PLAN DE CONTINGENCIA INFORMÁTICO

SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO S.A.S

SETP TRANSFEDERAL S.A.S

Neiva, Diciembre de 2018

FORMATO PRELIMINAR AL DOCUMENTO

Título:	**PLAN DE CONTINGENCIA INFORMÁTICO SETP TRANSFEDERAL S.A.S.**		
Fecha elaboración aaaa-mm-dd	2016-06-10		
Palabras Claves:	Plan de Contingencia Informático, SETP, tecnología, GTIC, información, seguridad		
Formato:	DOC	Lenguaje:	Español
Dependencia:	Sistema Estratégico de Transporte Público - SETP TRANSFEDERAL S.A.S.: Área Administrativa y Financiera – Desarrollos Tecnológicos		
Proyectó:	Andrés Felipe Gómez Escobar Ingeniero Contratista SETP Transfederal S.A.S.	Firmas	
Responsable de ejecución:	Andrés Felipe Gómez Escobar Ingeniero Contratista SETP Transfederal S.A.S.		
Aprobó:	Hernando Josué Benavides Vanegas Gerente SETP Transfederal S.A.S.		

CONTROL DE CAMBIOS

VERSIÓN	FECHA	No. SOLICITUD	RESPONSABLE	DESCRIPCIÓN
1.0	2016-06-10	No aplica	SETP TRANSFEDERAL S.A.S.	Creación del documento
2.0	2017-12-15	No aplica	SETP TRANSFEDERAL S.A.S.	Modificación Situación Actual
3.0	2018-12-14	No aplica	SETP TRANSFEDERAL S.A.S.	Modificación Situación Actual

PRESENTACIÓN

Uno de los activos más importantes de toda institución es la información que esta genera en sus diferentes acciones y ámbitos. Conscientes de esta premisa, podemos indicar que se debe adoptar medidas de seguridad para la información y así mismo estar preparados para poder afrontar contingencias y desastres de tipo diverso.

La Gerencia de Tecnología de la Información y de las Comunicaciones (GTIC), tiene, entre otros, el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. Con base a ello se presenta el Plan de Contingencia Informático del SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO DE NEIVA S.A.S – SETP TRANSFEDERAL S.A.S.

En la actualidad, los profesionales de la informática tienen como una de sus principales actividades y preocupaciones la seguridad de estos sistemas, que constituyen una base y respaldo a las funciones institucionales realizadas a través de los años. De igual manera, facilitan las tareas que se desarrollan en la ejecución de los diferentes procesos administrativos, logísticos, ejecutivos, informativos, sociales de planeamiento y de servicios.

GENERALIDADES

A. OBJETIVO

Formular un adecuado Plan de Contingencias, que permita la continuidad en los procedimientos informáticos de la GTIC, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la GTIC.

SITUACIÓN ACTUAL

A. DIAGNOSTICO

1. EQUIPOS DE COMPUTO

EQUIPO	MARCA	SERIAL CPU	PROCESADOR	RA	STORAGE	S.O.
Desktop	Acer Verinton X6630G	DTVGNAL003427027539600	Core i7 ™ 4770 CPU 3,40 GHz	8 GB	1 TB	Windows 7 Profesional 64 Bits
Desktop	Acer Verinton X6630G	DTVGNAL003427027519600	Core i7 ™ 4770 CPU 3,40 GHz	8 GB	1 TB	Windows 7 Profesional 64 Bits
Desktop	Acer Verinton X6630G	DTVGNAL003427027489600	Core i7 ™ 4770 CPU 3,40 GHz	8 GB	1 TB	Windows 7 Profesional 64 Bits
Desktop	Acer Verinton X6630G	DTVGNAL003427027449600	Core i7 ™ 4770 CPU 3,40 GHz	8 GB	1 TB	Windows 7 Profesional 64 Bits
Desktop	Acer Verinton X6630G	DTVGNAL003427027579600	Core i7 ™ 4770 CPU 3,40 GHz	8 GB	1 TB	Windows 7 Profesional 64 Bits
Desktop	HP PRODesk 600 G1 SFF	MXL4030XJ0	Core i7 ™ 4770 CPU 3,40 GHz	8 GB	1 TB (2 de 500GB)	Windows 7 Profesional
Desktop	HP PRODesk 600 G1 SFF	MXL4030XH3	Core i7 ™ 4770 CPU 3,40 GHz	8 GB	500 GB	Windows 7 Profesional
Portatil	Asus N551J	ECN0CJ045011506	Core 7	12 GB	1 TB	
Portatil	Asus S301L	E9NOCX557882397	Core i5 ™ 4210U CPU 1,70 GHz 2.40 GHz	6 GB	1 TB	Windows 8.1 Single Language 64 Bits
Portatil	Asus S301L	E9NOCX557897396	Core i5 ™ 4210U CPU 1,70 GHz 2.40 GHz	6 GB	1 TB	Windows 10 Home Single Language 64 Bits
Portatil	Asus S301L	E9NOCX557944394	Core i5 ™ 4210U CPU 1,70 GHz 2.40 GHz	6 GB	1 TB	Windows 8.1 Single Language 64 Bits
Portatil	Asus S301L	E9NOCX558026395	Core i5 ™ 4210U CPU 1,70 GHz 2.40 GHz	6 GB	1 TB	Windows 8.1 Single Language 64 Bits
Portatil	Asus S301L	E9NOCX558042396	Core i5 ™ 4210U CPU 1,70 GHz 2.40 GHz	6 GB	1 TB	Windows 8.1 Single Language 64 Bits
Portatil	Asus S301L	E9NOCX558047396	Core i5 ™ 4210U CPU 1,70 GHz 2.40 GHz	6 GB	1 TB	Windows 8.1 Single Language 64 Bits
Todo en uno	HP 20-R104LA	MXX5360GFL	Core i3 ™ 4160 CPU 3,10 GHz	4 GB	1 TB	Windows 10 Home Single Language 64 Bits
Todo en uno	HP Compaq Pro 4300	MXL4070JTR	Core i3 ™ 3240 CPU 3,40 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP Compaq Pro 4300	MXL4070J6R	Core i3 ™ 3240 CPU 3,40 GHz	4 GB	500 GB	Windows 10 Pro
Todo en uno	HP ProOne 400 G1 AiO	MXL4210C2T	Core i3 ™ 4130 CPU 2,90 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP ProOne 400 G1 AiO	MXL4252C3K	Core i3 ™ 4130 CPU 2,90 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP ProOne 400 G1 AiO	MXL4252C3G	Core i3 ™ 4130 CPU 2,90 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP ProOne 400 G1 AiO	MXL4210BXK	Core i3 ™ 4130 CPU 2,90 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP ProOne 400 G1 AiO	MXL4210C2W	Core i3 ™ 4130 CPU 2,90 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP ProOne 400 G1 AiO	MXL4210BWX	Core i3 ™ 4130 CPU 2,90 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP ProOne 400 G1 AiO	MXL4210BWZ	Core i3 ™ 4130 CPU 2,90 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP ProOne 400 G1 AiO	MXL4210BX6	Core i3 ™ 3240 CPU 3,40 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP ProOne 400 G1 AiO	MXL4210BXS	Core i3 ™ 4130 CPU 2,90 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits
Todo en uno	HP ProOne 400 G1 AiO	MXL4210BXG	Core i3 ™ 4130 CPU 2,90 GHz	4 GB	500 GB	Windows 7 Profesional 64 Bits

