SIERRA EXPORTADORA
RESOLUCIÓN DIRECTORAL
Nº 053-2010-OGA/SE

Lima, 25 de mayo de 2010

VISTOS:

La Ley Nº 28890, norma de creación de Sierra Exportadora, la Resolución de Presidencia Ejecutiva N° 045-2007-PE/SE y el Proyecto del Plan de Contingencias 2010, elaborado por la Unidad de Tecnología de la Información, y;

Sierra Exportadora Oficina de Asesoría Jurídica V° B°

CONSIDERANDO:

Que, mediante Ley N° 28890 se crea el Organismo Público Sierra Exportadora adscrito a la Presidencia del Consejo de Ministros, con personería jurídica de derecho público, con autonomía técnica, funcional, administrativa, económica y financiera y constituyendo Pliego Presupuestal;

Sierra Exportadora Oficina General de Administración V° B°

Que, mediante Resolución de Presidencia Ejecutiva N° 045-2007-PE/SE se asignan las funciones y responsabilidades de Administración y Finanzas contenidas en la Directiva N° 001-2007-PE/SE "Estructura Provisional de Responsabilidades de Sierra Exportadora";

Que, resulta necesario establecer al interior de la entidad un plan de contingencias en materia informática que identifique aquellos sistemas de información y/o recursos informáticos aplicados que son susceptibles de deterioro, violación o pérdida y que pueden ocasionar graves trastornos para el desenvolvimiento normal de la Entidad;

Que, de conformidad con lo dispuesto en la Ley N° 28890 y la Resolución de Presidencia Ejecutiva N° 045-2007-PE/SE;

SE RESUELVE:

ARTÍCULO ÚNICO.- Aprobar el Plan de Contingencia 2010, elaborado por la Unidad de Tecnología de la Información, que forma parte de la presente Resolución.

Sierra Exportadora
V° B°
Oficina de Asesoría Jurídica

REGÍSTRESE Y COMUNÍQUESE.

SIERRA EXPORTADORA

PC. José Manuel Ruiz Naupari
Jefe de Oficina General de Administración

PLAN DE CONTINGENCIAS 2010

CONTENIDO

Sierra Exportadora Oficina General de Administración V° B°

Sierra Exportadora Tecnología de Información V° B°

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

1. INTRODUCCION

La información de la institución es provista mediante el uso de Tecnologías de la Información y Comunicaciones (TIC). Estas tecnologías abarcan datos, sistemas de información, tecnología asociada, instalaciones y personal. Al conjugar una serie de elementos como hombres y equipos de cómputo, se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas y por ende de la institución.

Las actividades de control de las TIC incluyen controles que garantizan el procesamiento de la información para el cumplimiento misional y de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas.

Los componentes o recursos de un SI son los siguientes:

- Datos: En general se consideran datos tanto los estructurados como los no estructurados, las imágenes, los sonidos, etc.
- Aplicaciones: Se incluyen los manuales y las aplicaciones informáticas.
- Tecnología: El software y el hardware; los sistemas operativos; los sistemas de gestión de bases de datos; los sistemas de red, etc.
- Instalaciones: En ellas se ubican y se mantienen los sistemas de información.
- Personal: Los conocimientos específicos que ha de tener el personal de los sistemas de información para planificarlos, organizarlos, administrarlos y gestionarlos.

Un plan de contingencias es una estrategia planificada con una serie de procedimientos que nos facilita o nos orienta a tener una solución alternativa, que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.

Un plan de Contingencias consiste en la identificación de aquellos sistemas de información y/o recursos informáticos aplicados que son susceptibles de deterioro, violación o pérdida y que pueden ocasionar graves trastornos para el desenvolvimiento normal de la organización, con el propósito de estructurar y ejecutar aquellos procedimientos y asignar responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible y a unos costos razonables.

En Sierra Exportadora, se ha elaborado este plan de contingencias para poder seguir atendiendo a los usuarios en situaciones donde el sistema informático falle por desastres naturales o por factor humano.

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

2. DATOS DE LA INSTITUCION

Nombre de la Institución : SIERRA EXPORTADORA.

Dirección : Av. Conquistadores 970 – San Isidro

Infraestructura Informática :

- 06 Servidores: IBM XSeries 3650.
- 02 Servidores: DELL
- Sistema Operativo: Windows 2003 Server.
- 65 PC'S ACER Pentium IV conectadas en red.
- 36 PC'S IBM CORE 2DUO conectadas en red.
- 6 Notebooks DELL modelo LATIDUDE D620 Core2Duo conectadas en red.
- 2 Notebooks DELL modelo XPS Core2Duo conectadas en red.
- 2 Notebooks SONY VAIO DELL Core2Duo conectadas en red.
- 4 Impresoras Multifuncionales conectadas en red.
- 12 Impresoras Laser Jet conectadas en red.
- 15 impresoras Laser Jet instaladas en las Sedes Descentralizadas conectadas a través de una red VPN.
- 2 Fotocopiadora conectada en red
- Arquitectura Cliente/ Servidor.

Infraestructura del Data Center :

a. Controlador de Dominio (CDSIERRA)
b. Servidor de Backup (BKCDBACKUP)
c. Servidor de Archivos (FILE)
d. Servidor de Aplicaciones y Base de Datos (DATABASE)
e. Servidor de Correos (MAIL)
f. Servidor Web (WWW)
g. Servidor AntiSpam (SCMSERVER)
h. Servidor Firewall (SIEXFW)

a. Servidor Controlador de Dominio (CDSIERRA)

Este es el servidor principal de la infraestructura de servidores, en él radica la administración de los usuarios, grupos y políticas de usuario, DNS integrado al dominio.

La principal responsabilidades del servidor es la autentificación, cuyo proceso es garantizar y/o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, a través del uso de un password.

Sierra Exportadora V°B° Tecnología de Información

Sierra Exportadora V°B° Oficina General de Administración

En la actualidad el servidor cuenta con las siguientes características:

Sistema Operativo del Servidor:

El Sistema Operativo Base es Windows 2003 Server R2 Standard Edition (Ingles), con Service Pack 2.

Características Físicas del Servidor:

- Marca : IBM
- Modelo : XSeries 3650
- Procesador : Intel Xeon de 3 Ghz
- Memoria : 1 Gb RAM
- HD : 2 discos SCSI de 73 Gb

Distribución del espacio de disco:

Espacio Total en Disco: 73 Gb, particionado de la siguiente manera:

Partición C: 18.64 Gb: Destinado para la instalación del Sistema Operativo y programas.

Partición F: 30.07 Gb: Destinado para almacenar los backups de Dominio.

Partición E: 19.53 Gb: Destinado para el bat para las unidades de red y la documentación de las políticas de dominio.

b. Servidor de Backup (BKCDSIERRA)

Es un servidor que trabaja de manera simultánea y como respaldo del servidor de dominio, en caso de cualquier caída o perdida del controlador de dominio principal este asume la tarea de autentificación, administración de los usuarios, grupos y políticas de usuario, y servidor DNS.

