2.- SOLUCIÓN PROPUESTA Y PLAN DE CONTINGENCIAS

De acuerdo al análisis de riesgos y a la revisión de seguridad realizada, se presentan las sugerencias de los casos para combatir cada uno de los riesgos potenciales a los que se enfrenta la red informática de SASF.

2.1 RECOMENDACIONES CONTRA LA ACCIÓN DE VIRUS

Según lo mostrado en la situación actual en la sección de esquema de antivirus, es necesario estandarizar el software de antivirus en todas las estaciones de trabajo y servidores. Es aconsejable tener un proveedor de software antivirus para las estaciones y otro diferente para el servidor, para reducir la probabilidad de que un virus que no este en la lista de actualización, se filtre en toda la red.

Se sugiere que en las estaciones de trabajo se siga con la línea de Symantec (Norton Antivirus) y en el servidor central instalar McAfee. Optamos por Norton Antivirus ya que en la mayoría de las estaciones ya

se encuentra instalado este producto y es recomendable instalar el McAfee por la funcionalidad que brinda la consola de administración de la versión para servidores. Si no se opta por alguno de estos productos se tendría que analizar que el producto que se escoja no afecte el software instalado para las actividades que realiza la empresa.

El porque tener 2 antivirus diferentes, uno para el servidor y otro para las estaciones de trabajo es porque estos tienen variaciones en sus tablas de definiciones de virus, es más difícil que un virus se propague por la red debido a la diversificación de productos que puedan detectarlos.

Es necesario implementar un procedimiento para las actualizaciones automáticas de las definiciones de virus, tanto para Norton como para Macfee. Esta labor la debe realizar el administrador de red, cuidando que se ejecute en horas en que no se degrade el performance del tráfico de red.

2.2 RECOMENDACIONES CONTRA ACCESOS NO AUTORIZADOS

Frente a este riesgo potencial, es necesario implementar lo siguiente:

2.2.1 RECOMENDACIONES A NIVEL FÍSICO

- El servidor de archivos no debe ser accesible físicamente a cualquier persona.
- Es conveniente que exista un espacio físico donde se ubique el servidor, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su funcionamiento, como temperatura ambiental adecuada, aislado del polvo y plagas dañinas.
- En este espacio, además de ubicar el servidor, se pueden ubicar los elementos más sensibles de la red corporativa como el HUB/Switch y el servidor proxy.

2.2.2 RECOMENDACIONES A NIVEL LÓGICO

- Habilitar un firewall que evite ingresos desde redes externas hacia la red corporativa. Para la implementación del mismo presentamos las siguientes opciones:

  La primera opción consta de configurar adecuadamente el firewall que viene incluido con el sistema operativo Linux Suse 8.0.

La segunda opción seria adquirir un hardware de seguridad que entre sus características tenga implementado un firewall, el hardware sugerido es el siguiente: SGS360 APPLIANCE. Para más detalles del producto, ver anexos C.

La recomendación de hardware incrementaría los costo de seguridad los cuales se verían justificados por la posible expansión de la empresa.

- Instalar un sistema de detección de intrusos para monitorear los accesos o tentativas de accesos a la red corporativa para esto presentamos a continuación dos opciones:

  La primera opción es un software de IDS instalado en el servidor proxy de la red. Este puede ser **LIDS** (Linux Intrusión Detection System), que es un parche del kernel de Linux que permite implementar funcionalidades de IDS al sistema operativo, y debido a ser open source, no tiene costo.

La segunda opción es utilizar el IDS que esta implementado en el SGS360 APPLIANCE de Symantec.

- Deshabilitar los servicios que no sean necesarios y luego de esto verificar los posibles puertos que se encuentren abiertos innecesariamente para proceder a cerrarlos. Esta información se encuentra detallada en la situación actual (capítulo 1).
- Concienciar a los usuarios de la red, se deberá concienciar a los usuarios de la red, acerca de una política mínima de seguridad, por ejemplo, evitar las claves fácilmente descifrables. Esta información se encuentra detallada en las políticas de seguridad informática (capítulo 3).
- Solo esta permitido instalar en las computadoras el software requerido para el desarrollo de las actividades de la empresa, para esto se contará con un listado de dicho software, el cual deberá ser seleccionado por la Gerencia y jefes de área. Debido a que en SASF el servidor de Base de Datos y de archivos en ocasiones es al mismo tiempo una estación de trabajo, es fácil que se produzca pérdida de información. Es por esta razón que no se debe de instalar herramientas de desarrollo como lenguajes de programación y compiladores.
- Teniendo presente que la mayoría de los ataques informáticos no

vienen de fuera, sino de dentro, según lo indican las estadísticas de penetración a las redes corporativas expuestas en el anexo D, un usuario interno podría capturar contraseñas con una herramienta sniffer.