2. LICENCIAS ASIGNADAS

Nro.	LICENCIA	VER.	CANT.	COMPUTADOR	AREA
1	Office Home and Business 32/64 Bits - Caja	2013	1	SIN INVENTARIO	Social
2	Office Home and Business 32/64 Bits - Caja	2013	1	SIN INVENTARIO	Infraestructura
3	Office Home and Business 32/64 Bits - Caja	2013	1	SIN INVENTARIO	Infraestructura
4	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #055	Contratación
5	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #111	Infraestructura
6	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #034	Administrativa y Financiera
7	Office Home and Business 32/64 Bits - Caja	2013	1	SIN INVENTARIO	Administrativa y Financiera
8	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #132	Contratación
9	Office PRO 32/64 Bits - Caja	2013	1	INVENTARIO #043	Administrativa y Financiera
10	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #062	Administrativa y Financiera
11	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #095	Infraestructura
12	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #051	Administrativa y Financiera
13	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #072	Recepción
14	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #066	Infraestructura
15	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #048	Contratación
16	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #143	Contratación
17	Office Home and Business 32/64 Bits - Caja	2013	1	SIN INVENTARIO	Gerencia
18	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #121	Infraestructura
19	Office Home and Business 32/64 Bits - Caja	2013	1	INVENTARIO #119	Predial
20	Office Home and Business 32/64 Bits - Caja	2013	1	LICENCIA PERDIDA	Infraestructura

3. IMPRESORAS

Nro.	MARCA	SERIAL	IP	HOTSNAME	MAC	AREA
1	HP LASERJET PRO 400 MFP M425d	CND8FBT96F	192.168.3.22	NPI18196D	9c:b6:54:18:19:6d	RECEPCIÓN
2	HP LASERJET PRO 400 MFP M425dn	CNF8G813VQ	192.168.3.99	NPI3D0935	14:58:d0:3d:09:35	SOCIAL
3	HP LASERJET PRO 400 MFP M425dn	CNF8G813Z0	192.168.3.109	NPI3CABCE	14:58:d0:3c:ab:ce	FINANCIERA
4	HP LASERJET PRO 400 MFP M425dn	CNF8G813XK	192.168.3.13	NPI3D0932	14:58:d0:3d:09:32	CONTRATACION
5	HP LASERJET PRO 400 MFP M425dn	CNF8G813M2	192.168.3.12	NPI3CBBA1	14:58:d0:3c:bb:a1	INFRAESTRUCTURA

4. RECURSOS TECNOLÓGICOS ADQUIRIDOS AÑO 2017

Tipo De Equipo	Tipo De Impresora	Software	Características	Cantidad	Número Del Contrato	Fecha Del Contrato
OTROS	OTRA	Actualización software contable y financiero	OTRO	1	49	2/03/2017
OTROS	OTRA	Hosting sitio web	OTRO	1	67	13/06/2017
OTROS	OTRA	Microsoft Office 2016 Profesional Pro	PROGRAMAS OFIMÁTICA	4	85	22/08/2017
OTROS	OTRA	Tarjeta de red inalámbrica	OTRO	2	85	22/08/2017
OTROS	OTRA	CAL Windows Server 2012 R2	CAL Windows Server	50	85	22/08/2017
OTROS	OTRA	Firewall Appliance	OTRO	1	85	22/08/2017
PC ESCRITORIO	OTRA	Computador de escritorio todo en uno Lenovo	OTRO	4	85	22/08/2017
OTROS	OTRA	Disco duro externo USB	OTRO	2	85	22/08/2017
OTROS	OTRA	Batería drone Phantom 3 Pro	OTRO	1	85	22/08/2017
OTROS	OTRA	Endpoint Security	Antivirus	35	85	22/08/2017
OTROS	OTRA	Unidad externa DVD USB	OTRO	1	85	22/08/2017
OTROS	OTRA	UPS ONLINE RACK 6KVA FACTOR DE POTENCIA 0.8	OTRO	1	85	22/08/2017

5. RECURSOS TECNOLÓGICOS ADQUIRIDOS AÑO 2018

Tipo De Equipo	Software	Características	Cantidad	Número Del Contrato	Fecha Del Contrato
OTROS	Actualización software contable y financiero	OTRO	1	70	26/01/2018
OTROS	Hosting sitio web	OTRO	1	78	2/04/2018
OTROS	Autodesk AutoCAD LT 2018	Autodesk AutoCAD	6	89	7/07/2018

FASE DE REDUCCION DE RIESGOS

A. ANÁLISIS DE RIESGOS

Establecer los riesgos a los cuales está propensa la GTIC. De igual manera determinar el nivel o factor de riesgo, que lo clasificaremos en los siguientes:

Factor de Riesgo:

- Bajo
- Muy Bajo
- Alto
- Muy alto
- Medio

Ellos nos determinan nuestra tabla de riesgos y nivel de factores que a continuación detallamos:

RIESGO	Factor de Riesgo				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Incendio		X			
Inundación		X			
Robo Común		X			
Vandalismo, daño de equipos y archivos		X			
Fallas en los equipos, daño de archivos					X
Equivocaciones, daño de archivos			X		
Virus, daño de equipos y archivo					X
Terremotos, daño de equipos y archivos		X			
Acceso no autorizado, filtración de información					X
Robo de datos					X
Fraude, alteración de información				X	
Desastre Total		X			

Con base a la tabla anteriormente presentada, concluimos que nuestro análisis de riesgo a modo general, nos hace ver que las posibles contingencias que pudieran presentarse en su mayoría van de un factor de ocurrencia bajo y muy alto.

