Serpost
Sub-Gerencia de Tecnologías de la Información
608 02 OCT 2017
SECRETARIA
Hora: ... Firma: ...

Serpost
El Correo del Perú
GERENCIA GENERAL
15772 9 SEP 2017
RECEPCION
FIRMA: ..... HORA: 4:30 PM

MEMORANDO N° 450 –D/17

PARA : Sr. **ENRIQUE CABALLERO ELCORROBARRUTIA**
Gerente General (e)

ASUNTO : Plan de Contingencia y Seguridad de Centro de Datos

REF. : Memorándum N° 442-DI/17

FECHA : Los Olivos, 29 de setiembre de 2017

Me dirijo a usted, a fin de derivar el documento de la referencia, remitido por el Sub-Gerente de Tecnologías de la Información, mediante el cual adjunta el **Plan de Contingencia y Seguridad de Centro de Datos**, debidamente actualizado

Agradeceré que por medio de su Despacho se apruebe dicho documento.

Atentamente

Srta. Magali Angulo Daneri
Gerente de Desarrollo Corporativo
Serpost
El Correo del Perú

Gerencia General (e)
V°B°
Serpost
ENRIQUE CABALLERO ELCORROBARRUTIA
02/10/17
APROBADO

Serpost
Gerencia de Desarrollo Co...
07 OCT 2017
RECIBIDO
Hora 11:10 Firma

Tesmi:
Conocimiento
02.10.17

Sub-Gerencia de Tecnologías de la Información
V°B°
Serpost

DI,
Favor Proceder.
02.10.17

C C
DI

Serpost
SERVICIOS POSTALES DEL PERU S.A.

Plan de Contingencia y Seguridad del Centro de Datos

Subgerencia de Tecnologías de la Información

Departamento de Tecnología y Comunicaciones
Departamento de Sistemas de Información

Setiembre 2017

Resumen

ÍNDICE

Resumen

PRESENTACIÓN

La seguridad del Centro de Cómputo, de su personal, de la información y de la documentación del mismo, son fundamentales para asegurar el cumplimiento de los objetivos de Serpost S A

El establecimiento de procedimientos y medidas de seguridad están destinados a salvaguardar las instalaciones del Centro de Cómputo, al personal, la información y documentación generada contra cualquier evento natural o humano que de forma intencional o accidental puedan afectarlos y reestablecer el servicio si éste se viera interrumpido o minimizar el tiempo fuera de servicio

Las eventualidades se definen como eventos naturales o creados por el hombre que amenazan o que interrumpen la operación del Centro de Cómputo de Serpost S A , o que rompen la cadena de control de los procesos La seguridad del personal es primordial, el uso de estos procedimientos jamás deberá poner en peligro a los mismos

El personal de la Subgerencia de Tecnologías de la Información debe conocer estos procedimientos, tanto para aplicar las medidas preventivas así como en caso se presente una eventualidad actuar de la manera apropiada Sin embargo, consideramos que no sólo es responsabilidad de la Sub Gerencia de Tecnologías de la Información sino de todos los Centros de Responsabilidad de la empresa proteger la información y los equipos que la contienen, siendo ésta la mejor manera de preservar la integridad física de las personas, así como de salvaguardar la información vital de la empresa

El presente documento de trabajo es el Plan de Contingencia que contempla todos los riesgos y procedimientos de mitigación o reducción de las eventualidades por parte del Departamento de Tecnología y Comunicaciones

El plan de contingencia y centro de datos será revisado y/o actualizado en una periodicidad no mayor a dos (2) años o cuando ocurran cambios sustanciales que afecte la operatividad de la empresa

Capítulo
1

PLAN DE CONTINGENCIAS

1. PLAN DE CONTINGENCIA Y SEGURIDAD DE DATOS

Objetivos

Los objetivos del presente Plan de Contingencia de Datos son

- Proporcionar los procedimientos para la identificación de las eventualidades que puedan afectar el Centro de Cómputo
- Señalar las medidas preventivas para protección del personal y de la infraestructura del Centro de Cómputo
- Señalar los procedimientos de reparación del servicio en cada caso en que éste se afectara

Ámbito de Aplicación

Este plan contempla directamente la seguridad, procedimientos y métodos de recuperación en caso de desastre tanto del Centro de Datos como del personal de la Subgerencia de Tecnología de la información

Resultados Esperados.

- Tener salvaguardada la información crítica y relevante de Serpost S A
- Lograr, en caso de desastre, restaurar en el menor tiempo posible las aplicaciones y funciones más importantes del Centro de Datos
- Tener los procedimientos adecuados para salvaguardar la integridad física de las personas que laboran en el centro de cómputo.

1.1 PLAN DE REDUCCIÓN DE RIESGO (Plan de Seguridad)

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y la información contenida en los diversos medios de almacenamiento

Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto, es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles

1.1.1. ANÁLISIS DE RIESGO

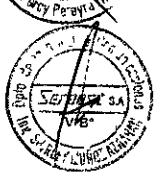
1. RIESGOS IDENTIFICADOS

Cód.	Identificación del Riesgos	Probabilidad	Impacto	Valoración
R1	Perdida de información en la Base de Datos	Medio	Alto	Importante
R2	Falta de equipos informáticos por falta de mantenimiento	Baja	Medio	Tolerable
R3	Riesgo de acceso no autorizado	Baja	Alto	Moderado
R4	Daño físico en los medios de respaldo de información	Baja	Alto	Moderado
R5	Perdida de los enlaces de comunicación	Medio	Bajo	Tolerable
R6	Falta de servidores por falta de mantenimiento	Baja	Medio	Tolerable
R7	Indisponibilidad de Base de Datos	Medio	Medio	Moderado
R8	Falta de soporte y mantenimiento de los aplicativos	Baja	Medio	Tolerable
R9	Incendio de Centro de Computo	Baja	Alto	Moderado

2. ACCIONES PARA MITIGAR LOS RIESGOS

Cód.	Identificación de Riesgos	Acciones para mitigar los riesgos
R1	Pérdida de información en la Base de Datos	Realizar copias de seguridad de la información, resguardar en una empresa especializada y realizar pruebas periódicas de restauración para verificar la correcta recuperación Contar con un especialista en Base de Datos Oracle, para mejora, afinamiento y reingeniería de algunos procesos críticos Contar con un equipo de Calidad en el área de Sistemas antes de pasar a producción los desarrollos
R2	Falla de equipos informáticos por falta de mantenimiento	Contar con un plan vigente de mantenimiento preventivo, correctivo de equipos informáticos a nivel nacional
R3	Riesgo de acceso no autorizado	Contar con Directivas, Normas y Procedimientos actualizados para el control de acceso a los servidores
R4	Daño físico en los medios de respaldo de información	Renovación periódica de los dispositivos de respaldo de información
R5	Pérdida de los enlaces de comunicación	Solicitar periódicamente al proveedor ISP el mantenimiento preventivo de los equipos de enlace de comunicación
R6	Falla de servidores por falta de mantenimiento	Contar con un plan de mantenimiento preventivo, correctivo de servidores
R7	Indisponibilidad de Base de Datos	Monitoreo constante de las actividades del servidor para alertar posibles causas que originen indisponibilidad con el proveedor Establecer políticas y procedimientos para mejorar la estructura de la base de datos corporativa
R8	Falta de soporte y mantenimiento de los aplicativos	Contratar los servicios de soporte y mantenimiento y mejora continua para los aplicativos de terceros



		Establecer mejoras o renovación de los aplicativos implementados en SERPOST S A, aplicando procedimientos respectivos como "Procedimiento estándar para el Ciclo de Desarrollo de Sistemas" y "Desarrollo de Aplicaciones" vigente, entre otros.
R9	Incendio de Centro de Computo	Mejora de la infraestructura del Centro de Computo acorde con los estándares para este tipo de ambiente

