchu para el Mundo"

SERVICIO DE PARQUES
MUNICIPALIDAD METROPOLITANA DE LIMA
OFICINA ADMINISTRACION DOCUMENTARIA
19 ENE 2012
UNIDAD DE TRAMITE DOCUMENTARIO
HORA: ..... Nº Exp.: .....

INFORME Nº 008 -2012/SERPAR-LIMA/GG/GA/MML

A	:	*Sr. GONZALO LLOSA TALAVERA* *Gerente General del Servicio de Parques de Lima*
DE	:	*DRA. GLORIA CHAVEZ IDROGO* *Gerente Administrativo*
ASUNTO	:	***PLAN DE CONTINGENCIA INFORMATICO Y SEGURIDAD DE INFORMACION 2011.***
REF.	:	*Informe N° 073-2011/SERPAR-LIMA/GA/UI/MML*
FECHA	:	*Lima, 18 de Enero de 2012.*

Tengo el agrado de dirigirme a usted, a fin de remitir adjunto al presente, el Informe de la referencia, conteniendo el Plan de Contingencia Informático y Seguridad de Información elaborado por la Unidad de Informática de la Entidad.

Cabe indicar que el Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de daños producidos por actos humanos o sucesos naturales en salvaguarda de la información, además constituye una recomendación de la Oficina de Control Interno, por lo que mucho agradeceré de usted, tenga a bien, luego de la evaluación correspondiente, aprobar el citado Plan.

Es cuanto informo a usted, para su conocimiento y fines.

Atentamente,

Dra. GLORIA CHAVEZ IDROGO
GERENTE ADMINISTRATIVO
SERVICIO DE PARQUES
MUNICIPALIDAD METROPOLITANA DE LIMA

Cc. Archivo

INFORME N 073-2011/SERPAR – LIMA/GA/UI/MML

A	:	*DRA. GLORIA CHAVEZ IDROGO* *Gerente Administrativo*
De	:	*SR. FRANKLIN GOMEZ ARQUIÑEGO* *Jefe de la Unidad de Informática*
Asunto	:	*Seguimiento de Medidas Correctivas*
Ref	:	*MEMORANDUM N° 177-2011/SERPAR-LIMA/GG/GA/MML*
Fecha	:	*Jesús María, 25 de Julio de 2011*

25 JUL 2011

Por el presente me dirijo a Ud. a fin de hacerle llegar las nuevas medidas correctivas que menciona el Plan de Contingencia así mismo se va a elaborar un Plan de Recuperación diseñado para la nueva Red que se va a implementar.

Finalmente, adjunto el Plan de Contingencia.

Es cuanto informo a usted, para su conocimiento y fines.

Atentamente

FRANKLIN GOMEZ ARQUIÑEGO
Jefe de la Unidad de Informática
SERVICIO DE PARQUES
MUNICIPALIDAD METROPOLITANA DE LIMA

c.c.
OCI
Archivo.

PLAN DE CONTINGENCIA INFORMÁTICO Y SEGURIDAD DE INFORMACION 2011

PRESENTACIÓN

El Plan de Contingencia Informático (o Plan de Contingencia Institucional) implica un análisis de los posibles riesgos a cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información. Corresponde aplicar a la Unidad de Informática aplicar 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*, así como los *procedimientos relevantes asociados con la plataforma tecnológica. La infraestructura informática* está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la Institución. *Los procedimientos relevantes a la infraestructura informática*, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

El Plan de Contingencia 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. La información como uno de los activos más importantes de la Institución, es el fundamento más importante de este Plan de Contingencia.