A continuación realizamos un desglose de las causas por las cuales mayormente se presentan este tipo de contingencias, para ello realizamos la siguiente lista de preguntas:

1. Con respecto al ***fuego***, que puede destruir los equipos y los archivos

- ¿La Entidad cuenta con protección contra incendios?
- ¿Se cuenta con sistemas de aspersión automática?
- ¿Cuenta con diversos extintores?
- ¿Detectores de humo?
- ¿Los empleados están preparados para enfrentar un posible incendio?

2. Con respecto al ***robo común***, llevándose los equipos y archivos

- ¿En qué tipo de comuna se encuentra la Entidad?
- ¿Los equipos de cómputo se ven desde la calle?
- ¿Hay personal de seguridad en la Entidad?
- ¿Cuántos vigilantes hay?
- ¿Los vigilantes, están ubicados en zonas estratégicas?
- ¿Existe un sistema de seguridad para prevenir el ingreso de personas no autorizadas?

3. Con respecto al ***vandalismo***, que dañen los equipos y archivos

- ¿Existe la posibilidad que un ladrón cause daños?
- ¿Hay la probabilidad que causen algún otro tipo de daño intencionado?

4. Con respecto a ***fallas en los equipos***, que dañen los archivos

- ¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?
- ¿Cuáles son las condiciones actuales del hardware?
- ¿Es posible predecir las fallas a que están expuestos los equipos?

5. A ***equivocaciones*** que dañen los archivos

- ¿Cuánto saben los empleados de computadoras o redes?
- Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?
- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

6. Con respecto a la acción de ***virus***, que dañen los archivos

- ¿Se prueba software en la oficina sin hacerle un examen previo?
- ¿Está permitido el uso de USB sin escanear en la oficina?
- ¿Se cuentan con procedimientos contra los virus?

7. Con respecto a ***terremotos***, que destruyen los equipos y archivos

- ¿La Entidad se encuentra en una zona sísmica?
- ¿El edificio cumple con las normas antisísmicas?
- Un terremoto, ¿cuánto daño podría causar?

8. Con respecto a ***accesos no autorizados***, filtrándose datos importantes

- ¿Existe registro de personal autorizado en la Entidad?
- ¿Qué probabilidad hay que un colaborador intente hacer un acceso no autorizado?
- ¿Existe comunicación remota de la red? ¿Qué tipo de servicio se utiliza (Telnet, FTP, etc)?
- ¿Contamos con Sistemas de Seguridad en el Correo Electrónico o Internet?

9. Con respecto al ***robo de datos***; y la posible difusión de estos.

- ¿Cuánto valor tienen actualmente las Bases de Datos?
- ¿Cuánta pérdida podría causar en caso de que se hicieran públicas?
- ¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?

10. Con respecto al ***fraude***, vía computadora.

- ¿Cuántas personas se ocupan de la contabilidad de la Entidad?
- ¿Los sistemas son confiables? ¿Pueden copiar datos en archivos?
- Las personas que trabajan en las diferentes áreas, ¿qué tipo de antecedentes laborales tienen?
- ¿Existe acceso a los sistemas desde otros sistemas externos o por personas no autorizadas?

B. PLAN DE RECUPERACIÓN DE DESASTRES

Ahora definimos las acciones a tomar para recuperarnos de la ocurrencia de un desastre. Este Plan de Recuperación contiene 3 etapas:

1 ACTIVIDADES PREVIAS AL DESASTRE

Como actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de información que nos asegure un proceso de recuperación con el menor costo posible a nuestra entidad, tenemos que señalar las siguientes acciones que son precisas de realizar en la ejecución del presente plan.

a. Definición y Establecimiento de un Plan de Acción

Establecer los procedimientos relativos a:

(1). Sistemas de Información.- La GTIC tendrá una relación de los Sistemas de Información con los que cuenta, debiendo identificar toda información sistematizada o manual, que sea necesaria para la buena marcha Institucional.

La relación de *Sistemas de Información* detallará los siguientes datos:

- ***Nombre del Sistema***, es determinado por el analista-desarrollador asignado por la GTIC.

- ***Lenguaje o Paquete*** con el que fue creado el Sistema, programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
- ***La Dirección,*** (Gerencia, Subgerencia, área, etc) que genera la información base (el <<dueño>> del sistema).
- Las ***unidades o departamentos*** (internos/ externos) que usan la información del Sistema.
- El ***volumen de los archivos*** que trabaja el Sistema.
- El ***volumen de transacciones*** diarias, semanales y mensuales que maneja el sistema.
- El ***equipamiento necesario*** para un manejo óptimo del Sistema.
- La(s) ***fecha***(s) en las que la información es necesitada con carácter de urgencia.
- El ***nivel de importancia*** estratégica que tiene la información de este Sistema para la Entidad (medido en horas o días que la Entidad puede funcionar adecuadamente, sin disponer de la información del Sistema). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
- ***Actividades*** a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Con toda esta información se realizará una lista priorizada (Ranking) de los Sistemas de Información necesarios para que el SETP TRANSFEDERAL S.A.S. recupere su operatividad perdida en el desastre (Contingencia).

(2). Equipos de Cómputo: Se tendrá en cuenta lo siguiente:

- ***Inventario actualizado*** de los equipos de manejo de información (computadoras, lectoras de microfichas, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso institucional.