3. EQUIPOS DE MISIÓN CRÍTICA

Los equipos de misión crítica son los siguientes

Servidor	Contenido	Prioridad
ARAGORN	Active Directory, DNS y servicio DHCP	1
NIMRODEL	Servidor de archivos y aplicaciones	2
TELPERION	Servidor de imágenes digitalizadas vía WEB	3
TELEFONIA	Servidor Telefonía IP (Asterisk)	4

4. APLICACIONES DE MISIÓN CRÍTICA

En la siguiente lista se detallan las aplicaciones de misión crítica

Aplicaciones	Contenido	Prioridad
Sistema Operativo Postal (SOP)	Soporta las actividades operativas postales del CCPL, registra y despacha la correspondencia de llegada internacional, correspondencia de tránsito entre las localidades del Perú	1
Sistema de Soporte de Administraciones Postales	Soporta las actividades de expendio, caja, despacho y distribución de las oficinas postales así como por medio del módulo de bóveda de valores abastecen de estampillas a las administraciones postales por medio de despachos	2
Sistema Integrado de Mensajería (SIM)	En este sistema se administra la información del servicio de clientes empresariales a nivel nacional	3
De Seguridad Informática Externa	Nos mantiene conectados de manera segura con Internet y Aduanas	4
De los Servidores publicados en Internet	Nos mantiene comunicados con nuestros clientes, proveedores y el mundo entero	5
Sistema ERP-SAP	Este sistema inicio sus operaciones el año 2013, en la misma se almacena información de los Departamentos de Presupuesto, Logística, Contabilidad y Tesorería	6
De Recursos Humanos (SPRING)	Para manejar los aplicativos y base de datos del área de RRHH	7

Aplicaciones	Contenido	Prioridad
De Finanzas y Contabilidad	Para manejar los aplicativos y base de datos de Finanzas y Contabilidad, la información histórica que se mantiene en el mismo hasta el año 2012, pues estos sistemas fueron reemplazados a inicios del año 2013 por el sistema ERP-SAP	8

Para el mantenimiento de las aplicaciones desarrolladas por Serpost S A se deberá cumplir con los procedimientos relacionados, como "Procedimiento estándar para el Ciclo de Desarrollo de Sistemas" y "Desarrollo de Aplicaciones" vigente entre otros

5. COPIAS DE RESPALDO

La copia de respaldo se realiza de forma permanente en coordinación con el proveedor de CDC

1.2 PLAN DE RECUPERACION DE DESASTRES

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de las PCs

Producidos los riesgos identificados (ver tabla Nro 1), las actividades a considerar en un Plan de Recuperación de Desastre se pueden clasificar en las siguientes etapas

1.1.2. ACTIVIDADES PREVIAS AL DESASTRE

Establecimiento de Plan de Acción

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a

a) Sistemas e Información
b) Equipos de Cómputo
c) Obtención y almacenamiento de los Respaldos de Información (BACKUPS)
d) Políticas (Normas y Procedimientos de Backups)

a) <u>Sistemas e Información</u>.

Relación de sistemas y aplicaciones en producción desarrolladas por la Subgerencia de Tecnologías de la Información.

Descripción
NIMRODEL
Servidor de Aplicaciones
TELEFONIA
Sistema de Control de llamadas Telefónicas
TELPERION
Imágenes Clientes Empresariales(área de Digitalización)

El orden de prioridad de activación deberá ser considerado según lo indicado en el punto 1 2 -PLAN DE REDUCCIÓN DE RIESGO Numeral 4 APLICACIONES DE MISION CRITICA, y las aplicaciones que no figuran en dicha lista deben ser consideradas final

b) **Equipos de Cómputo.** Se debe tener en cuenta lo siguiente

- Inventario actualizado de los equipos de manejo de información (computadoras, impresoras, etc), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso
- Pólizas de Seguros Comerciales Como parte de la protección de los Activos de la empresa, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del Computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados
- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada Sistema permanente de la Institución (que por sus funciones constituyen el eje central de los Servicios Informáticos de la Institución), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas

Servidores:

- Contar con el inventario actualizado de los servidores, especificando su contenido (software que usa data que contiene), su ubicación y nivel de uso
- Contar con Pólizas de Seguros Comerciales, como parte de la protección de los Activos de la empresa, pero haciendo la salvedad en el contrato que en casos de siniestros, la restitución del servidor siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando este dentro de los montos asegurados
- Señalización o etiquetado de los Servidores de acuerdo a la importancia de su contenido, para ser priorizado en caso de evacuación
- Contar con la información actualizada del plan de contingencia de los servicios que se encuentran alojados fuera de las instalaciones de SERPOST, como ejemplo CDC de FONAFE

Internet:

- Contar con los números telefónicos de contacto del proveedor de Internet que se encuentre vigente, el mismo que en la actualidad es proveído por CDC FONAFE

1.1.3. ACTIVIDADES DURANTE EL DESASTRE

Durante el desastre seguir las acciones descritas para el caso de Emergencia para los equipos de Cómputo y Emergencia para la Lógica de Datos (Ver Anexos 1 y 2)

1.1.4. ACTIVIDADES DESPUES DEL DESASTRE

1.1.4.1. Evaluación de Daños.

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

Para el caso de los servidores alojados en el centro de datos corporativo externo a SERPOST S A , se deber solicitar información del estado actual de los servicios

1.1.4.2. Priorizado de actividades del Plan de Acción.

Toda vez que el Plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, contemplando siempre las actividades estratégicas y urgentes de nuestra Institución

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su posterior asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico

1.1.4.3. Ejecución de Actividades.

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

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y 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 el servicio y la operatividad de la empresa

1.1.4.4. Retroactividad del Plan de Acción.

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

El otro elemento es evaluar cuál hubiera sido el costo de no haber tenido nuestra Institución el plan de contingencias llevado a cabo

Capítulo

2

SEGURIDAD DEL CENTRO DE DATOS

La Subgerencia de Tecnología de la Información debe mantener y asegurar la Seguridad del Centro de Datos de la siguiente manera

- A través del Departamento de Tecnología y Comunicaciones
    - Estableciendo políticas de acceso a los datos a las personas, otorgando a las personas que tienen derecho a ellas y negando a las que no, al cual también se le puede llamar protección de las privacidades (Datos personales) y manteniendo la seguridad (datos institucionales)
    - Garantizando 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

    Los accesos brindados a los usuarios ejercen un control de lectura, escritura, lo que origina la protección de los datos, mantenimiento de la privacidad y la seguridad del secreto (el mismo que se logra cuando no existe acceso a todos los datos sin autorización)

- A través del Departamento de Sistemas de la Información

    Incorporando dispositivos de seguridad durante el diseño de los aplicativos desarrollados en la empresa (auditorias, mecanismos de control, entre otros)

Asimismo, se deberán cumplir según su competencia con las directivas y normar referentes a la Seguridad de la Información, las cuales son

- Políticas de Seguridad para cumplir la norma 17799 2007 según Directiva N°010-G/10
- Política de Acceso a la Información Pública Aprobada el 18 de enero del 2013
- Directiva 002-G/16 Acceso a sistemas informáticos y Medidas de Seguridad
- Normas y Procedimientos para el Control e Inventario físico de bienes patrimoniales, 28 de agosto 2013
- Normas y Procedimientos para la Recepción, ingreso y salida de materiales del Almacén, 16 de enero 2017
- Capítulo XII de la utilización de los servicios informáticos del RIT

En el anexo 9, se describen conceptos relacionados a la Seguridad Informática a tomar en cuenta

Por otro lado, se deberá aplicar los controles referidos a temas informáticos, definidos en el Sistema de Gestión de Seguridad de la Información (NTP ISO/IEC 27001 2008) que deberá ser coordinado con cada una de las áreas de la empresa El comité de Seguridad de la Información de la empresa, el mismo que deberá ser alineada a la Norma de Seguridad de la

Información basados en la NTP ISO/IEC 27001 2008, para lo cual cuenta con una Política de Seguridad de la Información aprobada

A continuación se presenta algunos sucesos a ser considerados para preservar la Seguridad Informática

2.1 ACCESO NO AUTORIZADO

Para el control de la seguridad de la información se debe tener en cuenta medidas de seguridad que garanticen accesos autorizados a

- Área de Sistemas
- Computadoras personales y/o Terminales de la red
- Información Confidencial.