El Centro de Procesamiento de Datos o área de Informática, de SERPAR LIMA es la Unidad de Informática (UI). El presente estudio brinda las pautas del Plan de Contingencias Informático y Seguridad de Información 2011 en nuestra Institución

UNIDAD DE INFORMATICA

PLAN DE CONTINGENCIA INFORMATICO Y SEGURIDAD DE INFORMACION 2011

INDICE

2.3.1.1. Acceso No Autorizado

2.3.1.2. Destrucción

2.3.1.3. Modificaciones

CAPITULO I. - ANÁLISIS DE LA SITUACIÓN ACTUAL INFORMÁTICA EN SERPAR LIMA

1.1. Introducción

Cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgo y puede ser frente fuente de problemas. El Hardware, 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 se ha perdido, en que día y hora se ha producido 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 informático, etc.) que producen daño físico irreparable. Frente al mayor de los desastres solo 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 Plan de Contingencia

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 tan grande que resultaría fatal para la organización.

- Permite definir contratos de seguros, que vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades.

1.3. Sistema de Red de Computadoras en SERPAR

La Red de SERPAR cuenta con Tecnologías de la información (TI) en lo referente a: sistemas de información, conectividad y servicios informáticos que se brinda de forma interna y externa a las diferentes Oficinas y Parque. Se resume que la Administración de Red está dividido en dos rubros: 1) Conectividad: se encargada de la conexión alámbrica e inalámbrica de los equipos

de comunicación y 2) Manejo de servidores: se encarga de alojar todos los servicios y sistemas de comunicación e información."

Los servicios de Red implementados en SERPAR LIMA, implementados en sus servidores son los siguientes:

- Servidor de Correo Electrónico
- Servidor de seguridad / Firewall
- Servidor de Proxy
- Servidor de base de datos
- Servidor de Políticas de Grupo – Controlador de dominio

1.4. Sistema de Información en SERPAR

El Sistema de Información, incluye la totalidad del Software de Aplicación, Software en Desarrollo, conjunto de Documentos Electrónicos, Bases de Datos e Información Histórica registrada en medios magnéticos e impresos en papeles, Documentación y Bibliografía.

CAPITULO II. PLAN DE REDUCCIÓN DE RIESGOS

El presente documento implica la realización de un análisis de todas las posibles causas a los cuales puede estar expuestos nuestros equipos de conectados a la RED de SERPAR, así como la información contenida en cada medio de almacenamiento. Se realizara 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 Plan incluye la formación de equipos de trabajo durante las actividades de establecimiento tanto para la etapa preventiva, correctiva y 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

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 (Hw) b) Falla en el hardware de Red (Switches, cableado de la Red, Router, FireWall)
- Incendios

2.1.1. 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 que usaremos para tipificar los posibles problemas son:

Criterios	Escala			
Grado de Negatividad	Leve	Moderado	Grave	Muy Severo
Posible Frecuencia del Evento negativo	Nunca	Aleatorio	Periódico	Continuo

2.1.2. Clases de Riesgo

♣ Se ubica en zona sísmica la 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.

En lo que respecta a Fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de poca intensidad.

2.1.2.1. Clase de Riesgo: Incendio o Fuego

Grado de Negatividad: Muy Severo

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
El área de Servidores de SERPAR no cuenta con un extintor cargado, ubicado dentro del Área de Servidores.	***No cumple***
En todas las Oficinas de SERPAR, no cuenta con un extintor	***Instalar extintores para las áreas SERPAR.***
No se ejecuta un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, lo que no es eficaz para enfrentar un incendio y sus efectos.	***Implantar un Programa de Capitación para el manejo de extintores.***
Debido al incremento del número de computadores por oficina se hace necesario contar con extintores en las oficinas.	***Incrementar el número de extintores por área.***

Una probabilidad máxima de contingencia de este tipo, puede alcanzar a destruir un 50% de las oficinas antes de lograr controlarlo, también podemos suponer que en el área de Servidores tendría un impacto mayor, por no contar con las medidas de seguridad y ambiente que lo protege. Esta información permite resaltar el tema sobre el lugar donde almacenar los backups. El incendio, a través de su acción calorífica, es más que suficiente para destruir los Dispositivos de almacenamiento, tal como CD's, DV's, cartuchos, Discos duros, las mismas que no residen

en una caja fuerte (medio de seguridad que nos protege frente a robo o terremoto, pero no del calor) o lugar parecido. Estos dispositivos de almacenamiento muestran una tolerancia de temperatura de 5°C a 45°C, y una humedad relativa de 20% a 80%.