- ***Pólizas de Seguros Comerciales***. Como parte de la protección de los activos institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del computador siniestrado se hará por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.

- ***Señalización*** o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC's con información importante o estratégica y color verde a las PC's de contenidos normales.

- **Respaldo de PC´s**, tener siempre una relación actualizada de PC´s requeridos como mínimo para cada sistema permanente de la Entidad (que por sus funciones constituye el eje central de los servicios informáticos), para cubrir las funciones básicas y prioritarias de cada uno de estos sistemas cuando se requiera.

(3) Obtención y Almacenamiento de los Respaldos de Información (BACKUPS): Establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas o aplicativos de el SETP TRANSFEDERAL S.A.S., contando con:

- ***Backups del Sistema Operativo.*** En caso de tener varios sistemas operativos o versiones se contará con una copia de cada uno de ellos.

- ***Backups del Software Base.*** Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales.
- ***Backups del Software Aplicativo.*** Considerando tanto los programas fuentes como los programas objeto correspondiente, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final. Considerando las copias de los listados fuentes de los programas definitivos, para casos de problemas.
- ***Backups de los Datos.*** Base de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del software aplicativo
- ***Backups del Hardware***. Implementar mediante dos modalidades:

  - ***Modalidad Externa***. Mediante convenio con otra Entidad que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.
  - ***Modalidad Interna***. Teniendo dos locales, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

En ambos casos se probará y asegurará que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

(4). Políticas (Normas y Procedimientos de Backups): Establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente en el punto 3). Incluyéndose:

- Periodicidad de cada tipo de Backups.
- Respaldo de Información de movimiento entre los períodos que no se cuenta con Backups (backups incrementales).
- Uso obligatorio de un formulario estándar para el registro y control de backups.
- Correspondencia entre la relación de sistemas e informaciones necesarias para la buena marcha de la institución (mencionado en el punto a) y los backups efectuados.
- Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

b. Formación de Equipos Operativos para el Plan de Acción

Todas las áreas u oficinas del SETP TRANSFEDERAL S.A.S., que almacenen Información y que sirva para la operatividad institucional, designará un responsable de la seguridad de dicha

información. Pudiendo ser el jefe del área o el colaborador que maneje directamente la información.

Entre las acciones a tomar por la GTIC conjuntamente con las oficinas serán:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc, para los principales sistemas, subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones y la creación de los respaldos incrementales.
- Establecer procedimiento de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- Realizar procedimientos de control de inventario y seguridad de almacenamiento en el local alternante.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas y simulacros de desastres.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.

2. ACTIVIDADES DURANTE EL DESASTRE

Una vez presentada la contingencia, se ejecutará las siguientes actividades:

a. Plan de Emergencia

Establecer las acciones que se deben realizar cuando se presente un siniestro, así como la difusión de las mismas.

Conviene prever los posibles escenarios de ocurrencia del Siniestro:

- Durante el día.
- Durante la Noche o madrugada.

Este plan incluirá la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre la contingencia.

Si bien es cierto la integridad de las personas es lo primordial, se deben adoptar medidas con el fin de asegurar la información detallando:

- Vías de salida o escape.
- Plan de Evacuación de Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de información) del SETP TRANSFEDERAL S.A.S. (si las circunstancias del siniestro lo posibilitan).
- Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas) y lista de teléfonos de bomberos/ ambulancias.

En caso de contingencias como fallas en equipos de cómputo, fallas humanas, acción de virus, etc.; solicitar la ayuda de una persona capacitada para resolver el problema.

b. Formación de Equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro.

c. Entrenamientos

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se le hayan asignado en los planes de evacuación de personal o equipos para minimizar costos, se puede aprovechar las fechas de recarga de extinguidores o las charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de los siniestros (incendios, inundaciones, terremotos y/o apagones, etc.) pueden realmente ocurrir y tomar con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los gerentes y líderes de áreas del SETP TRANSFEDERAL S.A.S., dando el ejemplo de la importancia que la Gerencia otorga a la Seguridad Institucional.

3. ACTIVIDADES DESPUÉS DEL DESASTRE

Durante la contingencia, se tomará en cuenta lo planificado en el plan de Emergencia.

a. Evaluación de Daños.

Inmediatamente después que la contingencia ha concluido, se evaluará la magnitud de los daños producidos, estableciendo que sistemas están afectados, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se lanzará un pre-aviso a la entidad con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha institución.

b. Priorización de actividades del Plan de Acción

Toda vez que el Plan de acción contemple una pérdida total, la evaluación de daños reales y su comparación con el Plan, nos dará la lista de actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra institución.

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

c. Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción.

Cada uno de estos equipos contará con un coordinador que reportará diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, informará de inmediato a la jefatura a cargo del Plan de Contingencias.

Los colaboradores de recuperación tendrán dos etapas:

- **La primera**, la restauración de los servicios usando los recursos del SETP TRANSFEDERAL S.A.S. o local de respaldo.
- **La segunda**, es volver a contar con los recursos en las cantidades y lugares propios de los sistemas de información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro sistema e imagen institucional, como para no perjudicar la operatividad del SETP TRANSFEDERAL S.A.S. o local de respaldo.

d. Evaluación de Resultados.

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

De la evaluación de resultados y del siniestro, saldrán dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

e. Retroalimentación del Plan de Acción.

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

ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN

A. CONCEPTOS GENERALES

1. Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidas o transmitidas a otros.

2. Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

3. Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

4. Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

5. Base de Datos

Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

6. Acceso

Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

7. Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

8. Ataque Activo

Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una

computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

9. Ataque Pasivo

Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

10. Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

11. Incidente

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

B. SEGURIDAD INTEGRAL DE LA INFORMACIÓN

La Seguridad es un aspecto de mucha importancia en la correcta Administración Informática.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren.

En la seguridad de la información, deben tenerse en cuenta estas medidas para evitar la pérdida o modificación de los datos, información o software, por personas no autorizadas, para lo cual se deben tomar en cuenta una serie de medidas, entre las cuales figurarán el asignar números de identificación y contraseñas a los usuarios.