2.1.1 Control de acceso al área de Sistemas

El acceso al centro de cómputo (o sala de Servidores) está autorizado al personal que realiza funciones en el Departamento de Tecnología y Comunicaciones En caso que otra persona, que desea tener acceso a dicha área deberá solicitar la autorización respectiva al Jefe del Departamento de Tecnología y Comunicaciones, el mismo que podrá acceder únicamente bajo control y previo registró en el cuaderno de registro *Ver Normas para el Registro de Entradas y Salidas a la Sala de Servidores*

2.1.2 Acceso limitado a los terminales

Los usuarios que tienen asignados equipos de cómputo para el cumplimiento de sus funciones son responsables del buen uso de los mismos, así como de las contraseñas asignadas puesto que son de uso exclusivo y se encuentra totalmente prohibida su difusión En caso de tomar conocimiento que otra persona conoce su clave de acceso el trabajador, está obligado a modificar el mismo mediante el uso de los comandos propios del sistema operativo *(CRTL+ALT+SUPR, Cambiar contraseña)*

De otra parte, los usuarios deberán bloquear su terminal cuando éste no sea utilizado, pasado un tiempo predeterminado (5 - 10 Min) Las contraseñas de acceso a la red LAN deberán ser cambiadas mensualmente por los usuarios, mediante el uso de los comandos propios del sistema operativo *(CRTL+ALT+SUPR, Cambiar contraseña)*

2.1.3 Control de Acceso a la Información

Para prevenir que algunos usuarios o extraños (personal no autorizado) puedan encontrar alguna forma mediante la cual, logren el acceso a los sistemas de información de la empresa o la base de datos y descubrir información clasificada o datos no autorizados Se debe tener en cuenta lo siguiente

Programas de Control Para brindar los accesos a los sistemas de información se cuenta con un módulo de administración de cuentas de usuario para brindar los derechos de acceso a los usuarios según sus funciones, el mismo que se encuentra a cargo del Departamento de Sistemas de Información

Palabra de Acceso (Password) Los usuarios deben utilizar claves difíciles que contengan caracteres alfanuméricos que no se puedan imitar y copiar, para proteger los programas y datos contra usuarios no autorizados

En caso un usuario no autorizado obtenga una clave de acceso al sistema, podrá ingresar a la base de datos mediante el uso de los aplicativos Los usuarios son los responsables del uso de sus claves de acceso a fin de evitar que otra persona lo utilice de manera dañina

En caso que los usuarios se equivoquen en sus contraseñas los sistemas de información contemplan un máximo de tres intentos fallidos (aplicado en el SAP) posteriormente se cierra En todo proceso corporativo es recomendable que el responsable de cada área a fin que los usuarios a cargo actualicen de forma periódica su password

Niveles de Acceso. Los sistemas de información contemplan niveles de acceso de acuerdo a las funciones a realizar Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas

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

- Nivel de consulta de la información no restringida o reservada

  El privilegio de lectura está disponible para cualquier usuario y sólo se requiere un conocimiento de la estructura de los datos, o del Sistema de otro usuario para lograr el acceso La autorización de lectura permite leer pero no modificar la base de datos

- Nivel de mantenimiento de la información no restringida o reservada

  El concepto de mantenimiento de la información consiste en

  Ingreso. Permite insertar datos nuevos, pero no se modifica los ya existentes

  Actualización. Permite modificar la información, pero no la eliminación de datos

  Borrado. Permite la eliminación de datos

- Nivel de consulta de la información incluyendo la restringida o reservada
- Nivel de mantenimiento de la información incluyendo la restringida

Un usuario puede tener asignados todos, ninguno o una combinación de los tipos de autorización anteriores

2.2 DESTRUCCIÓN

Sin adecuadas medidas de seguridad la empresa puede estar a merced no sólo de la destrucción de la información sino también de la destrucción de su equipo informático

La destrucción del equipo puede darse por una serie de desastres como son incendios, inundaciones, sismos, o posibles fallas eléctricas, entre otros

Al perderse los datos y no encontrarse disponibles copias de seguridad, se deben volver a crear los datos o trabajar sin ellos, como por ejemplo memorándums, cartas, informes, entre otros que puedan servir como referencia para la generación de documentos similares, sin embargo, a pesar que esto pueda generar malestar en los usuarios, no causará mayor impacto en la empresa

Para el caso de archivos contables suponen una situación diferente, ya que volver a crearlos puede necesitar de mucho tiempo y costo, debido a que esta información es importante para la toma de decisiones diarias en la empresa Sin los datos al día, el funcionamiento se vería seriamente dañado Con la finalidad de evitar daños mayores por destrucción de la información, se realizan **backups** de la información vital para la empresa, y se contratarán los servicios de una empresa especializada en la custodia de archivos magnéticos

2.3 RELEVANCIA O INFIDENCIA

La revelación o infidencia es otra forma que utilizan los malos empleados para su propio beneficio La información, que es de carácter confidencial, es vendida a personas ajenas a la institución Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente

- **Control del uso de información en paquetes abiertos o cintas y otros datos residuales**

  Se deben formatear los discos o cintas que serán reutilizados a fin de que la información no sea conocida ni pueda ser utilizada por personas no autorizadas

- **Mantener datos sensitivos fuera del trayecto de la basura**

  Se deben eliminar los documentos que contengan información sensitiva de la empresa para que no sea mal utilizada por el personal que realiza el recojo de la basura Asimismo, para tener mayor seguridad en la protección de la información (cuando éstos sean descartados o eliminados) deben reducirse a destructores o picadores de papel

- **Preparar procedimientos de control para la distribución de información**

  Se debe mantener un control de la distribución de información múltiple a través de numeraciones de páginas o indicando su confidencialidad, con la finalidad de prevenir su difusión mal intencionada

2.4 MODIFICACIONES

Se deben tener en cuenta los siguientes puntos para la protección de la información ante una posible contingencia

1 Hacer de la copia de seguridad una política, no una opción

2 Se deben generar copias de seguridad de los archivos valiosos y almacenarlos en un lugar seguro, siendo dicha copia de seguridad obligatoria

3 Se debe contar con los equipos adecuados y disponibilidad de suministros para la ejecución de copias de seguridad

4 Los usuarios deben cumplir con la política de copias de seguridad (Política de Auditoria a las Copias de Seguridad)

Capítulo

3

AMENAZAS MÁS COMUNES CONTRA LA SEGURIDAD

Las amenazas más comunes contra la seguridad de datos de Serpost S A son las siguientes

3.1 Fuego

Una causa casi siempre relacionada con la electricidad son los incendios, y con ellos el humo, aunque la causa de un fuego puede ser un *desastre natural*, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio administrativo o en la parte operativa

Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos el humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos Quizás ante un incendio el daño provocado por el humo sea insignificante en comparación con el causado por el fuego y el calor, pero hemos de recordar que puede existir humo sin necesidad de que haya un fuego por ejemplo, en salas de operaciones donde se fuma No se debe permitir fumar bajo ninguna circunstancia

En muchos manuales de seguridad se insta a los usuarios, administradores o al personal en general a intentar controlar el fuego y salvar el equipamiento, esto tiene, como casi todo, sus puntos a favor y sus puntos en contra Evidentemente, algo lógico cuando estamos ante un incendio de pequeñas dimensiones es intentar utilizar un extintor para apagarlo, de forma que lo que podría haber sido una catástrofe sea un simple susto o un pequeño accidente Sin embargo, cuando las dimensiones de las llamas son considerables *lo último que debemos hacer* es intentar controlar el fuego nosotros mismos, arriesgando vidas para salvar *hardware* No importa el precio de nuestros equipos o el valor de nuestra información nunca serán tan importantes como una vida humana Lo más recomendable en estos casos es evacuar el lugar del incendio y dejar su control en manos de personal especializado