Para la mejor protección de los dispositivos de almacenamiento, se deben de colocar estratégicamente en lugares distantes, con una Segunda Copia de Seguridad custodiada en un lugar externo a SERPAR.

Las áreas funcionales distribuidas en SERPAR, existe al menos una computadora, por lo que se debe incrementar los elementos y medidas de seguridad contra incendios.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva a colocarlos cerca de las posibles áreas de riesgo que se debe proteger. A continuación se detallan los letreros y símbolos que debe conocer todo el personal en el uso del extinguidor.

CLASE A
(COMBUSTIBLES ORDINARIOS)

Madera, papel, caucho, telas y plásticos.

CLASE B
(IQUIDOS FLAMABLES Y GASES)

Gasolina, aceites, pinturas, lacas y brea.

CLASE C
(FUEGOS QUE INVOLUCRAN EQUIPO ELECTRÓNICO)

CLASE D
(METALES Y COMBUSTIBLES)

CLASE K

(FUEGOS EN EQUIPOS DE COCINA)

Aceites y grasas vegetales y/o animales

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

2.1.2.2. Clase de Riesgo: Robo Común de Equipos y Archivos

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Grado de Impacto: Moderado
Grado de Certidumbre: Aleatorio

Situación actual	Acción correctiva
Vigilancia permanente.	Existe vigilancia. La salida de un equipo informático y es registrada por el personal de la Oficina y no por el personal de seguridad en turno.
No se verifica si el Personal de Seguridad cumple con la inspección de los usuarios, sobre su obligación de cerrar puertas y ventanas al finalizar su jornada.	Al respecto Personal de Seguridad no emite recomendaciones sobre medidas de Alerta y seguridad.
Remitir aviso a la Oficina de Patrimonio, para retirar equipo de Informático.	No Cumple

No se han reportado casos graves en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización debida entre el Jefe del Área funcional y Jefe de Bienes y Servicios. Esto demuestra que los equipos se encuentran protegidos de personas no autorizadas y no identificables.

2.1.2.3. Clase de Riesgo: Vandalismo

Grado de Negatividad: Moderado

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
SERPAR está en una zona donde el índice de vandalismo es bajo .	Hay vigilancia.
Alguna probabilidad de turbas producto de manipulaciones políticas. La destrucción del equipo puede darse por una serie de desastres incluyendo el vandalismo, robo y saqueo en simultáneo.	Mantener buenos vínculos y coordinaciones permanentes con la seguridad del edificio.

2.1.2.4. Clase de Riesgo: Falla en los Equipos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
La Red de Servidores en el SERPAR no cuenta con una Red Eléctrica Estabilizada.	Proponer un Estudio para Instalar una Red Eléctrica Estabilizada.
Cada área funcional se une a la Red a través de Switch Caseros (NO Gabinetes), el recurso limitado de éstos, origina la ausencia de uso de los servicios de red: los Sistemas Informáticos, mantenimiento remoto.	Proteger los Switch, y su adecuado apagado y encendido, dependen los servicios de red en el Área.
La falla en el hardware de los equipos, requiere un rápido mantenimiento o reemplazo. Existe Mantenimiento de los equipos de cómputo.	Contar con proveedores, en caso de requerir reemplazo de piezas, y de ser posible contar con repuestos.

De ocurrir esta contingencia las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos.

El equipo de aire acondicionado y ambiente adecuado en el Área de Servidores, no favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales, necesitan de una fuente de alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del HW y la información podría perderse.

La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico. Se ha identificado los siguientes problemas de energía más frecuentes:

- Fallas de energía
- Transistores y pulsos
- Bajo voltaje
- Ruido electromagnético

- Distorsión

- Variación de frecuencia.