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 los colaboradores, de ahí que resulte obvio el interés creciente que día a día se evidencia sobre este aspecto de la nueva sociedad informática.

La seguridad de la información tiene dos aspectos importantes como:

- Negar el acceso a los datos a aquellas personas que no tengan derecho a ellos.

- Garantizar el ingreso 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.

AMENAZAS MÁS COMUNES CONTRA LA SEGURIDAD

A. INSTALACIONES ELÉCTRICAS

Para que funcionen adecuadamente, las computadoras personales necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible.

Las computadoras personales toman la electricidad de los circuitos eléctricos domésticos normales, a los que se llama tomas de corriente. Esta corriente es bastante fuerte, siendo una **corriente alterna** (ac), ya que alterna el positivo con el negativo. La mayor parte de las computadoras personales incluyen un elemento denominado **fuente de alimentación**, la cual recibe corriente alterna de las tomas de corriente y la convierte o transforma en la corriente continua de baja potencia que utilizan los componentes de la computadora.

La fuente de alimentación es un componente vital de cualquier computadora personal, y es la que ha de soportar la mayor parte de las anomalías del suministro eléctrico. Actualmente existe el concepto de fuente de alimentación redundante, la cual entrará en operación si se detecta una falla en la fuente de alimentación principal.

En nuestro medio se han podido identificar siete problemas de energía más frecuente:

1. Fallas de energía.
2. Transistores y pulsos.
3. Bajo voltaje.
4. Ruido electromagnético.
5. Distorsión.
6. Alto voltaje.
7. Variación de frecuencia.

Existen dispositivos que protegen de estas consecuencias negativas, los cuales tienen nombres como:

1. Supresores de picos.
2. Estabilizadores, y
3. Sistemas de alimentación ininterrumpida (SAI o UPS: UNINTERRRUPTIBLE POWER SISTEM.

B. SUMINISTRO ELECTRÓNICO

Las caídas, subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras, monitores, las impresoras y los demás periféricos.

Un corte de la alimentación de la unidad principal puede:

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

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

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

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

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

- Detiene el trabajo.

- El sistema queda expuesto a picos y subidas de tensión cuando vuelve la tensión. Normalmente se desconectan los equipos cuando se va la corriente, pero esto no siempre es posible. Cuando la empresa de electricidad restaura el servicio, a menudo viene con picos que pueden dañar los aparatos que no se hubieran desconectado.

1. U.P.S (SISTEMA DE ENERGIA ININTERRUMPIBLE)

Energía de seguridad para un sistema de computación, cuando la energía eléctrica de la línea se interrumpe o baja a un nivel de tensión inaceptable. El UPS suministra electricidad a una PC (estación o servidor) cuando falla el fluido eléctrico. Esta unidad hace transparente a las interrupciones de fracciones de segundo que inevitablemente detiene a los sistemas y le permite seguir trabajando durante varios minutos. Los pequeños sistemas UPS proveen energía de baterías por sólo unos pocos minutos. Los sistemas más sofisticados están conectados a generadores eléctricos y pueden proveer energía durante días enteros. Los sistemas UPS proveen generalmente protección contra sobrecarga y pueden proveer asimismo regulación de tensión.

Selección de un UPS. Al seleccionar un UPS se debe tener en cuenta los siguientes factores principales:

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

C. ACCIONES HOSTILES

1. ROBO

Los equipos de cómputo son posesiones muy valiosas del SETP TRANSFEDERAL S.A.S. y están expuestos al "robo", de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen el computador de la institución en realizar trabajos privados para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresa invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraída, discos son fácilmente copiados sin dejar ningún rastro.

Cómo evitar el robo:

- Colocar plataformas de anclaje en los diferentes elementos del computador (monitor, CPU, impresora, etc.)
- Diseñar muebles para ordenadores de forma que se pueda asegurar fácilmente la máquina y los periféricos (Tapas con llave, puertas, etc.).
- Evitar que quiten la tapa del ordenador y se lleven la unidad y tarjetas adaptadoras.

Cómo prevenir los robos con computadora

- Adoptando un sistema operativo de última tecnología y que permita el acceso a los equipos de acuerdo a las funciones de cada usuario.
- Creación de un equipo con misión especial que establezca y compruebe técnicas de seguridad para la computadora. Este equipo deberá incluir representantes de los departamentos de procesamiento de datos, seguridad, auditoría y usuario
- Ejecución de un análisis de riesgos en los sistemas que abarquen pérdidas potenciales por accidentes, así como por delitos intencionados.
- Establecer inspecciones y entrevistas que abarquen:

➢ Estado físico del local de la computadora y departamentos de usuarios.
➢ Control de acceso.
➢ Documentación.
➢ Segregación de deberes. Separar (Planeamiento/Desarrollo, de Ejecución y de Verificación/Control).
➢ Trabajo excesivo o innecesario del personal.
➢ Entorno general personal.
➢ Prestar atención especial a la información contable.

Evitar

- Depender de una sola persona para las funciones vitales.
- Repetición periódica de comprobaciones de seguridad. Emplear inspecciones ad-hoc.

2. FRAUDE

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, *los computadores* han sido utilizados en dicho propósito

En realidad, el potencial de pérdida a través de fraudes, y los problemas de prevención y detección del fraude, están en aumento en sistemas computarizados.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

Las tres principales áreas donde se produce el fraude son:

a. Manipulación de información de entrada, fácil de realizar y muy difícil de detectar, al ser los métodos de validación de entrada simples y, en general, conocidos por un gran número de personas de la empresa.
b. Alteración o creación de archivos de información. Se alteran los datos directamente del fichero o se modifica algún programa para que realice la operación deseada.
c. Transmisión ilegal. Interceptar o transferir información de teleproceso.