Temperaturas extremas

Todos comprendemos que las temperaturas extremas, ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos Es recomendable que los equipos operen entre 10 y 32 grados Celsius aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas

Para controlar la temperatura ambiente en el Centro de Cómputo, Serpost S A cuenta con dos acondicionadores de aire

Otra condición básica para el correcto funcionamiento de cualquier equipo, es que éste se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU

3.2 Fugas de agua

Los empleados que detecten agua en el piso del Centro de Cómputo o en un lugar donde haya equipos informáticos, *no deben pisar el agua* Si hay cajas eléctricas inundadas, el personal del Departamento de Tecnologías y Comunicaciones en coordinación con el área de Servicios Generales deben localizar y bajar el interruptor de energía eléctrica que controla la caja , en caso de que se detecte humedad en losas o muros, el personal no deberá tratar de *investigar* el problema El jefe de Departamento, el administrador del Centro de Cómputo o la persona designada deberán bajar todos los interruptores de energía eléctrica y realizarán la investigación respectiva para corregir el problema

3.3 Instalaciones eléctricas (caída y subida de tensión)

Por otro lado el personal no debe investigar o tratar de corregir cortos circuitos o chispas asociadas con los tableros eléctricos, contactos o equipos El personal del Departamento de Tecnología y Comunicaciones en coordinación con el área de Servicios Generales bajará los interruptores de suministro de energía eléctrica del área y realizarán la investigación respectiva para corregir el problema

3.4 Sabotaje Informático

El Sabotaje Informático se divide en dos partes

3 4 1 **Ataque Externo.** Referido a los ataques o intrusiones realizadas desde redes externas (Internet por ejemplo), trayendo consigo los Virus, Exploración de vulnerabilidades, escaneo de puertos, SPAM (Correo Electrónico, Site Web, entre otros), con la finalidad de poder hackear o crackear la red segura institucional, evitando así la publicación de información vital o volviendo lentos los procesos internos de la empresa

3 4 2 **Sabotaje o Ataque Interno.-** Se refiere a intentos de obtener información vital de la empresa, para sacar beneficio propio o destruir la información de la empresa, logrando así la pérdida de horas-hombre y pérdidas económicas Estos ataques pueden ser con conocimiento o no del usuario, como es en el caso de los virus, robo de información o modificación indebida

Problemas Generados por el Sabotaje Informático

- *Acceso no autorizado* Se deben analizar los riesgos que puede presentar una red frente a intentos de penetración externos o internos por parte de personas no autorizadas
- *Revelación de información* Se deben analizar los riesgos que puede presentar la red frente a la posibilidad de que personas ajenas a ella tengan acceso a información confidencial
- *Modificación de información* Se deben analizar los riesgos que puede presentar la red frente a la posibilidad de que personas internas o externas puedan modificar información crítica de la organización sin autorización
- *Intercepción de información* Se deben analizar los riesgos que puede presentar la red frente a la posibilidad de que personas internas o externas puedan interceptar datos transmitidos a través de intranets o a través de Internet, sin autorización
- *Ataques de negación del servicio (DoS - Denial of Service) y SPAM* Se deben analizar los riesgos que presenta una red frente a la posibilidad de que personas externas puedan hacer un sabotaje activo de la misma mediante técnicas de DoS (Denial of Service - Negación de Servicio), impidiendo así la prestación de los servicios en línea, así como la entrega de correo electrónico masivo no autorizados con información nociva a través de los servidores de correos institucionales (SPAM)

Políticas contra el Sabotaje Informático

Los siguientes puntos deben tenerse en cuenta como reglas a seguir a fin de evitar el sabotaje informático.

- La manipulación irregular, divulgación o uso indebido de la información de los recursos computacionales de una red deberían ser consideradas faltas graves, tal como se especifica en el Reglamento Interno de Trabajo (RIT)
- Ningún usuario debe poder monitorear el tráfico de la red o simular algún dispositivo de la red, esto debe ser también considerado una falta grave
- Identificar qué aplicación se adecua de mejor manera las exigencias de los usuarios navegadores, paquetes de oficina, utilitarios diversos, entre otros Esta tarea es responsabilidad del Área de Help Desk
- Deshabilitar las funciones y/o comandos no necesarios para la correcta ejecución de las aplicaciones Actualizar en forma periódica los parches y paquetes de servicio de las aplicaciones
- Las contraseñas de acceso a la red, deberían ser mayores a 09 caracteres, dando preferencia a las combinaciones alfanuméricas con símbolos
- En caso de tentativas de acceso incorrecto, las cuentas de acceso deberían ser bloqueadas y el acontecimiento debería ser reportado al administrador del recurso

Utilización de los Recursos

- El servicio de filtro de contenido se aplica a todos los usuarios que accedan a internet
- Para el servicio proxy a internet solo están autorizados las conexiones a puertos TCP 80 (http) y 443 (https), salvo requerimiento a FONAFE debidamente justificado
- La transmisión, distribución, reproducción o almacenamiento de cualquier tipo de información, data o material que viole cualquier ley aplicable o regulación al respecto, o que infrinja cualquier derecho de autor o propiedad intelectual se encuentra estrictamente prohibida
- El acceso de los usuarios a internet debe ser limitado, a fin que este no interfiera con el desarrollo y el desempeño normal de sus funciones laborales
- Los recursos de internet, deben usarse para labores propias del trabajo de cada empleado
- Se puede solicitar el acceso solamente a determinadas páginas de Internet, de acuerdo al trabajo que realice cada empleado
- El acceso a internet no es visitar sitios con contenido impropio como descargar música y/o películas, etc ; así mismo el servicio de filtro de contenido estarán habilitados por defecto para denegar el acceso a páginas que contengan temas de Pornografía, Terrorismo, Apuestas, Violaciones, Hacking, juegos, chat Por tal motivo su descarga y visualización serán bloqueados a nivel general Asimismo, se cuenta con equipo de seguridad perimetral que permite otorgar accesos a los usuarios a través de perfiles de acceso a Internet, los mismos que se muestran en el siguiente cuadro

Perfiles de Accesos a Internet

Grupo de usuarios	Accesos	Restricciones por Grupo	Restricción General
Usuarios Nivel 1	Accesos sites de gobierno (gob.pe)	Resto de contenidos	No acceso a contenido no productivo (chat, pornografía, terrorismo, apuestas, violencia, juegos, P2P)
Usuarios Nivel 2	Sites web autorizados	No redes sociales	
Usuarios Nivel 3	Streaming y redes sociales	No descarga de archivos	
Usuarios Nivel 4	Acceso completo (descarga de zip y exe)	N/A	

Política de Uso de Internet:

- El acceso a Internet incluye visitar WEB, sites, enviar y recibir correspondencia electrónica, transmitir y recibir archivos y obtener ("bajar") aplicaciones de Internet

Cuando acceda a Internet:

- Usar solamente servicios que se tenga acceso autorizado
- No ejecutar programas de verificación de seguridad, en sistemas o servidores de Internet, sin la aprobación explicita del propietario del sistema o servidor
- Siempre representarse como usted mismo-nunca como otra persona
- No colocar en Internet material pornográfico y tampoco acceder a este tipo de material

Cuando está usando notas electrónicas por Internet:

- No enviar notas de manera que parezca que fueran enviadas por otra persona
- No enviar anuncios no solicitadas vía email
- No hacer "forward" automático de notas internas de la organización, para un site Internet
- No enviar o responder cartas-cadenas, "cadenas" o similares

Internet No debe ser usada en los siguientes casos:

- Para engaño o lucro personal
- Para representarse como otra persona
- Para proveer la lista de empleados a terceros
- Para solicitudes comerciales que no sean para el negocio de su organización
- Cuando pueda interferir en el trabajo o en el de otros empleados
- Cuando pueda interferir en la operación de los

Tráfico de información

Cualquier archivo o software obtenido por descarga originada fuera de la red, debería ser sometido a verificación de virus antes de ser abierto o ejecutado, además el origen de los mismos debería ser una "fuente conocida"

Toda información obtenida vía Internet debería ser considerada sospechosa hasta ser confirmada por otra fuente de información diferente de aquella que la originó

Correo Electrónico

Uso Aceptable Los sistemas de correo electrónico en general deberían ser utilizados sólo para aspectos de interés de Serpost S A

Privilegios generales

Los privilegios en cuanto a la utilización del correo electrónico por los usuarios finales, debería ser restringido exceptuando aquellos que sean necesarios para llevar a cabo sus tareas Los usuarios finales del correo electrónico no deberían poseer privilegios para modificar el funcionamiento del mismo en cualquier aspecto

Individualización de los Usuarios

Todos los usuarios de correo electrónico tienen una única cuenta individual en el sistema, protegida por contraseña, siendo autenticados al momento de su acceso

Perfil	Descripción
0	Servicio RPC, OWA y buzón de correo de 8 GB
1	Servicio RPC, OWA y buzón de correo de 4 GB
2	Servicio OWA y buzón de correo de 2 GB
3	Buzón de correo de 1 GB

- Se mantendrá la configuración por defecto de las notificaciones por tamaño de buzón de Microsoft Exchange
- No se habilitaran lo protocolos POP3, NNTP
- Solo se realizara la copia de respaldo a la información de los usuarios que pertenezcan a los perfiles 1 y 2 La política de retención de backup para respaldar la información de los usuarios que pertenezcan a los perfiles 1 y2 será de 60 días
- Cuando SERPOST lo solicite, el proveedor del Servicio de Administración de CDC entregara en formato "pst" el buzón del usuario recuperado usando la herramienta de restauración que el proveedor utilice
- El servicio de filtro de correo no deseado (antispan) se aplica sin excepción a todas las cuentas de correo electrónico

Política de Uso de Correo Electrónico

- Las políticas de uso del correo electrónico deberá basarse obligatoriamente en las normas del estado, para este fin, específicamente la norma 005-2003-INEI/DTNP (Ver "Anexo 1· Normas para el uso del servicio de correo electrónico en las entidades de la Administración Publica Directiva N° 005-2003-INEI/DTNP")

3.5 Amenazas Telefónicas

Durante las operaciones normales del Centro de Cómputo, cualquier persona que conteste un teléfono, está sujeta a recibir amenazas telefónicas dirigidas contra las instalaciones o al personal del Centro de Cómputo El personal que reciba una amenaza por teléfono documentará dichas amenazas La persona que reciba la llamada hará lo siguiente

3 5 1 Tratar todas las amenazas como hechos reales
3 5 2 No elaborará supuestos acerca de los motivos del que hace la amenaza telefónica
3 5 3 Notificar únicamente al Jefe del Departamento de Tecnología y Comunicaciones, a la Sub Gerencia de Tecnologías de la Información o al Departamento de Seguridad en su defecto
3 5 4 No ocasionar pánico comentando la amenaza con otros empleados

El Jefe del Departamento de Tecnología y Comunicaciones, luego de una evaluación rápida de la amenaza (como, por ejemplo, una bomba) hará lo siguiente

- Coordinará las acciones pertinentes con Seguridad, de ser el caso el Departamento de Seguridad deberá avisar a la Policía, previa coordinación con la Gerencia de Administración y la Gerencia General

3.6 Pruebas de seguridad

Pruebas de penetración Hacer pruebas de penetración para verificar que el sistema de seguridad fue bien implementado y bien configurado

Simulación de ataque Simular todo tipo de ataques externos a la red, para verificar que los sistemas de seguridad proactivos son eficaces y que los sistemas de seguridad reactivos reaccionan de manera adecuada protegiendo la red.

Capítulo

4

MEDIDAS DE PRECAUCIÓN Y RECOMENDACIÓN

4.1 EN RELACIÓN AL CENTRO DE CÓMPUTO.

El acceso al Centro de Cómputo se encuentra restringido al personal autorizado del área El personal de la empresa debe encontrarse debidamente identificado con su fotocheck siempre en un lugar visible

Se cuenta con periodicidad de 30 días calendarios el cambio de password de ingreso a la red LAN la cual contiene una cadena mínima de 09 caracteres

Para que personal externo pueda acceder al centro de cómputo deberá contar con la autorización del Jefe del Departamento de Tecnología y Comunicaciones o del Subgerente de Tecnologías de la Información

Se recomienda por seguridad de los terminales, la anulación del acceso al USB, debiendo utilizarse los recursos de red cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos

Se encuentran restringido el uso de cámaras fotográficas al centro de datos de Serpost S A, sin permiso por escrito del Subgerente de Tecnologías de la Información

La responsabilidad de la protección de los equipos de cada área se encuentra a cargo de los responsables de cada Centro de Responsabilidad de la Empresa

4.2 MEDIOS DE ALMACENAMIENTO.

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

Cintas Magnéticas

- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango
  Temperatura 4°C a 32°C
  Humedad Relativa 20 % a 80 %
- El ambiente debe contar con aire acondicionado
- Las cintas deben colocarse en estantes o armarios adecuados
- Deberá mantenerse alejados de los campos magnéticos
- Se les debe dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas que se hayan registrado sobre ellas
- La custodia de las cintas se realiza a través de una empresa de servicios especializada

Recomendaciones para el mantenimiento de los Discos Duros.

Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores

El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio

Se debe evitar que la microcomputadora se coloque en zonas donde haya acumulación de calor Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras

No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco

4.3 RESPECTO A LOS MONITORES.

La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección

Generalmente éstos vienen en forma de una pantalla con un terminado áspero o algún tipo de capa contra brillo con una base de sílice, sobre la superficie de la pantalla del monitor

Se recomienda sentarse por lo menos a 60 cm (aproximadamente 2 pies) de la pantalla No sólo ésto reducirá su exposición a las emisiones (que se disipan a una razón proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual

También manténgase por lo menos a 1 m o 1 20 m (aproximadamente 3 ó 4 pies) del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante

Finalmente apague su monitor cuando no lo esté usando

4.4 RECOMENDACIÓN PARA EL CUIDADO DEL EQUIPO DE CÓMPUTO.

- **Teclado.** Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función
- **Cpu**. Mantener la parte posterior del cpu liberado en por lo menos 10cm Para asegurar así una ventilación mínima adecuada
- **Mouse** Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste
- **Scanner.** Mantener fuera del scanner grapas y clips pues, de introducirse dentro del equipo insertarse, puede causar daños irreparables en sus circuitos
- **Impresora** El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel
  En caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado

Mantener Las Áreas Operativas Limpias Y Pulcras

Se deben mantener las áreas operativas limpias y pulcras a fin de evitar los siguientes problemas el peligro de fuego generado por la acumulación de papeles bajo el falso piso, el daño potencial al equipo por derramar el café, leche o chocolate en los componentes del sistema, el peligro de fuego que se presentan por el excesivo almacenamiento de hojas continuas, el peligro por fumar y las falsas alarmas creadas por detectores de humo Estos son solamente algunos de los problemas encontrados en las áreas operativas con reglas poco estrictas de limpieza

Capítulo

5

SEGURIDAD EN REDES

5.1CONTROL DE ACCESO A LA RED

- Identificación para la red con clave de acceso
- Protección con clave de todas las áreas sensitivas de datos y restricción de acceso a los programas, según su uso
- Registro de toda la actividad de la estación de trabajo
- Protección con clave de acceso o bloqueo de todas las operaciones de copia a disquete en las estaciones de trabajo

5.2 PROTECCION DEL SERVIDOR

Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro

5.3 PROTEGIENDO LA RED

Estaciones de trabajo sin conectores USB. Una posible solución para poder impedir la copia de programas y datos fuera de la red en pendrive, y que a través de los pendrive ingresen virus y otros programas dañinos a la red, es dotar a los usuarios vulnerables con estaciones de trabajo sin conectores USB

5.4 TECNOLOGIA RAID,

La redundancia en el diseño de RAID significa que una parte de los datos almacenados se duplica para ayudar a detectar errores y corregirlos Este método de almacenamiento pone fin a los errores de lectura y escritura y ofrece una verdadera tolerancia a fallas
Además, los sistemas RAID pueden ofrecer a los usuarios de las redes, acceso a todos los datos, aunque un disco duro en el arreglo, falle catastróficamente

Anexo

1

CASOS DE EMERGENCIA PARA LOS EQUIPOS DE CÓMPUTO

1.1 De las Emergencia Físicas

CASO A: Error físico de disco de un Servidor (Sin RAID).