Sistema Operativo del Servidor:

El Sistema Operativo Base es Windows 2003 Server R2 Standard Edition (Ingles), con Service Pack 2.

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

Características Físicas del Servidor:

- Marca : IBM
- Modelo : XSeries 3650
- Procesador : Intel Xeon de 3 Ghz
- Memoria : 2 Gb RAM
- HD : 2 discos SCSI de 36 Gb y 2 discos SCSI de 143 Gb.

Distribución del espacio de disco:

Espacio Total en Disco: 179 Gb, particionado de la siguiente manera:

Partición C: 19.77 Gb: Destinado para la instalación del Sistema Operativo y programas.

Partición F: 17.01 Gb: Destinado para el reporte de jobs del sistema de Backup y almacenamiento de los backups de correos.

Partición E: 136.61 Gb: Destinado para almacenar los backups de Correo, Archivos, Usuarios Antiguos, Web, Intranet, otros.

c. Servidor File Server (FILE)

Es el servidor dentro de nuestra infraestructura de red, que almacena los datos y la información generada por cada usuario de la institución, al que se le ha asignado un usuario y contraseña. La información almacenada es estrictamente de índole laboral y propiedad de la institución.

Sistema Operativo del Servidor:

El Sistema Operativo Base es Windows 2003 Server R2 Standard Edition (Ingles), con Service Pack 2.

Características Físicas del Servidor:

- Marca : IBM
- Modelo : XSeries 3650
- Procesador : Intel Xeon de 3 Ghz
- Memoria : 2 Gb RAM
- HD : 2 discos SCSI de 36 Gb y 2 discos SCSI de 143 Gb.

Sierra Exportadora V°B° Tecnología de Información

Sierra Exportadora V°B° Oficina General de Administración

Distribución del espacio de disco:

Espacio Total en Disco: 179 Gb, particionado de la siguiente manera:

Partición C: 18.68 Gb: Destinado para la instalación del Sistema Operativo y programas.

Partición E: 4.89 Gb: Destinado para almacenar información referente a la institución Ejemplo: Contratos.

Partición F: 78.13 Gb: Destinado para almacenar los Archivos de los diferentes usuarios de la institución.

Partición G: 34.92 Gb: Destinado para almacenar el backup del servidor de Archivos.

d. Servidor de Base de Datos (DATABASE)

Este servidor es el principal contenedor de información de las diferentes Bases de Datos de la institución, las cuales se conectan a través de aplicaciones Windows o Sistemas de Información.

Es aquí donde se instalan las principales aplicaciones (De preferencia con tecnología mínima Cliente/Servidor), al igual que con sus Bases de Datos respectivas.

Sistema Operativo del Servidor:

El Sistema Operativo Base es Windows 2003 Server R2 Standard Edition (Ingles), con Service Pack 2

El Software Motor de Base de Datos es SQL Server 2000

Características Físicas del Servidor:

- Marca : IBM
- Modelo : XSeries 3650
- Procesador : Intel Xeon de 3 Ghz
- Memoria : 3 Gb RAM
- HD : 3 discos SCSI DE 73 Gb

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

Distribución del espacio de disco:

Espacio Total en Disco: 143 Gb, particionado de la siguiente manera:

Partición C: 27.95 Gb: Destinado para la instalación del Sistema Operativo, programas y utilitarios.

Partición E: 108.56 Gb: Destinado para los Sistemas de Información, Aplicaciones y Bases de Datos.

e. Servidor Exchange (MAIL)

Servidor propiamente de correo electrónico, que se dedica a prestar servicios de alojamiento de la base de datos del servicio de Correo, almacena los buzones de los diferentes usuarios, así también permite el intercambio de correos internos y externos.

Sistema Operativo del Servidor:

El Sistema Operativo Base es Windows 2003 Server R2 Standard Edition (Ingles), con Service Pack 2, con el sistema de correos Microsoft Exchange Server 2003.

Características Físicas del Servidor:

- Marca : IBM
- Modelo : XSeries 3650
- Procesador : Intel Xeon de 3 Ghz
- Memoria : 3 Gb RAM
- HD : 2 discos SCSI DE 143 Gb

Distribución del espacio de disco:

Espacio Total en Disco: 143 Gb, particionado de la siguiente manera:

Partición C: 18.64 Gb: Destinado para la instalación del Sistema Operativo y programas.

Partición E: 117.98 Gb: Destinado para almacenar los buzones de los diferentes usuarios e información de la Base de datos del servidor Exchange MDBDATA (Priv1.edb, priv1.stm).

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

f. Servidor Web (WWW)

Servidor en el cual se aloja el Portal Institucional de Sierra Exportadora y los aplicativos y software necesarios para optimizar su disponibilidad en internet.

Además del servidor y la conexión a internet, el sistema debe contar con una serie de programas básicos para dar servicio web

Sistema Operativo del Servidor:

El Sistema Operativo Base es Windows 2003 Server R2 Standard Edition (Ingles), con Service Pack 2, con el servicio IIS (Internet Information Services) para la publicación y administración de los servicios web (Portal Sierra Exportadora, intranet, ftp).

Características Físicas del Servidor:

- Marca : IBM
- Modelo : XSeries 3650
- Procesador : Intel Xeon de 3 Ghz
- Memoria : 2 Gb RAM
- HD : 2 discos SCSI de 73 Gb

Distribución del espacio de disco:

Espacio Total en Disco: 73 Gb, particionado de la siguiente manera:

Partición C: 18.68 Gb: Destinado para la instalación del Sistema Operativo y programas.

Partición E: 49.57 Gb: Destinado para alojar el portal institucional, el portal del datasiex, la intranet institucional, el servicio ftp.

Sierra Exportadora Vo Bo Tecnología de Información

Sierra Exportadora Vo Bo Oficina General de Administración

g. Servidor Firewall (SIEXFW)

Es el servidor que maneja un sistema que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados, es decir determina quién puede entrar para utilizar los recursos de red de Sierra Exportadora.

El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad.

Sistema Operativo del Servidor:

Sistema operativo Check Point basado en código cerrado altamente seguro y certificado.

Características Físicas del Servidor:

- Marca : DELL
- Modelo : XSeries 3650
- Procesador : Intel Xeon de 3 Ghz
- Memoria : 1 Gb RAM
- HD : 80 Gb.

Distribución del espacio de disco:

Disk /dev/sda: 79.4 GB, 79456894976 bytes

Device Boot	Start	End	Blocks	Id	System
/dev/sda1 *	1	13	104391	de	Dell Utility
/dev/sda2	14	32	152617+	83	Linux
/dev/sda3	33	482	3614625	83	Linux
/dev/sda4	483	9660	73722285	f	Win95 Ext'd (LBA)
/dev/sda5	483	9074	69015208+	83	Linux
/dev/sda6	9075	9269	1566306	83	Linux
/dev/sda7	9270	9530	2096451	82	Linux swap
/dev/sda8	9531	9660	1044193+	83	Linux

Sierra Exportadora V°B° Tecnología de Información

Sierra Exportadora V°B° Oficina General de Administración

h. Servidor Anti-spam (SCMSERVER)

Appliance dedicado a filtrar SPAM (emails de publicidad, correos basura, spyware, otros) en los diferentes buzones de correos existentes, minimizando el riesgo de ingreso y que estos saturen la bandeja de entrada, y recarguen la base de datos del servidor de correo.