Para los cuales existen los siguientes dispositivos que protegen los equipos de estas anomalías:

- Supresores de picos

- Estabilizadores

- Sistemas de alimentación ininterrumpida (UPS), este último sería lo más recomendable.

Existen formas de prever estas fallas, con la finalidad de minimizar su impacto, entre ellas tenemos:

Tomas a Tierra o Puestas a Tierra

Se denomina así a la comunicación entre el circuito Eléctrico y el Suelo Natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra humedad, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

En la práctica protege de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y para disipar sobretensiones de origen atmosférico o industrial.

La Toma a Tierra tiene las siguientes funciones principales:

a) Protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas.

b) Protege a personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales.,

c) Facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Las Inspecciones deben realizarse trimestralmente, con el fin de comprobar la resistencia y las conexiones. Es recomendable que esta labor se realice en los meses de verano o en tiempo de sequía. Es recomendable un mantenimiento preventivo anual dependiendo de las propiedades electroquímicas estables.

Extensiones eléctricas y capacidades

Las computadoras ocupan rápidamente toda la toma de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado.

No solo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.

Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.

No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase más corriente de la que los cables están diseñados para soportar. Se debe utilizar los enchufes de pared siempre que sea posible.

Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar limitar el daño ante fallas eléctricas.

Adquirir toma de corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar con enchufes de espigas planas, como cilíndricas.

Tanto las tomas corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

2.1.2.5. Clase de Riesgo: Equivocaciones

Grado de Negatividad: Moderado

Frecuencia de Evento: Periódico

Grado de Impacto: Moderado

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Las equivocaciones que se producen en forma rutinaria son de carácter involuntario.	Capacitación inicial en el ambiente de trabajo. Instruir al nuevo usuario con la elaboración de un Manual de Procedimientos
Cuando el usuario es practicante y tiene conocimientos de informática, tiene el impulso de navegar por los sistemas.	En lo posible se debe cortar estos accesos, limitando su accionar en función a su labor de rutina.
La falta de institucionalizar procedimientos produce vacíos y errores en la toma de criterios para registrar información.	Reuniones y Actas de Trabajo para fortalecer los procedimientos.
Ante nuevas configuraciones se comunica a los usuarios sobre el manejo, claves, accesos y restricciones, tanto a nivel de Sistemas, Internet.	Enviar oficios circulares múltiples comunicando los nuevos cambios y políticas. Convocar reuniones de capacitación antes nuevas opciones en los sistemas.

2.1.2.6. Clase de Riesgo: Acción de Virus Informático

Grado de Negatividad: Muy Severo

Frecuencia de Evento: Continuo

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
No se cuenta con un Software Antivirus corporativo. Pero no hay un contrato anual para su actualización.	No se cumple. Se debe evitar que las licencias no expiren, se requiere la renovación de contrato anualmente.
Todo Software (oficina, informática, mantenimiento, drives, etc.) es manejado por personal de Informática, quienes son los encargados de su instalación en las PC's con su respectivo software.	Se cumple.
Se tiene un programa permanente de bloqueo acciones como cambiar configuraciones de red, acceso a los servidores, etc.	Se cumple a través de políticas de usuarios.
De tener Antivirus este tiene que ser instalado el antivirus de red y en estaciones de trabajo. Antes de logear una maquina a la red (dominio) se comprueba al existencia de virus en la PC.	No se cumple
Informática no recibe comunicación del personal de reemplazo por vacaciones. ni cuando se integran y cuando ya o pertenecen a la institución por lo tanto supone que es la Oficina usuaria la que capacita al reemplazante	Se debe informar a Informática del reemplazo para registrarlo y darle los accesos permitidos a la Red y los Sistemas, por el tiempo que dure el reemplazo. Al término del periodo de reemplazo se restituye los valores originales a ambos usuarios.