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

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

CASO B: ERROR DE MEMORIA RAM

En este caso se dan los siguientes síntomas

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios
- Ante procesos mayores se congela el proceso
- Arroja errores con mapas de direcciones hexadecimales
- Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se auto corregirá
- 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, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen

  6 Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas

7. Probar los sistemas que están en red en diferentes estaciones

8 Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios

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

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

1 Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área

2 El servidor debe estar apagado, dando un correcto apagado del sistema

3 Ubicar la posición de la tarjeta controladora

4 Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar

5 Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen

6 Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas

7 Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios

CASO D: CASO DE INCENDIO TOTAL

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

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

CASO E: CASO DE INUNDACION

- Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20cm de altura para la ubicación de los servidores De esta manera evitaremos inconvenientes como el referido
- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura
- Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión

- Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas

- Proveer cubiertas protectoras para cuando el equipo esté apagado

CASO F: CASO DE FALLAS DE FLUIDO ELECTRICO

Se puede presentar lo siguiente

- Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador

- Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia (*)), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación

- Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS).

* Llámese corriente de emergencia a la brindada por grupo electrógeno y/o UPS.

** Llámese corriente normal a la brindada por la compañía eléctrica

*** Se contará con transformadores de aislamiento (nivelan la corriente) asegurando que la corriente que entre y salga sea 220v, evitando que los equipos sufran corto circuito por elevación de voltaje (protegiendo de esta manera las tarjetas, pantallas y CPU del computador)

Anexo

2

DE LAS EMERGENCIAS LÓGICAS DE DATOS

CASO A: ERROR LÓGICO DE DATOS

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

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

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

PASO 1: Verificar el suministro de energía eléctrica En caso de estar conforme, proceder con el encendido del servidor de archivos, una vez mostrado el prompt de Dos, cargar el sistema operativo de red

PASO 2: Deshabilitar el ingreso de usuarios al sistema

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

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

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios

CASO B: CASO DE VIRUS

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

- Se procederá a realizar un backup de la información de la pc infectada por virus
- Se pasará el antivirus al backup para la eliminación de los virus
- Se procederá a formatear la pc infectada con virus
- Se ingresará la información del backup a la pc formateada para su reutilización

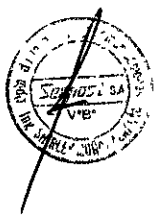
Anexo

3

PROCEDIMIENTOS ESPECÍFICOS

Es necesario tener permanentemente documentados los cambios y/o actualizaciones que se lleven a cabo en los servidores, a continuación se detallan procedimientos específicos para

- Procedimiento para crear, bloquear y eliminar de usuarios de dominios.
- Procedimiento para dar derechos y accesos a carpetas a usuarios
- Procedimiento para crear carpetas en servidor de archivo Linux
- Procedimiento para crear carpetas clientes empresariales



Procedimiento para crear, bloquear y eliminar usuarios del dominio Serpost

1 Se remitirá vía correo electrónico la creación de los usuarios al CDC
Se deberá definir en el correo electrónico el nombre del usuario, el nivel de acceso a internet, perfil del correo y el grupo de correo a la cual pertenecerá

Para acceso a Red , Internet y Correo

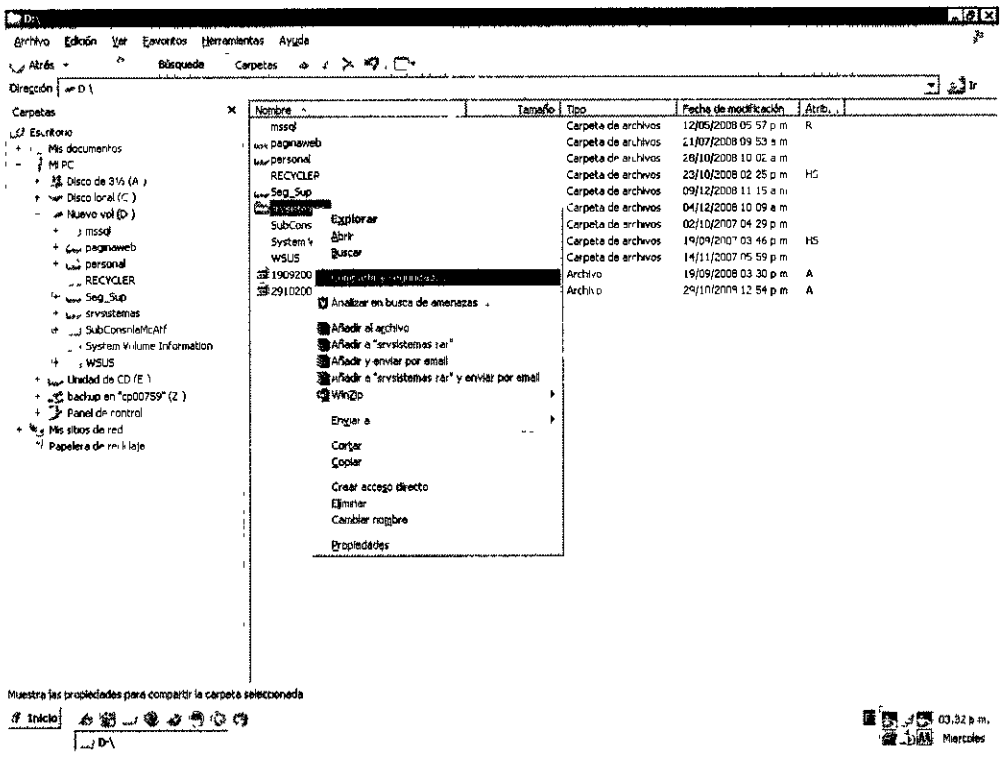
ÁREA: XXXXXXXXX
NOMBRE DE USUARIO: XXXXXXXX
Nivel de Acceso a Internet: XXXXXXXX