Sistema Operativo del Servidor:

Sistema Operativo propietario de la marca Mcafee basado en Linux.

Características Físicas del Servidor:

- Marca : DELL
- Modelo : Appliance
- Procesador : Intel Celeron 2.4 Ghz
- Memoria : 2 Gb de RAM
- HD : 80 Gb

3. OBJETIVOS DEL PLAN

- Optimizar los esfuerzos y recursos necesarios para atender cualquier contingencia frente a los sistemas de información de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes y durante la emergencia.
- Asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos, y de los medios de almacenamiento.
- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.
- Reanudar con la mayor brevedad posible la operatividad de los equipos y/o sistemas críticos, en aras a minimizar el impacto de manera que la correcta recuperación de los sistemas y procesos quede garantizada y se conserven los objetivos estratégicos de la institución.

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

La vigencia de este plan está sujeto a cambios tecnológicos, de equipamiento y de los sistemas informáticos relacionados con la institución.

4. ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN.

4.1 La Seguridad Física

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Falla, local o general, tres serían las medidas a preparar para ser utilizadas en relación a la cronología de la falla.

4.1.1 Antes

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar la falla o, en su caso, aminorar las consecuencias que de él se puedan derivar.

Es un concepto aplicable a cualquier actividad, pero nos centraremos sólo a lo referente a la Unidad de Tecnología de Información, en la que las personas hagan uso particular o profesional de entornos físicos;

- Ubicación del Centro de Procesamiento de Datos dentro del edificio.
- Elementos de la construcción.
- Potencia eléctrica.
- Sistemas contra Incendios.
- Control de accesos.
- Selección de personal.

4.1.2 Durante

Se debe de ejecutar un plan de contingencia adecuado. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa.

La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la institución, para ello se debe contar con los medios necesarios para afrontarlo como el plan de contingencia que coordina las necesidades del negocio y las operaciones de

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

recuperación del mismo.

Son puntos imprescindibles del plan de contingencia:

- Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas
- Establecer un periodo crítico de recuperación, en la cual los procesos debe de ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por que se establecerán las prioridades del proceso.
- Determinar las prioridades del proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Establecer objetivos de recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de desastre y el momento en el que el centro alternativo puede procesar las aplicaciones críticas.
- Asegurar la capacidad de las comunicaciones.
- Asegurar la capacidad de los servidores back-up.

4.1.3 Después

Los contratos de seguros vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades que se puedan derivar para el centro de proceso de datos una vez detectada y corregida la falla. De la gama de seguros existentes, se pueden indicar los siguientes:

- Centros de proceso y equipamiento: se contrata la cobertura sobre el daño físico en el CPD (Centro de Procesamiento de Datos) y el equipo contenido en el.
- Gastos extra: cubre los gastos extra que derivan de la continuidad de las operaciones tras un desastre o daño en el centro de proceso de datos. Es suficiente para compensar los costos de ejecución del plan de contingencia.
- Interrupción del negocio: cubre las pérdidas de beneficios netos causadas por las caídas de los medios informáticos o por la suspensión de las operaciones.
- Transporte de medios: proporciona cobertura ante pérdidas o daños a los medios transportados.
- Contratos con proveedores y de mantenimiento: proveedores o

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

fabricantes que aseguren la existencia de repuestos y consumibles, así como garantías de fabricación.

5. PLAN DE CONTINGENCIA

Se tendrá en cuenta:

5.1 Análisis y evaluación de Riegos.
5.2 Asignación de prioridades.
5.3 Implementación del plan (acciones correctivas y preventivas).
5.4 Distribución y mantenimiento del plan.

5.1 ANALISIS Y EVALUACIÓN DE RIESGOS

Es necesario reconocer y reducir los riesgos potenciales que afecten a los productos (aplicativos) y servicios; es por ello que se considera dentro de un Plan de Contingencia, como primer paso la Reducción de Riesgos, para favorecer el cumplimiento de los objetivos institucionales.

El análisis y evaluación de riesgos consta de:

5.1.1 Realización de un diagnóstico integral del Sistema de Información.

5.1.2 Elaborar una lista de Servicios afectados y su magnitud del impacto.

5.1.3 Identificar los procesos de los servicios afectados.

5.1.4 Orden de prioridades.

5.1.1.- Diagnóstico integral del Sistema de Información.

Si consideramos que "No existe producto y/o servicio sin un proceso. De la misma manera, que no existe proceso sin un producto o servicio". Aunque no todos los procesos generan un producto o servicio útil (creando valor agregado) para la institución. Por lo que es necesario realizar un análisis de las operaciones y los procesos que involucran. Estos son:

- Organización. Cualquier grupo, empresa, corporación, institución, etc.
- Función. Un grupo dentro de la organización funcional. Funciones características: personal, contabilidad, logística, almacén, mercados, operaciones.
- Proceso. Cualquier actividad o grupo de actividades que emplee un insumo, le agregue valor a éste y suministre un producto a un cliente externo o

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

interno. Los procesos utilizan los recursos de una organización para suministrar resultados definitivos.

- Proceso Presupuestal. Relacionado directamente con el sistema del SIAF del Ministerio de Economía y Finanzas para la asignación presupuestal de la institución, Dependencia directa a la conexión de Internet. Manejo constante del correo institucional.
- Proceso Logístico. Relacionado directamente con el SIGA Relacionado directamente con las aplicaciones del SEACE para las convocatorias respectivas. Dependencia directa a la conexión de Internet. Manejo constante del correo institucional.
- Proceso Contable. Relacionado con el sistema del SIAF del Ministerio de Economía y Finanzas para los compromisos de pago respectivo, y con el sistema de viáticos para la generación y rendición de los mismos. Dependencia directa a la conexión de Internet. Manejo constante del correo institucional.
- Proceso Tesorería. Relacionado con el Sistema de Fondos fijos para la determinación y asignación de montos para la caja chica de la institución a nivel sede central y sedes descentralizadas. Dependencia directa a la conexión de Internet. Manejo constante del correo institucional.
- Proceso de Operaciones. Relacionado con el Sistema de Viáticos para la generación de los mismos y la rendición respectiva. Necesidad de la conexión a Internet para la recopilación de información relacionada a su gestión. Manejo constante del correo institucional.

Sierra Exportadora
V°B°
Tecnología de Información

Sierra Exportadora
V°B°
Oficina General de Administración

5.1.2.-Lista de Servicios afectados según causa e impacto.

Se tienen en cuenta dos factores:

- Los que afectan a la seguridad del local.
- Los que afectan la integridad de los datos.