En estos últimos años la acción del virus informático ha sido contrarrestada con la diversidad de productos que ofrece el mercado de software. Las firmas y/o corporaciones que proporcionan software antivirus, invierten mucho tiempo en recopilar y registrar virus indicando en la mayoría de los casos sus características y el tipo de daño que puede provocar, por este motivo se requiere de una actualización periódica del software antivirus

2.1.2.7. Clase de Riesgo: Fenómenos Naturales

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
La última década no se han registrado contingencias debido a fenómenos naturales como: terremotos, inundaciones, aluviones, etc.	Medidas de prevención.

Potencialmente existe la probabilidad de sufrir terremotos debido a las contantes movimientos continuos que hay en nuestro País.	Medidas de prevención.
El ambiente donde se encuentra los Servidores principales, no es apropiado ante estos posibles movimientos.	Ubicación apropiada.

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en la sala de Computación Central, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

2.1.2.8. Clase de Riesgo: Accesos No Autorizados

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Se controla el acceso al Sistema de Red mediante la definición de "Cuenta" o "Login" con su respectiva clave	Se cumple
A cada usuario de Red se le asigna los "Atributos de confianza" para el manejo de archivos y acceso a los sistemas.	Se cumple
Cuando el personal cesa en sus funciones y/o es asignado a otra área, se le redefinen los accesos y autorizaciones, quedando sin efecto la primera.	Se cumple de modo extemporáneo, siendo lo indicado actualizar los accesos al momento de producirse el cese o cambio
Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado. En algunos casos los usuarios escriben su contraseña (Red o de Sistemas) en sitios visibles.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica.
No se tiene un registro electrónico de Altas/Bajas de Usuarios, con las respectivas claves.	Se debe implementar

Todos los usuarios sin excepción tienen un "login" o un nombre de cuenta de usuario y una clave de acceso a la red. No se permiten claves en blanco

Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o utilizar un bloqueador de pantalla. Ello se aplica tanto a su autenticación como usuario de Red como usuario de Sistemas en SERPAR, si lo tuviere.

2.1.2.9. Clase de Riesgo: Robo de Datos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Las Oficinas tienen disponible disqueteras, quemadoras de CD/DVD, puertos USB, pero no se lleva un control sobre la información que ingresa y/o sale del ordenador.	Personal de Planta debe manejar información delicada de la Oficina.
El servicio de Internet es potencialmente una ventaja abierta para el robo de información electrónica	Existen políticas que regulan el uso y acceso del Servicio de Internet.
El acceso a los terminales se controla, mediante claves de acceso, de esta manera se impide el robo de información electrónica. A través de las políticas se seguridad se impide el ingreso a los Servidores.	Se cumple

El robo de datos se puede llevarse a cabo bajo tres modalidades:

- La primera modalidad consiste en sacar "copia no autorizada" a nuestros archivos electrónicos aun medio magnético y retirarla fuera de la institución.

- La segunda modalidad y tal vez la más sensible, es la sustracción de reportes impresos y/o informes confidenciales.

- La tercera modalidad es mediante acceso telefónico no autorizado, se remite vía Internet a direcciones de Correo que no corresponden a la Gestión Institucional.

2.1.2.10. Clase de Riesgo: Manipulación y Sabotaje

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Existe el problema de la inestabilidad laboral, la misma que podría obligar a personas frustradas, o desilusionadas a causar daños	La protección contra el sabotaje requiere:

físicos y lógicos en el sistema de información de la institución. Esto se puede traducir desde el registro de operaciones incorrectas por parte de los usuarios finales, hasta la operación de borrar registros en el sistema y conductas de sabotaje	Una selección rigurosa del personal. Buena administración de los recursos humanos Buenos controles administrativos Buena seguridad física en los ambientes donde están los principales componentes del equipo. Asignar a una persona la responsabilidad de la protección de los equipos en cada área.
No se comunica el movimiento de personal a Informática, para restringir accesos del personal que es reubicado y/o cesado de a SERPAR.	Es conveniente la comunicación anticipada del personal que será reubicado y/o cesado con el objeto de retirar los derechos de operación de escritura para otorgarle los derechos de consulta antes de desactivar la cuenta.
Existe el antecedente de origen sabotaje interno. Como es el caso de trabajadores que han sido despedidos y/o están enterados que van a ser rescindidos su contrato, han destruidos o modificado archivos para su beneficio inmediato o futuro.	Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado.