Entornos que conducen al fraude con computadoras

- Baja moral entre el personal. Los colaboradores en los departamentos de procesamiento de datos y usuarios de la computadora, muestran falta de disciplina respecto a las precauciones de seguridad y en mantener una operación ordenada y sistemáticamente realizada.
- Documentación deficiente. La documentación del sistema está incompleta, anticuada y desordenada. Sólo el diseñador del sistema tiene una idea verdadera de lo que hace el sistema.
- Colaborador innecesariamente atareado todo el tiempo. Colaboradores con pocos permisos para ausentarse, en la misma función, durante largo tiempo y rara vez toman vacaciones (Una vez que un fraude está en marcha, el delincuente necesita mantener continua vigilancia para evitar ser descubierto).
- Falta de segregación de deberes. Se permite a los programadores ingresar datos, el personal de operaciones interviene en programación, etc.
- Deficiente administración de la operación. Falta de control de documentos y de procedimientos de autorización, regulando cambios del sistema y alteraciones a los ficheros de datos. Falta general de control del sistema.
- Alta incidencia de equivocaciones de la computadora. Errores creados por un diseño deficiente del sistema hacen que el personal y gerentes acepten errores susceptibles de "inculpar a la computadora".

3. SABOTAJE

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

La protección contra el sabotaje requiere:

- Una selección rigurosa de los colaboradores.
- 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 sola persona la responsabilidad de la protección de los equipos en cada área.

El problema de la seguridad del computador debe ser tratado como un problema importante de dirección. 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 índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existe un plan idóneo o una recomendación simple para resolver el problema de la seguridad. Realmente no es una situación estática o un problema "puntual", sino que requiere un constante y continuo esfuerzo y dedicación.

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

- Ubicar los equipos en lugares más seguros en donde se prevea cualquier contingencia de este tipo.
- Mantener una lista de números telefónicos de las diferentes dependencias policiales a mano y en lugares donde se pueda hacer un llamado de emergencia.
- Mantener adecuados archivos de reserva (backups)
- Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Montar procedimientos para remitir registro de almacenamiento de archivos y recuperarlos.
- Usar rastros de auditoría o registro cronológico (logs) de transacción como medida de seguridad.

FALLAS GENERICAS FUNCIONALES DE LOS SISTEMAS

A. FALLAS COMUNES

Se han encontrado varias fallas comunes a muchos sistemas de computación. Estos incluyen:

1. Autentificación

Llamamos autentificación a la comprobación de la identidad de una persona o de un objeto. En muchos sistemas, los usuarios no pueden determinar si el hardware y el software con que funcionan son los que se supone que deben ser. Esto hace fácil al intruso reemplazar un programa sin conocimiento del usuario. Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.

2. Cifrado

La lista maestra de contraseñas debe ser almacenada, cifrada, lo que a menudo no se hace.

3. Implementación

Un diseño bien pensado de un mecanismo de seguridad puede ser implementado de forma improcedente.

4. Confianza implícita

Un problema corriente, una rutina supone que otra está funcionando bien cuando, de hecho, debería estar examinando detenidamente los parámetros suministrados por la otra.

5. Compartimiento implícito

El sistema puede depositar inadvertidamente información importante del sistema, en un espacio de direcciones del usuario.

6. Comunicación entre procesos

El intruso puede usar un mecanismo de SEND/RECEIVE para probar varias posibilidades. Por ejemplo el intruso puede pedir un recurso del sistema y suministrar una contraseña. La información devuelta puede indicar "contraseña correcta", confirmando la contraseña adivinada por el intruso.

7. Verificación de la legalidad

El sistema puede no estar realizando una validación suficiente de los parámetros del usuario.

8. Desconexión de línea

En tiempos compartidos y en redes, cuando la línea se pierde (por cualquier razón), el sistema operativo debe inmediatamente dar de baja del sistema al usuario o colocar al usuario en un estado tal, que sea necesaria la reautorización para que el usuario obtenga de nuevo el control. Algunos sistemas permiten que un proceso "flote" después de una desconexión de línea. Un

intruso puede llegar a obtener el control del proceso y usar cualesquier recurso a los que tenga acceso el proceso.

9. Descuido del operador

Un intruso puede engañar a un operador y hacer que cargue un paquete de disco con un sistema operativo falso.

10. Paso de parámetros por referencia en función de su valor

Es más seguro pasar los parámetros directamente en registros, que tener los registros apuntando a las localidades que contienen los parámetros. El paso por referencia puede llevar a una situación en la cual los parámetros, pueden aún encontrarse en el espacio de direcciones del usuario después de una verificación de la legalidad. El usuario podría así suministrar parámetros legítimos, verificarlos, y modificarlos justo, antes de ser utilizados por el sistema.

11. Contraseñas

Las contraseñas son, a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse con número máximo (3) de intentos infructuosos.

12. Entrampamiento al intruso

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

13. Privilegio

En algunos sistemas hay demasiados programas con muchos privilegios. Esto es contrario al principio del menor privilegio.

14. Confinamiento del programa

Un programa prestado de otro usuario puede actuar como caballo de Troya: puede robar o alterar los archivos del usuario que los prestó.

15. Residuos

A menudo el intruso puede encontrar una lista de contraseñas con sólo buscar en una papelera. Los residuos se dejan a veces en el almacenamiento después de las operaciones rutinarias del sistema. La información delicada debe ser siempre destruida antes de liberar o descargar el medio que ocupa (almacenamiento, papel, etc.). Las trituradoras de papel son algo corriente en ese aspecto.

16. Blindaje

Una corriente en un cable genera un campo magnético alrededor de él; los intrusos pueden de hecho conectarse a una línea de transmisión o a un sistema de computación sin hacer contacto físico. Puede usarse el blindaje eléctrico para prevenir tales "intrusiones invisibles".

17. Valores de umbral

Están diseñados para desanimar los intentos de entrada, por ejemplo. Después de cierto número de intentos inválidos de entrar al sistema, ese usuario (o el terminal desde donde se intentan las entradas) debe ser bloqueado y el administrador del sistema, advertido. Muchos sistemas carecen de esta característica.

B. ATAQUES GENÉRICOS A SISTEMAS OPERATIVOS

Ciertos métodos de penetración se han utilizado efectivamente en muchos sistemas.

1. Asincronismo

Con procesos múltiples que progresan de forma asincrónica, es posible que un proceso modifique los parámetros cuya validez ha sido probada por otro, pero que aún no ha utilizado. Con esto, un proceso puede pasar valores malos a otro, aún cuando el segundo realice una verificación extensa.