Los que afectan a la seguridad del local:

CONTINGENCIA	CAUSA	FACTOR DE RIESGO
Inundación	Puede darse en el caso de descuido de los usuarios o del personal de limpieza en dejar las llaves de los caños de los baños abiertas durante toda la noche.	Bajo
Incendio	Puede darse ya que el material que hay en almacén es inflamable. Al respecto se cuentan con extinguidores en todos los pisos.	Medio
Robo	Se cuenta con cerco eléctrico en la puerta principal y en la parte posterior que da al estacionamiento, además de contar con vigilancia las 24 horas del día.	Alto
Corte de energía eléctrica	No se cuenta con generadores eléctricos. Se cuenta con un UPS's, en la sala de servidores dedicado para los servidores.	Medio
Sismos	Desastres provocados por la naturaleza en donde no hay control humano.	Bajo

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

Los que afectan la integridad de los datos:

CONTINGENCIA	CAUSA	FACTOR DE RIESGO
Virus informáticos	Se cuenta con un servidor firewall, antivirus actualizado permanentemente, y el control de acceso a Internet.	Bajo
Problemas de comunicación del cliente con el servidor	Tarjeta de red dañada, Cable de red partido, Problemas en el switch. El cableado de datos no es estructurado y presenta signos de tener más de 5 años de antigüedad	Alto
Problemas en el cableado eléctrico de las estaciones de trabajo	Cables eléctricos viejos, Toma corrientes en mal estado, etc. El cableado eléctrico dedicado para los equipos de computo tienen una central independiente con un pozo a tierra	Medio
Problemas con los recursos compartidos de la red.	Recursos compartidos sin los permisos debidos, recursos compartidos a más usuarios de los debidos.	Bajo
Caída temporal del servidor por falla mecánica.	Desperfecto en el procesador, desperfecto en el disco duro o en la memoria RAM. Desperfecto de software.	Bajo
Pérdida total o parcial de las estaciones de trabajo	Discos Duros, Placas y Memorias que puedan dañarse.	Bajo

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

5.1.3.-Procesos de los servicios afectados:

Los que afectan a la seguridad del edificio:

Todos los sucesos que afecten la seguridad del edificio afectarán directa o indirectamente al normal desarrollo de los procesos de la institución.

- Inundación: Ocasionaría pérdidas totales o parciales de hardware dependiendo donde se produzca el siniestro, puesto que se cuenta con servicios higiénicos en cada piso. El siniestro ocasionará que se interrumpan las actividades hasta solucionar el problema.
- Incendio: Puede ocasionar pérdidas totales o parciales. Si la pérdida es total, los costos serían muy altos puesto que habría que adquirir todos los equipos nuevamente, retrasando el desempeño de las funciones de las áreas afectadas.
- Corte de energía eléctrica: Discontinuidad en el trabajo. Se paralizaría las labores hasta el retorno de la energía eléctrica. Se salvaguarda la seguridad física y lógica de los servidores al contar con un UPS lo que nos da el tiempo necesario para proceder al corte del servicio de manera normal.
- Robo: Pérdidas totales o parciales, según la gravedad de los hechos. Aquí intervendrían costos de Hardware.
- Sismos: Generaría pérdidas totales o parciales, dependiendo la magnitud del sismo, y los daños colaterales que este produzca.

Los que afectan la integridad de los datos:

- Virus informáticos: Generaría molestias en el sistema, ya que lo degradan y lo hacen más lento. Habría pérdidas totales o parciales, de la información almacenada.
- Los problemas de comunicación del cliente con los servidores, éstos afectaran el normal desempeño del área afectada por razones de tener una estructura de red en cascada, donde cada área está conectada a un switch y este al servidor. De esta manera se afectaría el proceso del área afectada.
  Con relación al cableado general de datos éste no se encuentra estructurado y tiene un tiempo de uso de más de 5 años, lo cual significa un riesgo latente para la estabilidad de la trasmisión de datos de la red interna, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema.
- Caída temporal del servidor por falla mecánica: ocasionaría pérdidas totales o parciales, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema. Habría que evaluar el costo de reparación del desperfecto mecánico.
- Pérdida total del servidor: ocasionaría pérdidas totales o parciales, por lo tanto, hay una interrupción en las actividades hasta solucionar el problema y el sistema del SIAF y el SIGA dejarían de funcionar, habría que evaluar el costo de reparación o de reposición, así como el costo en el que se incurriría al no utilizar el sistema.

Sierra Exportadora V° B° Tecnología de Información

Sierra Exportadora V° B° Oficina General de Administración

- Pérdida total o parcial de las estaciones de trabajo: ocasionaría pérdidas parciales, y su reposición estaría sujeta al informe del proveedor al tener una garantía de 2 años por lo tanto, las actividades se interrumpirían hasta solucionar el problema.

Para garantizar que el personal sea consciente de los riesgos, las medidas, y la importancia de velar por la seguridad de información, SIERRA EXPORTADORA asegurará que:

- Los programas de entrenamiento de personal incluirán el tema de seguridad de información.
- El personal se mantenga informado de amenazas, buenas prácticas y procedimientos de control.

5.2 ASIGNACION DE PRIORIDADES

Después de acontecer el o los problemas antes mencionados, tendremos que establecer un orden de prioridades, para poder restablecer los sistemas y así, poder comenzar a operar normalmente, teniendo en cuenta que la institución tiene que estar interconectado permanentemente con el MEF, a través del SIAF y con las sedes descentralizadas a través del correo electrónico y la interconexión VPN.

1. Hacer funcionar los servidores en el siguiente orden:
   - Primero: Encender el controlador de dominio(CDSIERRA) y verificar que se encuentren levantados todos los servicios,
   - Segundo: Encender el servidor de Backup (BKCDSIERRA) y verificar los servicios.
   - Tercero: Encender el servidor de Archivos(FILE)
   - Cuarto: Encender el servidor de Base de Datos(DATABASE)
   - Quinto: Encender el servidor de Seguridad (SIEXFW)
   - Sexto: Encender el servidor de Correo(MAIL)
   - Séptimo: Encender el servidor Web(WWW)
   - Octavo: Encender el servidor Antispam(SCMSERVER)
2. Restablecer los backups si fuera necesario. (Detalle del proceso de Backup)

Se programará el Backup todos los viernes de cada semana según el siguiente criterio de prioridad.

Sierra Exportadora V°B° Tecnología de Información

Sierra Exportadora V°B° Oficina General de Administración

Se programará los backups de acuerdo a las siguientes horas, se recomienda manejar un margen como mínimo de 5 minutos de intervalos entre cada programación de la ejecución de backup y programación de Backups

Controlador de Dominio	1	Hora : 10:55 pm
Correo	2	Hora : 11:00 pm
Archivos	3	Hora : 11:05 pm
Base de Datos	4	Hora : 11:10 pm
Web	5	Hora : 11:15 pm
Backup	6	Hora : 11:20 pm

Almacenamiento de los Logs de Backups

Se almacenaran los logs del backup en la carpeta Reporte de Jobs de Backup que se encuentra en la unidad de disco E: del servidor de backup (BKCDSIERRA) de acuerdo al nombre cada servidor.

Programación y Rutas de los Backups:

Prioridad 1: Servidor Controlador de Dominio (CDSIERRA)

Realizar el Backup según el siguiente orden:

System State, C:\Windows, C:\System Volume Information, C:\Program Files, C:\Document and Settings.