De ser el caso:
Perfil de correo. XXX
Grupo de correo: XXXXXXX

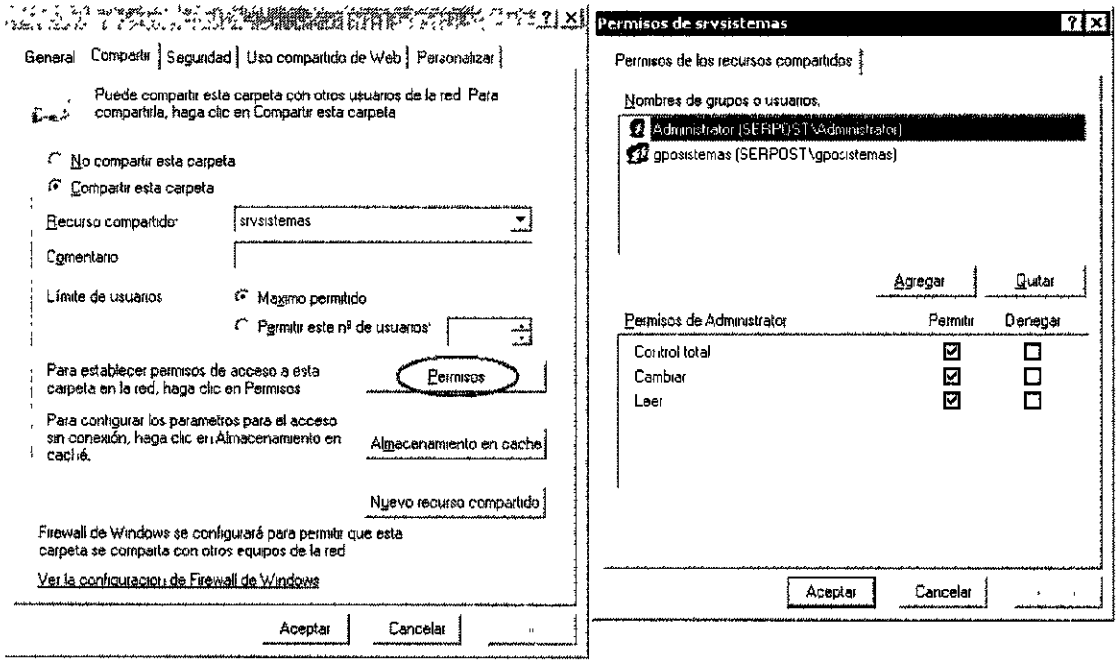
2 Para eliminar la cuenta de red, correo e internet de usuarios al dominio Serpost, se debe enviar la relación de usuarios y accesos a eliminar al CDC

Procedimiento para dar derechos a los servidores administrados por Serpost.

1 Click derecho sobre la carpeta a compartir, luego click en la opción "compartir y seguridad"



2 Luego seleccionar la opción "Compartir esta carpeta" y agregar a los usuarios que tendrán acceso a la carpeta y seleccionar el tipo de permiso a habilitar, una vez agregados hacer click en "OK"



Procedimiento para crear carpetas en servidor de archivo Linux.

Ingresar al servidor de archivos

cd /home/data
/home/data # ls (l)

cd gpostal/
mkdir dempresarial
chgrp –R gpodempresarial dempresarial
chmod 0770 dempresarial
ls
cd /etc/samba/
ls
vi smb conf

marcar y pegar con botón derecho

rcsmb restart

Escape q! Salir sin grabar
wq! Salir y grabar

gpodempresarial = el grupo que se creó en el Active Directory

Procedimiento para crear carpetas clientes empresariales

Servidor de archivos
Servidor de imagenes

Entrando al de archivos (Creando carpeta "Profuturo")

cd /home (Servidor de archivosl)
cd imagenes
mkdir profuturo
cp –r mlamolina/* profuturo/ (mlamolina = copiando estructura a profuturo)

l
chgrp –R gpodigitalizacion profuturo
l
chmod -R g+w profuturo
ls -R profuturo
cd /root/bin/Parametros
cd Clientes
mkdir profuturo
cp –r mlamolina/* profuturo/
l
cd
vi clientes txt/ (si no está creada, lo creo) wq!
cd
vi listado sh (solo para ver, se puede omitir)

ssh servidor de imagenes (Servidor de imagenes)
cd /home/
mkdir profuturo
cp –r mlamolina/* profuturo/
cd /root/bin/Parametros/Clientes/
mkdir profuturo
cp –r mlamolina/* profuturo/
cd /srv/www/clientes/
ls
mkdir –p profuturo/imagenes/peccpl/
ls –R profuturo
vi /etc/apache2/default-server conf (sombreo, bajo, click derecho)
rcapache2 reload

Procedimiento para habilitación accesos a usuarios

Se ingresa al Servidor AD
Se busca usuario de red
Se asigna permiso de acceso a Internet (de acuerdo a los perfiles definidos en el presente lineamiento)

Anexo

4

NORMAS DE OBLIGADO CUMPLIMIENTO POR PARTE DE LOS USUARIOS

- Cada usuario deberá cambiar su contraseña periódicamente
- Cada usuario deberá tener cuidado en no revelar y/o mostrar su contraseña.
- Cada usuario deberá cerrar la sesión o bloquear su estación de trabajo al momento de refrigerio
- Cada usuario deberá apagar el equipo al finalizar su jornada laboral, en caso otra persona continué utilizando la estación de trabajo, el usuario deberá cerrar la sesión de red
- Cada usuario deberá reportar al Departamento de Tecnologías y Comunicaciones las fallas y/o síntomas anómalos que presenten los equipos
- En la medida de lo posible los usuarios evitarán el uso de USB para reducir el riesgo de proliferación de virus
- Los usuarios que tengan acceso a Internet deberán acceder a sitios seguros y no descargarán contenido ni programas no autorizados, sin licencias o de procedencia no confiable

Anexo

5

MEDIO AMBIENTE EN LAS DIVERSAS CIUDADES DEL PAÍS

Debido a la diversidad climática de nuestro país, se incluye un cuadro con información pertinente que pueda ayudar a la hora de determinar un buen uso y mantenimiento de los equipos, así como la selección de nuevo equipamiento.

Ciudad	Lluvia	Calor	Helada	Granizada	Inundación	Sequía	Otros
Abancay	Nov-Abr	-	Jun-Jul	May-Jun	-	-	Vientos
Ayacucho	Oct-Mar	Ene-Dic	-	-	-	-	-
Cusco	Nov-Mar	-	May-Jun	May-Jun	-	-	Vientos
Huancayo	Nov-Abr	-	Ago-Jul	Ene-Mar	-	-	-
Huánuco	Oct-Mar	Jul-Ago	-	-	-	-	-
Juliaca	Dic- Mar	-	May-Jul	Oct-Nov	-	-	Vientos
Pucallpa	Nov-Abr	Todo el año	-	-	-	-	-
Puerto Maldonado	Oct-Nov	Todo el año	-	-	-	-	-
Puno	Ene-May	-	May-Jul	Ene-Mar	-	-	Nevada

Anexo

6

LIMA – Directorio Telefónico para Atenciones de Emergencia

Lista de Teléfonos para Atenciones de Emergencia

Emergencias Policiales

Policía Nacional del Perú	
Escuadrón de emergencia PNP	105
Dirección contra el Terrorismo (DIRCOTE)	482-8988
Dirección Nacional de Investigación Criminal (DIRINCRI)	431-5865
Unidad de Desactivación de Explosivos (UDE)	433-4461
	481-2901

Bomberos

Central de Emergencias	
Incendios /Rescates /Emergencias Médicas	222-0222
	116

Defensa Civil

Central de Defensa Civil	
Emergencias a Nivel Nacional	225-9898
	115

Lista de Anexos Importantes – Serpost S.A.