2. Rastreo

Un usuario revisa el sistema de computación, intentando localizar información privilegiada.

3. Entre líneas

Se usa un terminal especial para conectarse a la línea de comunicación mantenida por un usuario dado de alta en el sistema, que está inactivo en ese momento.

4. Código clandestino

Se hace un parche en el sistema operativo bajo la pretensión de una depuración. El código contiene trampas que permiten realizar a continuación reentradas no autorizadas al sistema.

5. Prohibición de acceso

Un usuario escribe un programa para hacer caer al sistema, poner al sistema en un ciclo infinito, o monopolizar recursos del sistema. Lo que se intenta aquí es el negar el acceso o servicio a los usuarios legítimos.

6. Procesos sincronizados interactivos

Los procesos usan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.

7. Desconexión de línea

El intruso intenta obtener acceso al trabajo de un usuario después de una desconexión de línea, pero antes de que el sistema reconozca la desconexión.

8. Disfraz

El intruso asume la identidad de un usuario legítimo, después de haber obtenido la identificación apropiada por medios clandestinos.

9. Engaño al operador

Un intruso inteligente puede, a menudo, engañar al operador del computador y hacer que realice una acción que comprometa la seguridad del sistema.

10. Parásito

El intruso utiliza un terminal especial para conectarse a una línea de comunicación. El intruso intercepta los mensajes entre el usuario y el procesador, modifica el mensaje o lo reemplaza por completo.

11. Caballo de Troya

El intruso coloca un código dentro del sistema que le permita accesos posteriores no autorizados. El caballo de Troya puede dejarse permanentemente en el sistema o puede borrar todo rastro de si mismo, después de la penetración.

IMPLEMENTACIÓN

Para este caso se tiene que tener preparado los planes de contingencia para poder aplicarlos. Puede también tratarse esta etapa como una prueba controlada.

A. EMERGENCIA FÍSICAS (CASOS)

1. 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:

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

2. Error de Memoria RAM

En este caso se dan los siguientes síntomas:

a. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
b. Ante procesos mayores se congela el proceso.
c. Arroja errores con mapas de direcciones hexadecimales.
d. El servidor deberá contar con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.
e. 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
f. inmediatamente.
g. Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar las memorias malogradas.
- Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
- Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- Probar los sistemas que están en red en diferentes estaciones.

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

3. Caso de Incendio Total

La mejor manera de **prevenir** un incendio es no provocarlo. Observe las prohibiciones de no fumar y las normas de prevención propias del local en que se encuentre, y con mayor razón en un centro de cómputo.

En presencia del fuego tenga en cuenta que:

- Puede tratar de apagar un fuego en una oficina siempre que tenga detrás una puerta que le permita salida.
- Si el fuego prende en sus ropas, no corra, tírese al suelo y ruede. Si el hecho ocurre a otra persona cúbrala con alguna prenda o con una toalla humedecida, si se encuentra próximo a un aseo. No se quite la ropa si tiene quemaduras.
- En presencia de aparatos eléctricos, no eche agua al fuego**.** Tampoco debe hacerlo ante líquidos inflamables (alcohol, aceite, gasolina, etc).
- Si hay mucho humo póngase un pañuelo en la boca y nariz, a ser posible mojado, y salga agachado o gateando. Respire profundamente para evitar desvanecimientos.
- Al salir de una dependencia, procure cerrar las ventanas y las puertas, pues las corrientes avivan el fuego.
- Si se encuentra aislado y no puede ponerse a salvo, diríjase a la habitación más alejada del fuego (pero no a un nivel superior a menos que esté seguro de que los equipos de rescate se encuentran muy cerca y provistos de escaleras largas u otro equipo.
- Si se ve obligado a huir a través de las llamas para ponerse a salvo, no se entretenga en recoger nada, cúbrase (incluyendo la cabeza) con una manta, una toalla, una cortina o un abrigo mojados si es posible, luego aguante la respiración y corra.

Con respecto a los equipo de computo

En el momento que se dé aviso 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 discos duros y CD.

a. Ante todo, se debe conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, se debe tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

b. 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).

c. Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas.

d. 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.

5. Caso de Inundación

a. Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.

b. En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.

c. 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.

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

e. Proveer cubiertas protectoras para cuando el equipo esté apagado.

6. Caso de Fallas de Fluido Eléctrico

Se puede presentar lo siguiente:

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

b. 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.

c. 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.

B. EMERGENCIAS LÓGICAS DE DATOS (CASO)

1. Caso de Virus

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

Para servidor:

a. Contar con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación.

b. El antivirus muestra el nombre del archivo infectado y quién lo usó.

c. Estos archivos (exe, com, ovl, nlm, etc.) serán reemplazados del CD original de instalación o del backup.

d. Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

Se revisará las computadoras que no estén en red con antivirus de CD.

De suceder que una computadora se haya infectado con uno o varios virus a nivel disco duro, se debe proceder a realizar los siguientes pasos:

a. Utilizar un CD que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado. Reiniciar el computador con dicho CD.

b. Retirar el CD con el que arrancó el computador e insertar el CD antivirus, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, se borrará el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el scaneado, reconstruir el Master Boot del disco duro.

MEDIDAS DE PRECAUCION

A. EN RELACIÓN AL CENTRO DE CÓMPUTO

a. Los equipos no deben estar ubicados en las áreas de alto tráfico de personas o con un alto número de invitados.

b. Con respecto a los grandes ventanales, se deben cubrir con persianas, cortinas o algún protector para evitar la entrada del sol y calor, los cuales son inconvenientes para el equipo de cómputo, puede ser un riesgo para la seguridad de los mismos.

c. Otra precaución que se debe tener en el cuidado de los equipos es que en la oficina no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no queden perfectamente selladas y despidan polvo.

d. El acceso a las diferentes oficinas y al uso de los equipos debe estar restringido a personas ajenas. Los colaboradores del SETP TRANSFEDERAL S.A.S. deberán tener su carné de identificación siempre en un lugar visible

e. Establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.

f. Al momento de reclutar a los nuevos colaboradores se les debe realizar exámenes psicológicos y médico, y tener muy en cuenta sus antecedentes de trabajo en otras instituciones, ya que un Centro de Cómputo depende en gran medida, de la integridad, estabilidad y lealtad de los colaboradores.

g. El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.

h. Establecer controles para una efectiva disuasión y detección, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contienen.

i. Establecer políticas para la creación de los passwords y establecer periodicidad de cambios de los mismos.

j. Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.

k. Establecer políticas de control de entrada y salida del personal, así como de los paquetes u objetos que portan.

l. Los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de Cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.

m. Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Gerencia.

n. Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

B. RESPECTO A LA ADMINISTRACIÓN DE LOS BACKUPS

a. Se administrará bajo la lógica de un almacén, esto implica ingreso y salida de medios magnéticos (discos removibles, CD's, etc.) obviamente teniendo más cuidado con las salidas y cuidando que el grado de temperatura y humedad sean los adecuados.