Prioridad 2: Servidor de Correo (MAIL)

Realizar el Backup según el siguiente orden:

System State, E:\Exchsrvr\MDBDATA, Microsoft exchange Server>MAIL>Microsoft Information Store, Microsoft exchange Server>MAIL>Site Replicacion Service, C:\Windows, C:\System Volume Information, C:\Program Files, C:\Document and Settings. E:\System Volume Information.

Prioridad 3: Servidor de Archivos (FILE)

Realizar el Backup según el siguiente orden:

System State, , C:\Program Files, C:\System Volume Information, C:\Windows, C:\Document and Settings, E:\Contratos, E:\System Volume Information, F:\Todo, C:\CDSPIJ

Sierra Exportadora V°B° Tecnología de Información

Sierra Exportadora V°B° Oficina General de Administración

Prioridad 4: Servidor de Base de Datos (DATABASE)

Realizar el Backup según el siguiente orden:

System State, C:\Windows, C:\Base_Datos, C:\BD_SisViaticos, C:\Document and Settings, C:\Program Files, C:\System Volume Information, C:\BK4_BD, E:\Base_Datos, E:\Siaf, E:\STDoc, E:\Reportes ,E:\Aplicaciones, E:\System Volume Information, E:\Instaladores

Prioridad 5: Servidor Web (WWW)

Realizar el Backup según el siguiente orden

System State, C:\Windows, C:\Document and Settings, C:\Program Files, C:\System Volume Information, E:\datasiex, E:\ftp, E:\IntranetSIEX, E:\Pagina Web, E:\System Volume Information

Proridad 6: Servidor de Backup (BKCDSIERRA)

Realizar el Backup según el siguiente orden

System State, C:\Windows, C:\Program Files, C:\Document and Settings, C:\System Volume Information.

3. Restablecer el sistema de Internet y Correo Electrónico, para tener comunicación con el MEF a través del SIAF, y la comunicación con las sedes a través del correo y aquellas que se encuentran interconectadas.

4. Verificar el correcto funcionamiento de los servicios.

5.3 IMPLEMENTACION DEL PLAN DE CONTINGENCIA

La implementación del plan de contingencia está relacionada en su mayoría a la Unidad de Tecnología de Información con respecto a los procesos y/o funciones afectadas de producirse emergencias de los siguientes tipos:

5.3.1- De las Emergencia Físicas

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 siguientes acciones:

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

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.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la institución, 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:

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

- 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.

Error de Tarjeta(s) Controladora(s) de Disco

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

- 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 la posición de la tarjeta controladora.
- Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
- 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.
- Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

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 de Inundación

- 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.
- 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.

Sierra Exportadora V° B° Tecnología de Información

Sierra Exportadora V° B° Oficina General de Administración

Caso de Fallas de Fluido Eléctrico

Se puede presentar lo siguiente:

- Si fuera corto circuito, el UPS mantendrá activo los servidores, mientras se repare la avería eléctrica; hasta un lapso de 20 minutos.
- Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia), solamente a los servidores; hasta que la Unidad de tecnología de Información disponga el corte del servicio de manera correcta y no se produzca daños lógicos y/o físicos en los servidores.
- Cuando el fluido eléctrico de la calle se ha restablecido se procederá a restaurar los servicios en el orden establecido para el correcto funcionamiento de los servidores.

5.3.2.- De las Emergencias Lógicas de Datos

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:

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.

2 Deshabilitar el ingreso de usuarios al sistema.

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

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

5 Al término de la operación de reparación se procederá a habilitar entradas a

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

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 de Virus

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

Para servidor:

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

Para estaciones de trabajo:

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

- Utilizar un disquete que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado. Reiniciar el computador con dicho disquete.
- Retirar el disquete con el que arrancó el computador e insertar el disquete antivirus, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el scaneado, reconstruir el Master Boot del disco duro

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

5.4 DISTRIBUCION DEL PLAN DE CONTINGENCIA

El presente Plan de contingencias se distribuirá a todos los empleados de la institución, quienes estarán en la obligación de cumplir con los procedimientos establecidos al presentarse alguna contingencia.

En caso de modificarse el plan de contingencia, se actualizarán todas las copias de cada uno de los empleados, y se procederá a la destrucción de la copia anterior, para unificar la información.

6. POLITICAS Y MEDIDAS DE SEGURIDAD DE INFORMACION

La 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 esta institución, 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.

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.

El objetivo de seguridad de información es proporcionar un ambiente confiable al mismo tiempo proteger recursos de información y asegurar la continuidad y la razón de ser de la institución, previniendo y minimizando el impacto de incidentes de seguridad. Las directrices de seguridad de información tienen los siguientes componentes básicos que deben mantenerse en todo momento:

- **Confidencialidad**: protegiendo la información sensible de exposición o intercepción no autorizada.
- **Integridad:** salvaguardando la exactitud e integridad de información y software de los computadores.
- **Disponibilidad:** asegurando que esa información y los servicios esenciales estén disponibles a los usuarios cuando sean requeridos.
- **Autenticidad**: asegurando que la información fue enviada por el originador.

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

En Sierra Exportadora estamos todos comprometidos a:

- Construir confianza entre colegas para permitir que nuestra información se comparta de manera segura tan ampliamente como sea posible.
- Salvaguardar nuestra información sensible y los servicios esenciales IT de las amenazas potenciales de seguridad.
- Prepararnos para mantener "la continuidad del negocio" a lo largo de posibles fallas en IT o desastres que afecten el ambiente de oficina.

Lograremos esto mediante:

- Manteniendo un conocimiento de los riesgos de seguridad para la información y los servicios IT.
- Evaluando riesgos e identificando requerimientos de seguridad antes de desarrollar o usar nuevos sistemas IT por guardar o comunicar información confidencial.
- Manteniendo a todo el personal informado sobre los procedimientos de seguridad y cualquier amenaza de seguridad que podrían afectarlos.
- Controlando estrictamente el acceso a la información y sistemas IT por personal ajeno a sierra Exportadora según las necesidades de la institución y políticas de acceso.
- Manteniendo los planes de continuidad para los procesos críticos del negocio.
- Revisando la aplicación de medidas de seguridad y conduciendo un programa anual de mejoramiento en seguridad de información.
- Exigiendo que toda organización que comparta información y servicios IT con Sierra Exportadora se adhiera a las políticas y estándares de nuestra institución.
- Tratando las faltas deliberadas de seguridad como un asunto disciplinario serio.

Sierra Exportadora Vº Bº Tecnología de Información

A continuación la relación de políticas de seguridad:

Sierra Exportadora Vº Bº Oficina General de Administración

6.1. POLITICA DE CONTROL DE ACCESO A LA INFORMACION:

Acceso a los sistemas de información de la institución de Sierra Exportadora representa riesgos de seguridad tanto para los sistemas de información como para la infraestructura IT que los soporta. El propósito de esta política es entregar las pautas que permitan conceder acceso a los sistemas de información de Sierra Exportadora a través de la infraestructura IT local.