El peligro más temido por los centros de Procesamiento de Datos, es el sabotaje. Instituciones 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 trabajador o un sujeto ajeno a la propia institución. Un acceso no autorizado puede originar sabotajes.

Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios. Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del Indice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existen un plan Idóneo o una recomendación simple para resolver el problema de la seguridad. Realmente no es una situación estática a un problema "puntual", sino que requiere un constante y continuo esfuerzo y dedicación, educando también al usuario a hacer responsable.

Resumen de la Clase de Riesgos

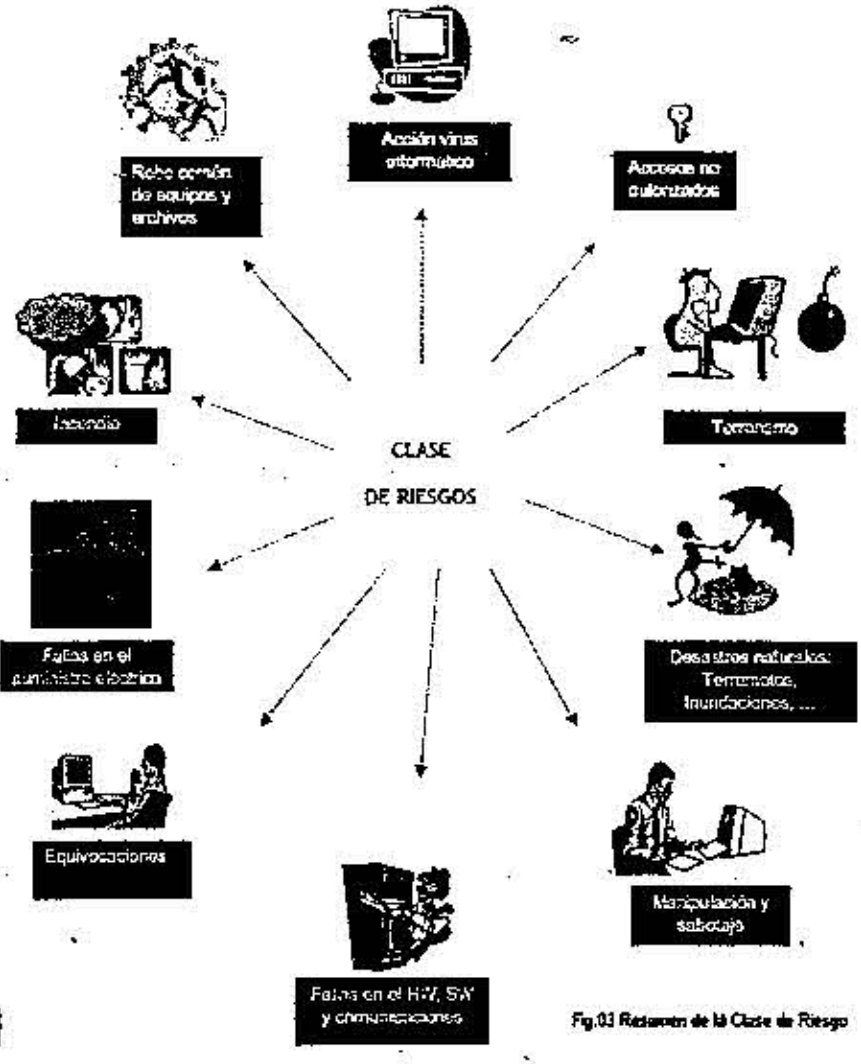

Fig.03 Relación de la Clase de Riesgo

2.2. Análisis en las fallas en la Seguridad

En este se abarca 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.

2.3. Protecciones actuales

Se realizan las siguientes acciones:

♣ Se hace copias de los archivos que son vitales para la institución. No se cumple por no tener implementado un Storage o Servidor Backup.