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

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

d. El proceso de etiquetado tiene que quedar registrado.

C. RESPECTO A LA ADMINISTRACIÓN DE IMPRESORAS

a. Todo listado que especialmente contenga información confidencial, debe ser destruido.

b. Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.

c. Establecer controles respecto a los procesos remotos de impresión.

D. PARA EL MANTENIMIENTO DE LOS DISCOS DUROS

a. 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.

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

c. 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.

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

e. Para mantener la velocidad en el equipo, se debe realizar una vez al mes el proceso de desfragmentación para conservar en óptimo estado la respuesta del equipo; Windows incluye un desfragmentador de disco fácilmente localizable en el menú Inicio/Todos los programas/Accesorios/Herramientas del Sistema/Desfragmentador de disco.

f. Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un microcomputador.

D. RESPECTO A LOS MONITORES

a. Usar medidas contra la refección para reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día.

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

c. También manténgase por lo menos a 1 m. o 1.20 m. (3 o 4 pies) del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.

d. Finalmente apague su monitor cuando no lo esté usando

E. PARA EL CUIDADO DEL EQUIPO DE CÓMPUTO

a. Teclado. Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función. Para eliminar el polvo del teclado, lo más conveniente es voltearlo y soplar el aire comprimido para que éste salga completamente. Se debe evitar en lo posible quitar las tapas de las teclas de la PC para lavarlas, ya que su reposición puede generar fallas mecánicas.

b. CPU. Mantener la parte posterior del CPU liberado en por lo menos 10cm. Para asegurar así una ventilación mínima adecuada.

c. CD-ROM. Antes de usar cualquiera de estos componentes, se debe verificar que el CD-ROM/DVD o CDRW del equipo se encuentren limpios, de igual forma, cada CD o DVD que se utilicen deben encontrarse libres de polvo y partículas para forzar menos al láser y prolongar su duración.

d. Protectores de pantalla. Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.

e. Impresora. El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel.

f. Caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.

g. Papelera de reciclaje. Windows reserva un 10% de la capacidad del disco duro para mantener algo de la información que ya se haya eliminado, con la finalidad de que en cualquier momento se pueda recuperar. No obstante, la papelera de reciclaje, ubicada en el Escritorio de la computadora, debe limpiarse con regularidad para no llenarse de basura que le estará quitando espacio en disco duro. Se debe seleccionar el ícono y hacer clic derecho, posteriormente elegir la opción Explorar, podrá ver todos los archivos ubicados en su papelera y eliminar aquéllos que no necesite o, en su caso, vaciar la papelera de reciclaje.

h. Término de sesión o apagado. En muchas ocasiones, por la prisa o mal uso de la computadora, no se cierran las aplicaciones correctamente o bien, no se apaga la computadora de forma adecuada, esto provoca pérdida de información y daña el sistema operativo.

F. MANTENER LAS ÁREAS OPERATIVAS LIMPIAS Y PULCRAS

Para proteger a nuestras computadoras del polvo, resulta muy conveniente adquirir algunas fundas para los CPU, monitor, teclado, escáner, y/o cualquier otro equipo de cómputo para evitar que entre el polvo a los componentes más sensibles y cause daño; no se debe olvidar que la limpieza es necesaria, para ello se pueden emplear aire comprimido, espumas y una pequeña franela.

DISPOSICIONES FINALES

1. El Plan de Contingencia contará con el apoyo correspondiente por parte de la Gerencia, para suministrar de recursos financieros, humanos y materiales a fin de su implementación y ejecución.

2. Realizar la conformación de un Comité Técnico Institucional, el cual sea el encargado de planificar, implementar y supervisar la ejecución del Plan de Contingencia Informático, que asegure la legalidad, consistencia, adecuado uso, seguridad, inviolabilidad y sostenibilidad de los Sistemas de Información, hardware y software.

3. Los Gerentes, Líderes de áreas y colaboradores que laboren en el SETP TRANSFEDERAL S.A.S., deben tomar parte de las actividades y están obligados a participar en la implementación y ejecución del Plan de Contingencia.

4. Definir políticas de seguridad, como una herramienta para el control permanente del cumplimiento del Plan de Contingencia.

5. Implementar un Plan de Capacitación y Entrenamiento a todos los colaboradores del SETP TRANSFEDERAL S.A.S., con la finalidad de mantener al personal debidamente entrenado para prevenir y enfrentar cualquier emergencia, así como, disponer de un plan de entrenamiento de todos los colaboradores en la solución de situaciones de emergencia a través de charlas periódicas en los que se describan los riesgos existentes.

6. Las medidas que debemos adoptar para protegernos son tantas como amenazas existen, es por ello que se debe difundir a todas las áreas del SETP TRANSFEDERAL S.A.S. copias del Plan, documentos resumen, carteles, afiches u otro tipo de documento para su información.

7. Implementar un servidor de respaldo que haga de backup a todos los servidores, reemplazando a uno u otro según se necesite, para ello se realizará las acciones necesarias para que el SETP TRANSFEDERAL S.A.S. cuente con dicho servidor que cumpla a su vez con una gama de funciones como por ejemplo: Servidor de Archivo, Servidor de Respaldo, Almacenamiento masivo, Servidor de usuarios y/o Workgroups, etc.