La política permitirá:

- Proveer consistencia cuando se permita acceso a terceros a las aplicaciones y sistemas de información.
- Ofrecer las bases para identificar los mecanismos de control de acceso apropiados.
- La alineación con las políticas de control de acceso por Dominio del Grupo.
- Mantener un equilibrio apropiado entre el acceso eficaz a la información y la seguridad de la información como un activo.

El acceso a la información y aplicaciones debe concederse con base en un beneficio claramente definido para la institución, bajo las siguientes reglas:

1. Debe concederse acceso a la información y aplicaciones de acuerdo con la clasificación de seguridad de la información a ser accedida.
2. Se aplicarán controles de acceso de acuerdo con las políticas de seguridad y normas asociadas con los servicios a ser accedidos.
3. Las condiciones y derechos de acceso deben ser claramente especificados en los contratos y acuerdos de nivel de servicio con terceros.
4. El cumplimiento de las condiciones de seguridad deberá ser supervisado.

Del acceso al dominio de red:

En principio, solo usuarios autorizados pueden acceder a los servicios de información de Sierra Exportadora desde cualquier localización por la naturaleza de su trabajo. La realización de esto dependerá de la disponibilidad de los controles adecuados, los cuales serán aplicados de acuerdo con las siguientes reglas:

1. El acceso general dentro del dominio de Sierra Exportadora es de manera controlada, regiendose bajo politicas de seguridad, otorgando los privilegios y permisos autorizados a los servicios y aplicaciones con los se que cuenta la Red.
2. La información y servicios sensibles se agruparán en ambientes de red lógicamente separados los cuales tendrán controles de acceso adicionales.
3. El acceso a la infraestructura IT de sierra Exportadora será controlado. Esto incluye, control de acceso tanto de terceros.

De los procesos:

- Alcance del acceso. Debe existir un proceso formal parar definir claramente los requisitos del negocio (alcance) que demanden acceso a los sistemas de información.
- Autorización. Debe haber un proceso de autorización formal implementado para conceder acceso a los sistemas de información y aplicaciones de Sierra Exportadora.

6.2. POLÍTICA DE PRIVILEGIOS DE USUARIO

Descripción

Esta política de privilegios de usuario es una política interna del TI y define los privilegios que se les permite tener en la red de organización a los distintos usuarios, en concreto define qué grupos de usuarios tienen privilegios para instalar los programas en su propio ordenador u otros sistemas. Esta política define los usuarios que tienen accesos y control de datos sensibles o regulados.

Esta política define el acceso a Internet, a los sitios específicos para algunos usuarios u otras formas en que pueden o no pueden utilizar sus sistemas informáticos.

Finalidad

Esta política está diseñada para minimizar el riesgo a los recursos de la organización y a los datos mediante el establecimiento de privilegios de usuarios, de datos y a los equipos de la red a la mínima admisible, al mismo tiempo en que permite a los usuarios a realizar funciones de trabajo sin inconvenientes.

Sierra Exportadora V°B° Tecnología de Información

Sierra Exportadora V°B° Oficina General de Administración

Privilegios de Equipo local

Hay tres categorías principales de usuarios o red. Estas categorías incluyen:

1. Usuario Restringido - Puede operar en la computadora y guardar documentos, pero no puede guardar la configuración del sistema.

2. Usuario Estándar (usuario) - Puede cambiar muchos ajustes del sistema e instalar programas que no afectan a los archivos del sistema de Windows.

3. Administradores - Disponen de un acceso completo a leer y escribir datos en el sistema y añadir o eliminar cualquier programa o cambiar la configuración del sistema. La mayoría de los usuarios de las redes más comunes se debe restringir a los usuarios en sus equipos locales. Sólo los usuarios con una formación especial o de una necesidad de acceso adicional se les debe permitir cambiar la configuración del sistema e instalar programas que no son programas del sistema operativo. Esto se debe a que muchos virus o software espías, pueden ser instalados de una forma sutil para engañar al usuario o la instalación puede ser totalmente transparente para el usuario de la computadora. Si el usuario no tiene la capacidad de instalar programas o cambiar la configuración a unos ajustes más vulnerables, la mayoría de estos posibles problemas de seguridad se pueden prevenir.

Por lo tanto, sólo los usuarios que demuestren una necesidad y habilidad por la capacidad del usuario o administrador en los equipos locales se les han permitido este nivel de acceso. Tras la demostración de una necesidad especial de acceso adicional, el administrador de TI debe aprobar antes de que el acceso pueda hacerse efectiva. Grupos que pueden permitirse este tipo de acceso son:

1. Los administradores de dominio

2. Escritorio de Ayuda personal

3. Desarrolladores de aplicaciones con fines de prueba que han desarrollado capacitación o habilidades.

Privilegios de Red

La mayoría de los usuarios de la red tendrán acceso a los siguientes tipos de recursos de red.

1. Correo electrónico - La mayoría de los usuarios tendrán acceso completo a su propio correo electrónico. Que no será capaz de transferir la propiedad a otra persona.

2. Una unidad de red personal en un servidor de archivos en red - Se trata de una carpeta en una unidad que sólo el usuario principal de esta unidad puede leer y escribir, de dominio exclusivo de los administradores. El usuario no podrá transferir la

Sierra Exportadora V° B° Tecnología de Información

Sierra Exportadora V° B° Oficina General de Administración

propiedad a otra persona.

3. Un grupo o unidad de la división de organización - Esta es una carpeta que los miembros de determinados grupos o divisiones en la organización pueden tener acceso. El acceso permite leer o escribir y puede variar según necesidades de la organización.

4. Acceso a bases de datos - Puede haber otras bases de datos que pueden almacenarse en una unidad compartida o en algún otro recurso. La mayoría de las bases de datos tendrá un estándar a nivel de usuario que proporciona a los usuarios permisos apropiados para ingresar datos y ver información. Sin embargo, sólo los administradores de la base de datos tendrán pleno acceso a todos los recursos sobre una base de datos. Los administradores de la base de datos sólo tendrán pleno acceso a la base de datos que administran.

Grupos a los que se permitió los accesos adicionales incluyen:

1. Operador de copia de seguridad - Permitido para leer los datos en el dominio con el fin de salvar los archivos de copia de seguridad de los medios de comunicación. Este grupo no puede escribir todos los datos en el dominio.

2. Operador de cuenta - puede gestionar y ver la información acerca de cuentas de usuario en el dominio.

3. Operador del Servidor - Tiene todos los privilegios en los servidores, incluyendo lectura y escritura de datos, instalar programas y cambiar la configuración.
4. Administrador de dominio - Tiene todos los privilegios sobre todos los equipos del dominio incluyendo servidores y estaciones de trabajo. Los privilegios incluyen la lectura y la escritura de datos, instalar programas y cambiar la configuración.

Aplicación

Sierra Exportadora Vº Bº Tecnología de Información

Dado que la seguridad en los datos y la integridad, junto con la protección de los recursos es fundamental para el funcionamiento de la organización, los empleados que no adhieren a esta política puede estar sujeto a acciones disciplinarias hasta e incluyendo el despido.