♣ Al robo común se cierran las puertas de entrada y ventanas

♣ 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. No se cumple por no tener un constante Licenciamiento permanente.

♣ A las equivocaciones, los empleados tienen buena formación. Cuando se requiere personal temporal se intenta conseguir a empleados debidamente preparados. Tampoco se cumple ya que le personal debe estar en constante actualización de software de Oficina.

♣ 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, se cierra la puerta de entrada. Varias computadoras disponen de llave de bloqueo del teclado.

♣ Al robo de datos, se cierra la puerta principal y gavetas de escritorios.

♣ Al fuego, en la actualidad no se encuentran instalados extintores, en sitios estratégicos y debe brindarse entrenamiento en el manejo de los extintores al personal, en forma periódica.

2.3.1. Seguridad de información

La Seguridad de información y por consiguiente de los equipos informáticos, es un tema que llega a afectar la imagen Institucional de las empresas, incluso la vida privada de personas. Es obvio el interés creciente que día a días se evidencia sobre este aspecto de la nueva sociedad informática.

Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y a menudo es vulnerable a cualquier ataque.

La Seguridad de información tiene tres directivas básicas que actúan sobre la Protección de Datos, las cuales ejercen control de:

♣ La lectura

Consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales y mantenimiento de la seguridad en el caso de datos institucionales.

♣ La escritura

Es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad que se les ha confiado.

♣ El empleo de esa información

Es Secreto de logra cuando no existe acceso a todos los datos sin autorización. La privacidad se logra cuando los datos que puedan obtenerse no permiten el enlace a individuos específicos o no se pueden utilizar para imputar hechos acerca de ellos.

Por otro lado, es importante definir los dispositivos de seguridad durante el diseño del sistema y no después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

2.3.1.1. Acceso no autorizado

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados:

♣ Control de acceso a Informática

La libertad de acceso a Informática puede crear un significativo problema de seguridad. El acceso normal debe ser dado solamente a la gente que trabaja en esta oficina. Cualquier otra persona puede tener acceso únicamente bajo control.

Debemos mantener la seguridad física de la Oficina como primera línea de defensa. Para ello se toma en consideración el valor de los datos, el costo de protección, el impacto institucional por la pérdida o daño de la información. La forma propuesta de implantar el Control de Acceso a Informática, sería la siguiente:

♣ Para personas visitantes, vigilancia otorgara el Credencial de Visitante. No se Cumple

♣ Para personal de SERAPR, con autorización del encargado de la Oficina. No se cumple

♣ Acceso limitado computadoras personales y/o terminales de la red.

Los terminales que son dejados sin protección pueden ser mal usados. Cualquier Terminal puede ser utilizado para tener acceso a los datos de un sistema controlado.

♣ Control de acceso a la información confidencial.

Sin el debido control, cualquier usuario encontrara la forma de lograr acceso al Sistema de Red, a una base de datos o descubrir información clasificada. Para revertir la posibilidad de ataque se debe considerar:

Programas de control a los usuarios de red

El sistema Operativo residente en los servidores de Informática es Linux. A través del Servicio de "Samba LDAP" permite administrar a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente.

Palabra de acceso (password)

Es una palabra o código que se ingresa por teclado antes que se realice un proceso.

Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados. La identificación del usuario debe ser muy difícil de imitar y copiar. No se cumple porque se descubrió que los usuarios se estandarizan contraseñas por área.

El Sistema de Información debe cerrarse después que el usuario no autorizado falle tres veces de intentar ingresar una clave de acceso. Las claves de acceso no deben ser largas puesto que son más difíciles de recordar. Una vez que se obtiene la clave de acceso al sistema, esta se utiliza para entrar al sistema de Red de Información vía Sistema Operativo.

La forma más común de intentar descubrir una clave es Observando el Ingreso de la clave

En todo proceso corporativo es recomendable que el responsable de cada área asigne y actualice de forma periódica el "password" a los usuarios.