Seguridad	
Dpto de Tecnología y Comunicaciones	5085
Dpto. de Sistemas de Información	5027 /5333
Help Desk	5330
Circuito Cerrado	5555
Central Telefónica	5044
Recepción	9
	5045

Anexo

7

HERRAMIENTAS DE SEGURIDAD DE LA INFORMACIÓN[1]

Actividad en Internet

Air SmartGate
Cyber Snoop
Ianalyst
Internet Cleanup
Internet Manager
Internet Risk Management
NetFocus
System Activity Manager
Web Spy
WebTrends Firewall Suite
Etrust Firewall
ISA Server
WinGuardian

Análisis de Red

Abend-AID Fault Manager
Actiview Trouble Manager
AimIT
BindView
Centennial Discovery
Enterprise Security Manager
Event Log Monitor
Expert Observer
Kane Security Analyst
Link Analyst
NT Manage
NTRama
Sentinel Software Security
SPQuery
TripWire
WebTrends Netware Management
Ethereal

Panda Antivirus Platinum
PC-Cillin
Per Antivirus
Protector Plus
Quick HealRAV AntiVirus
Sophos
The Cleaner
Trojan Defense Suite
VirIT

Anti-espionaje

Ad-Search
Anticotillas Plus
FlashLock
Guideon
Hook Protect
Iprotect
PC Security Guard
Rainbow Diamond Intrusion Detector
Top Secret Office
Etrust Intruder Detection

Anti-Spam

Spam Buster
Spamkiller
SpammerSlammer

Anti-Virus y Troyanos

AntiViral Toolkit Pro
AVTrojan
AVX
BootProtect
Compucilina
ESafe Protect
Fobiasoft Guardian
F-Secure
The Hacker Antivirus
Inoculate
InVircible Antivirus
Iris Antivirus
Kaspersky Anti-Virus
MAMSoft
McAfee VirusScan
Norman Thunderbyte Virus Control
Norton Antivirus

Bloqueo y Restricción

Absolute Security
AceControl
Anfibia Soft Deskman
CDLock
ChildProof
Clasp2000
Deskman

[1] *En cursiva, las Herramientas recomendadas.*

ViruSafe Web

Arranque

Access Denied
Boot Sentry
BootLocker
MindSoft Custody
ScreenLock
SCUA Security
Sentry
ThunderGuard
Xlock

Auditoría

FileAudit
Log Monitor
SecurityCharge

Backup

@Backup
Adsm
ArcServe
AutoSave
Backup ATM Network
Backup Exec
Connected Online Backup
Data Recovery for Netware
DataKeeper
Discview
Drive Image
ImageCast
NetBackup
Norton Ghost
Novabackup
Open File Manager
Replica
Retrospect
SurvivelT
Ultrabac

Password Guardian
Password Keeper
Password Power
Password Tracker
Passwords
Planet Keeper
Private Bookmarks
PwlTools
Qwallet
Random Password Generator
Secret Surfer
Software Safe
v-GO Universal Password
VMVault

Control Remoto

AMI Server Manager
ControlIT
Desktop Locker 1 0
DesktopShield
DeviceLock Me
GS98 Access Control
ISS Complock
Lock n Safe
MausTrap
MicroManager
MindSoft GuardianShip
MindSoft Restrictor
PC Lock
PC Restrictor
Poledit
RedHand Pro
SecureIT Pro
SecurityWizard
Smart98
StormWindow
System Security
TrueFace
Windows Security Officer
WinFile Vault
WinLock

Contraseñas

007 Password Recovery
Aadun
Absolute Security
Advanced Password Generator
Asterisco
Claves
ePassword Keeper
EXE Protector
Guardian
Info Keep
LockDown
CrackZip
Locker
MasterPass
Office Password
Open Pass
PassGo
PassGuard
Password Corral
Password Generator
WebTrends Security Analyzer

Encriptación de Comunicaciones

Bbcom VPN
F-Secure VPN
Go Secure
GuardianPRO VPN
Intel VPN
KryptoGuard LAN and VPN
PGP
Power VPN
SafeGuard VPN
SideWinder
SmartGate
SonicWall Pro
VPN 1 Internet Gateway
VPNWare System

CoSession
Kane Security Monitor
LapLink
NetOp
NetSupport Manager
DameWare
PCAnywhere
Proxy
ReachOut Enterprise
Remote Administrator
ServerTrak
Timbuktu Pro
TrendTrak

Cookies

Cache & Cookie Washer
Cookie Crusher
Cookie Pal
CyberClean
The Watchman
Window Washer

Detectores de Agujeros de Seguridad

Check Point RealSecure
Hackershield
Intruder Alert
LanGuard network Scanner
Lucent RealSecure
NetProwler
NetRecon
PassMan Plus
SecureNet Pro Software
Krypton Encoding System
MindSoft Shelter
Neocrypt
Norton Secret Stuff
NovaLock
Passworx
PCSafe
PGP
Quick Crypt
RSA Bsafe
SafeGuard LanCrypt
SafeSuite Realsecure
SECRETsweeper
SECURE
Secure Shuttle Transport
Security BOX
SecutityManager
Shyfile
SpartaCom Cryptogram
TEACrypt
Text Watchdog
The DESX Utility
ThunderCrypt
Unbreakable Encryption
WINZAP
Xcrypto

Espionaje

2Spy!

Encriptación de Software

ABI-CODER
Absolute Security
AutoEncrypt
BestCrypt
CodedDRAG
Combo
Cryptext
Cryptit
CryptoIdentify
Cryptoman
PGP File
PGP Mail
Data Safe
DataCloak
Easy Code
EasyCrypto
Emerald Encryption
Encrypt IT!
Encrypted Magic Folders
Enigma
Enigma 98
File Protector
FileCrypto
FileDisk Protector
FlyCrypt
Folder Guard
Hideit! Pro
HotCrypt
InfoSafe
Interscope BlackBox
Invisible Secrets
Jumblezilla
Kremlin
Stealth Logger
SupervisionCam
System Spy
Watcher
WinGuardian

Filtros de Internet

CommandView
Cyber Attack defense System
Cyber Sentinel
Digital ID
e-Sweeper
Go Secure!
Mail-Gear
MailSweeper
MailVault
Message Inspector
Predator Guard
Private-I
Real Secure
Shields UP!
SigabaSecure
SmartFilter
WEBsweeper
World Secure Mail

Firewall

Activity Monitor
Alot Monica
AppsTraka
ASCII Spy
AY Spy
Boss Everyware
Canary
Date Edit
Desktop Surveillance
El Espía
EventControl
IntraSpy
Key Logger
Keyboard Monitor
KeyKey
MyGuardian
Omniquad Detective
Password Revealer
PC Spy
RemoteView
Snooper
Spector
SpyAnywhere
Stealth Activity
Stealth Keyboard Interceptor

Gestión de Accesos

Absolute Protect
Access Manager Secondary Radius
Azza Air Bus
Border Protector
C2000
Cnet/2
Defender
E-Z Lock
GuardianPro Authentication
Hands Off Personal
Identity Protector
IKey
Lock Protector
Navis Access
Navis Radius Access Control
Palladium Secure Remote Access
Panda Security
Personal Protector
PrivateEXE
RSA SecurID
SafeGuard Easy
SafeWord Plus
SmartGuard
SmartLock
Steel-Belted RADIUS
UserLock
VicinID
WinFuel

Mantenimiento

Diskeeper
More Space
Partition Commander
Partition Magic
Security Setup
System Commander
Windows Commander

Altavista Firewall
BlackIce
CheckPoint
CyberArmor
Elron Firewall
FireProof Firewall KIT System
GuardianPRO Firewall
GuardIT
HackTracer
MindSoft Firewall
NeoWatch
Netmax Firewall
Norton Personal Firewall
Raptor Firewall
Secure Connect Firewall
SmartWall
Sygate Personal Firewall
Tiny Personal Firewall
Watchguard Livesecurity SYS
WinRoute Pro
ZoneAlarm Pro

Recuperación de Datos

ConfigSafe Desktop
CoreSave
Easy Recovery
Easy Restore
Esupport
File Recovery
GoBack
Instant Recovery
Lost & Found
PictureTaker Personal Edition
SecondChance
Shredder
System Snapshot
Undelete
Unerase

Seguridad en Comercio Electrónico

Comerse Protector
CryptoSwift
Etrust
NetSecure
RSA Keon
SAFEsuite Decisions
Safety Net

Suites de Seguridad Informática

ESafe Desktop
F-Secure Workstation Suite
McAfee Office 2000 Pro
NetMax Professional Suite
Norton Internet Security 2000
Observer Suite
Ontrack SystemSuite 2000
Secur-All

Ocultación

BlackBoard FileWipe
Boss
Camouflage
Don't Panic!
Hidden 7
Invisible Files
Sentry98
WebPassword
WinShred
WipeClean