Sierra Exportadora Vº Bº Oficina General de Administración

6.3. POLITICA DE USO DE PC:

Comprende el establecer el procedimiento del uso de los computadores, impresoras (hardware), aplicaciones y herramientas (software) propiedad de la institución, asignados a los empleados de la institución.

Alcanza a todos los usuarios que se conectan a la red de Sierra Exportadora a través del computador y a cualquiera de los Servicios IT.

La política de uso de hardware y software se establece para todos los empleados con cualquier tipo de contrato temporal o directo, y que por razones de su función tienen acceso a un computador, sus herramientas y aplicaciones, propiedad de la institución.

Esta política se establece con el fin de hacer más eficiente la administración y desempeño de los recursos de información y tecnología, estableciendo un marco de operación ético y profesional.

Los computadores, impresoras (hardware), aplicaciones y herramientas (software) propiedad de la institución están habilitados para conectarse a la red de Sierra Exportadora, teniendo en cuenta que se hace para propósitos de la institución y bajo las políticas y normas de Seguridad IT de la institución

El computador ya tiene instaladas las aplicaciones y herramientas (software) necesarias para realizar sus actividades, siendo estos los recomendados y licenciados por Sierra Exportadora.

Se restringe la instalación de cualquier componente de hardware o software al equipo asignado por la institución, a excepción de lo justificado por la administración y aprobado por la Unidad de tecnología de Información.

La Política permitirá:

- Todo dispositivo de conexión a red debe ser aprobados por el responsable de Infraestructura IT en cada localidad. En particular, los módems NO deben conectarse a la red de computadores sin autorización expresa de IT.
- De acuerdo con las políticas de la institución, los computadores están asegurados bajo una póliza. Lo cual no excluye ni deja sin responsabilidad a los empleados de la guarda y custodia de los computadores asignados.
- Acceso a los sistemas de información y aplicaciones debe ser autorizado por la Administración en coordinación con la Unidad de tecnología de Información.
- Los empleados de la institución deben tener en cuenta que están sujetos a normas legales que pueden afectar sus labores diarias, tales como la protección de los datos, la legislación de derechos de propiedad intelectual y actos de mal uso de los computadores a su cargo.

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

Políticas relacionadas

- Contrato de Trabajo
- Pólitica Marco de Seguridad IT
- Política Escritorio Limpio
- Política Acceso Internet
- Política Uso Password

6.4. POLITICA DE ACCESO A INTERNET

El acceso a Internet es únicamente para uso exclusivo y en beneficio de los objetivos de la institución.

El acceso a Internet está permitido solamente a través de la red de Sierra Exportadora, y por ningún motivo debe haber dispositivos conectados a la red que permitan acceso a Internet sin autorización de la Unidad de Tecnología de Información.

Responsabilidades del usuario

Es responsabilidad del usuario utilizar los servicios de Internet exclusivamente en función de negocios de la institución, acatando las siguientes reglas:

- El servicio de correo (e-mail) por internet no se usará para intercambiar información "confidencial" de la compañía, o información crítica que requiera una entrega garantizada (es posible que utilizando este servicio los mensajes puedan ser interceptados y alterados).
- Una excepción al punto anterior es emplear un método seguro autorizado por IT (ej. Redes Privadas Virtuales VPN)
- El código y contraseña asignados a cada usuario para permitir acceso a Internet no podrán ser usados para propósitos personales.
- Transacciones comerciales de Sierra Exportadora no son permitidas vía Internet (compras, órdenes, pagos, etc.) a menos que se tomen medidas de seguridad apropiadas.
- Todas las comunicaciones vía Internet serán hechas en una manera "profesional" siguiendo la Política de Comunicaciones de Sierra Exportadora.

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

- Todo software bajado de Internet debe ser verificado por la Unidad de tecnología de Información para examinar posibles virus, códigos maliciosos, y debe tener un licenciamiento requerido antes de instalarse en su equipo de trabajo. Es recomendable bajar el software de vendedores confiables (por ejemplo, SUN, Microsoft, IBM, etc).
- La política de derechos de propiedad de Sierra Exportadora debe ajustarse a: solamente software comprado por Sierra Exportadora puede ser cargado como activo propio de la institución.

Es responsabilidad de todos los Gerentes de Línea, verificar periódicamente el cumplimiento de las pautas anteriores.

Uso apropiado de internet

El acceso a Internet es considerado apropiado mientras su uso está relacionado con la razón de ser de la institución y es necesario para el desarrollo de las actividades del empleado.

Las siguientes pautas explican porque los Procedimientos de Comunicación del Negocio llaman la atención en el "cuidado extra que se deben tener al utilizar sistemas públicos".

- Todo uso de Internet no debe hostigar, calumniar, o destruir operaciones de otros.
- Todo uso de Internet debe seguir leyes y regulaciones, incluyendo aquellas como:
  - Controlar la importación y exportación de tecnología, software y datos.
  - Restringir el uso de tecnología de telecomunicaciones y encripción.
  - Controlar la transmisión de datos personales a través de fronteras nacionales.

- Todo uso de Internet debe obedecer las leyes de derechos de autor.
- La información transferida en Internet no es segura por naturaleza. El personal nunca debe transferir información confidencial para la institución que clasifique como personal-confidencial.
- Cuando accede a Internet usando una cuenta de Sierra Exportadora, el usuario representa a Sierra Exportadora; por tanto, su uso debe ser apropiado y su conducta debe ser profesional.
- Utilizar programas de Internet solamente es posible como último recurso, con la autorización de la UTI y de acuerdo con la Política de Seguridad de Información

Sierra Exportadora Tecnología de Información V° B°

Sierra Exportadora Oficina General de Administración V° B°

de la institución.

- Programas adquiridos o copiados de fuentes externas pueden contener virus perjudiciales. Personal que recibe archivos ejecutables y/o binarios es individualmente responsable de tomar las medidas apropiadas para asegurar que estos archivos sean seguros previo a su ejecución.
- Internet proporciona al personal las oportunidades de transmitir datos o software que pueden estar sujetos a derechos de propiedad literaria, a menudo bajo la ley americana. Personal que usa software o datos de Internet debe estar consciente en todo momento del respeto a los derechos de propiedad literaria de cualquier restricción contractual y normas de la compañía. Aquellos que violen estos derechos de propiedad literaria pueden estar sujetos a acusaciones (tanto la institución como el personal empleado) - y también pueden estar sujetos procedimientos disciplinarios internos en la institución.