No se puede depender de un operador o responsable de terminal, que trabe la operatividad normal de la Institución.

Niveles de Acceso

Las políticas de acceso aplicadas, deberá identificar los usuarios autorizados a emplear determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas.

La forma fundamental de autoridad la tiene el Administrador de Redes con derechos totales. Entre otras funciones puede autorizar nuevos usuarios, otorgar derechos para modificar estructuras de las Bases de Datos, etc.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

Nivel	Concepto
Consulta de la información	El privilegio de lectura está disponible para cualquier usuario y solo se requiere presentaciones visuales o reportes. La autorización de lectura permite leer pero no modificar la Base de Datos.
Mantenimiento de información	Permite el acceso para agregar nuevos datos, pero no modifica los ya existentes, permite modificar pero no eliminar los datos. Para el borrado de datos, es preferible que sea responsabilidad de la Unidad de Informatica.

2.3.1. 2. Destrucción

Sin adecuadas medidas de seguridad la institución puede estar a merced no solo de la destrucción de la información sino también de la destrucción de sus equipos informáticos. La destrucción de los equipos puede darse por una serie de desastres como son: incendios, inundaciones, sismos, posibles fallas eléctricas o sabotaje, etc.

Cuando se pierden los datos y no hay copias de seguridad, se tendrá que recrear archivos, bases de datos, documentos o trabajar sin ellos.

Está comprobado que una gran parte del espacio en disco está ocupado por archivos de naturaleza histórica, que es útil tener a mano pero no son importantes para el funcionamiento normal. Un ejemplo típico son las copias de la correspondencia conservados como documentos de referencia o plantilla. Si se guarda una copia de seguridad de estos archivos las consecuencias de organización pueden ser mínimas.

Los archivos Electrónicos Contable son de disposición diferente, ya que volver a crearlos puede necesitar de mucho tiempo y costo. Generalmente la institución recurre a esta información para la toma de decisiones.

Sin los datos al día, si el objetivo se vería seriamente afectado. Para evitar daños mayores se debería hacer copias de seguridad de la información vital para la institución es un servidor de Backup o Storage y almacenarlos en lugares apropiados (de preferencia en lugar externo a las instalaciones).

Hay que protegerse también ante una posible destrucción del hardware o software por parte del personal no honrado. Por ejemplo, hay casos en la que, trabajadores que han sido recientemente despedidos o están enterados que ellos van a ser cesados, han destruido o modificado archivos para su beneficio inmediato o futuro. Depende de los Jefes inmediatos de las áreas funcionales dar importancia a estos eventos, debiendo informar al Jefe de Informatica para el control respectivo.

2.3.1. 3. Modificaciones

Hay que estar prevenido frente a la tendencia a asumir que "si viene de la computadora, debe ser correcto".

La importancia de los datos modificados de forma ilicita, está condicionada al grado en que la institución, depende de los datos para su funcionamiento y toma de dediciones. Esto podría disminuir su efecto su los datos procedente de las computadoras se verificaran antes de constituir fuente de información para la toma de decisiones.

Los elementos en la cual se han establecido procedimientos para controlar modificaciones ilícitas son:

- Nuestra mejor protección contra la perdida/modificación de datos consiste en hacer copias de seguridad, almacenando en copias no autorizadas de todos los archivos valiosos en un lugar seguro.

- Los usuarios: los usuarios deben ser concientizados de la variedad de formas en que los datos pueden perderse o deteriorarse.

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.

Procedimientos para controlar modificaciones ilícitas

Física: Fenómenos naturales, fuego, temperatura, ..

Instalaciones eléctricas y de datos

Acceso del personal, ...

Software y Datos:

- Copias de seguridad:

¿Dónde? ¿Cuándo? ¿Cuántas? ¿Tipos? ...

Control de fuga de información

Acceso de usuarios:

Categorías, Niveles, ..

para las: Aplicaciones, Internet, Correo, ...