- El personal de la institución no debe asumir que, cuando se tiene acceso a Internet, un anuncio o una red está libre de cualquier derecho de propiedad o restricciones de licencia. Uno de los problemas legales es que la licencia debe ser controlada por la ley del país del proveedor, y no de la ley del país en el cual el software es usado. Esto involucrará un riesgo tangible de cualquier compañía estando sometido a un número de legislaciones, muchas desconocidas y no bien desarrolladas.
- Software libre y software de domino público, es software que está disponible sin ningún costo, regularmente a través de boletines electrónicos. Los programas de libre acceso incluyen versiones de demostración de software comercial el cual ofrece un subconjunto restringido del paquete para la venta. Es frecuente adquirir copias "limpias" de software libre de fuentes comerciales. El software tomado de dominio público no es pago y es usado a riesgo propio. La diferencia principal entre software de dominio público y el libre radica en que el autor de software de dominio público pierde los derechos de propiedad cuando el software es colocado en el dominio público mientras el autor de programas compartidos aún conserva estos derechos. Programas compartidos son a menudo adquiridos de la forma "véalo y úselo si aplica". El pago es solamente requerido si el usuario encuentra utilidad en el producto. La institución no acepta responsabilidades por resultados derivados del software libre o programas compartidos.
- El contenido de cualquier base de datos accedida desde Internet, puede ser usado solamente en convenio con los derechos de propiedad de autor. El convenio normalmente especificará cuáles datos pueden ser usados. Además, transmisiones de datos de una base de datos a través de sistemas de telecomunicaciones (aún dentro de las premisas de la compañía) está prohibido a menos que se hayan recibido permisos del autor autorizando hacer esto.

Los siguientes son ejemplos de acciones o actividades que pueden terminar en

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

acciones disciplinarias. No es una lista completa. Las acciones disciplinarias pueden ser desde advertencias verbales hasta la terminación del contrato dependiendo la severidad de la acción:

- Usar los recursos y tiempo de Sierra Exportadora para beneficios personales.
- Enviar mensajes con amenazas, atormentar racialmente, o acosar sexualmente.
- Hurtar o copiar archivos electrónicos sin autorización.
- Enviar o anunciar materiales confidenciales fuera de la institución o internamente a personal no autorizado.
- Negarse a cooperar con investigaciones.

Uso inapropiado de internet

El uso de acceso a Internet en Sierra Exportadora es inapropiado cuando:

- Contradice cualquiera de los puntos contemplados en la sección anterior.
- Se viola la privacidad del usuario y sus datos personales.
- Se alteran o dañan los datos o programas almacenados en su equipo.
- Se alteran de forma intencional los sistemas o recursos de la red.
- Se usa o copia software propietario sin que el usuario esté autorizado para ello.
- Usar la red de la institución y el acceso a Internet como un canal para intentar acceder otros sistemas de cómputo o equipos tanto en redes internas como externas.
- Curiosear en forma excesiva y no autorizada el acceso a otros equipos empleando métodos incorrectos.

Control de uso de internet

Sierra Exportadora provee el acceso a Internet para facilitar comunicaciones institucionales y recolección de información. Este servicio es proporcionado para el uso de información legítima, en el transcurso de las labores asignadas únicamente. El uso inapropiado de este servicio puede terminar con la pérdida de privilegios de acceso e incluso acciones disciplinarias. Dentro de sus funciones, personal autorizado de la Unidad de Tecnología de Información y Gerentes de Línea pueden controlar el uso de acceso a Internet o revisar el contenido de los archivos transmitidos (enviados o recibidos) por este medio.

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración

6.5. POLITICA DE USO DEL CORREO ELECTRONICO (E-MAIL)

El correo electrónico es una herramienta vital en el negocio de hoy. Su uso está creciendo rápidamente y necesitamos usarlo ahora con mayor disciplina y efectividad. No tiene que ahogar a todos - el correo electrónico más eficaz es corto, claro y pertinente.

El correo electrónico es de uso exclusivo por el personal autorizado y para sus actividades relacionadas con los intereses de Sierra Exportadora.

Política de Sierra Exportadora

Lo que se espera de usted	Lo que usted puede esperar de sus colegas
Acceda por lo menos una vez al día su correo electrónico.	Respeto de su tiempo personal no asumiendo que leerá mensajes durante fines de semana y feriados
Mantenga contacto a través de "acceso remoto" si es viajero frecuente.	Selectividad en lo que le envían para que cuente con suficiente tiempo para responder.
Permita a los colegas saber cómo se mantendrá en contacto mientras está por fuera.	Lectura y respuesta de los mensajes que usted envía
Codifique los mensajes con prioridades: Personal, Confidencial o Alta Prioridad, según el caso.	Acuso de recibo de mensajes de Alta Prioridad en el mismo día laboral.
Siga este código de conducta en todo momento y anime a otros a hacerlo.	Mantenimiento de la privacidad, confidencialidad e integridad de notas que usted ha enviado.

Un tiempo y un lugar para todo

Si bien es cierto que el correo electrónico es el método de comunicación preferido puesto que está al alcance inmediato del usuario, éste es esencial para cartas cortas, mensajes y documento/intercambio de información. Pero existen otros medios más eficaces en algunos casos, como:

- El contacto personal o la llamada telefónica.
- El contacto directo en caso de emergencia o cuando se necesite respuesta inmediata.
- Cuando se manejan volúmenes grandes de información.
- Cuando se comparten sistemas de almacenamiento de información (carpetas, servidores o sistema de manejo de documentos) con otros de su equipo de trabajo.

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina Ocoa de Administración

- Cuando se trata de información general que puede ser publicada en un boletín o en la Web de Sierra Exportadora.

Obligaciones del Remitente

- **¿Para qué es el correo electrónico?** Declare el propósito de su mensaje claramente. Dígale a las personas si es para acción o para información. Generalmente la lista de Para: indica que usted está pidiendo una acción y la lista de Cc: significa para información.
- **¿Quién realmente necesita recibir esto?** No sobrecopie - sólo copie a aquellos que realmente necesitan saber. Nunca envíe a más de una persona para acción (Para:) a menos que quiera que todos tengan una acción.
- **¿Recibirá su mensaje el nivel correcto de atención?** Use títulos significativos y señale prioridad. Tenga en cuenta que la señal de prioridad puede perderse por los distintos sistemas de correo electrónico, así que incluya la prioridad en el título del mensaje cuando envía a través de Internet.
- **¿Cómo comunicar mejor el mensaje?** Es su responsabilidad comunicar su mensaje - mírelo a través de los ojos del destinatario. Un mensaje en correo electrónico claro es corto y puntual, idealmente no más de una pantalla. Si usted no puede hacer esto, entonces resuma en el primer párrafo.
- **¿Cuándo hacer seguimiento?** No asuma que un destinatario ha aceptado una acción porque ha leído su mensaje. Permita un tiempo razonable para leer y responder. Reconozca los fines de semana, los días de fiesta y las horas en las distintas zonas alrededor del mundo.
- **Enviando un anexo**. Evite enviar anexos grandes o numerosos - comprímalos para que sean leídos rápidamente y para usar la red eficazmente. Dé nombres significativos a los anexos y diga lo que ellos contienen.
- **Chequeo final antes de enviarlo**. ¿Son estas las listas correctas de Para y Cc ? ¿Está claro el contenido y las acciones? ¿Hay algo que sería mejor dejar por fuera? ¿Desea poner una fecha de vencimiento en el mensaje para ayudar al destinatario a manejar su buzón de entrada?

Sierra Exportadora Vº Bº Tecnología de Información

Sierra Exportadora Vº Bº Oficina General de Administración