Para evitarlo, es conveniente que la red, en lugar de estar basada en un HUB, esté basada en conmutador (SWITCH).

Eso evitará que todos los paquetes de información lleguen a todas las tarjetas de red. Usando una red conmutada puede evitar muchos intentos de espionaje de la información que circula por la red.

- Es recomendable agregar contraseña del BIOS a todos los equipos de la red, para evitar vulnerabilidades de acceso dependientes de los Sistemas Operativos Instalados.

2.3 RECOMENDACIONES PARA PREVENIR FALLAS EN LOS EQUIPOS

- La primera opción será designar a uno o más empleados a que

dediquen un tiempo para el aprendizaje y formación, mediante la toma de un curso, para que ellos sean los encargados en brindar mantenimiento preventivo y correctivo a los equipos que posee la empresa.

Como otra opción sugerimos el contratar los servicios de una empresa que de forma periódica realice mantenimiento preventivo a los equipos y correctivo si lo amerita la situación.

Sea la decisión que se que se escoja se sugiere que como mínimo se realice por lo menos una vez al año y llevar un control, de la vida útil de los diferentes dispositivos.

- Para evitar el caos que provocaría una avería en el servidor de archivos, o en uno de sus discos duros, plantéese la utilización de un cluster.

- Un sistema de alimentación sin interrupciones (UPS) es hoy en día imprescindible, al menos para el servidor de archivos, el servidor proxy y el HUB/Switch.

- Al llevar un control de lo instalado mediante las listas de software se recomienda que todo nuevo software que se piense instalar sea probado en un computador que posea el software estándar para las actividades de la empresa con la finalidad de confirmar que este nuevo software no afectara a las otros ya instalados.

2.4 RECOMENDACIONES CONTRA EL ROBO DE DATOS Y FRAUDE

2.4.1 MEDIDAS PREVENTIVAS CONTRA EL ROBO DE DATOS

El conocimiento de las señales y los métodos de robo ayudarán a los jefes de área a estar más conscientes de posibles problemas. Aunque las estadísticas de robo de empleados son alarmantes, SASF puede defenderse implementando medidas preventivas como:

- Publicar la Política de Seguridad de la empresa.
- Promover el concepto de responsabilidad del empleado.
- Capacitar a los empleados para estar en alerta ante ladrones (y que vean la importancia del robo a la empresa)
- Entrevistar bien a los postulantes.
- Exigir certificado de antecedentes.
- Revisar bien sus referencias.

- Capacitar bien a los empleados nuevos en los procedimientos.
- Dar énfasis a las políticas de seguridad de la empresa.
- Mantener la puerta trasera cerrada.
- Mantener un ambiente de trabajo limpio y ordenado.
- Desarrollar buenos canales de comunicación con los empleados para resolver quejas.
- Capacitar a los empleados para que tengan una carrera profesional dentro de la empresa.
- El liderazgo - el jefe debe poner el ejemplo en seguir las normas.
- Ser duro con los empleados que roban, como ejemplo a los demás.

2.4.2 CÓMO PREVENIR ATAQUES DE INGENIERÍA SOCIAL

Para comprobar si se están realizando ataques de este tipo se recogerán estadísticas de incumplimiento de procedimientos. Por ejemplo, analizar el número de personas que han llamado a la empresa y que no se les ha entregado la información porque no proporcionaban todos los datos de identificación solicitados. Poder reconocer ciertas señas típicas de una acción de esta naturaleza, como son rehusarse a entregar información de contacto, tener mucho apuro, referenciar a una persona importante, intimidación o requerimiento de información olvidada, por enumerar las más comunes, es claramente otra manera de estar alertas. De cualquier

forma, en la actualidad, es vital educar, capacitar, sensibilizar sobre las políticas y procedimientos definidos y que son relativos a este tema.

Una forma de defensa contra estos ataques es conocer los conceptos básicos que pueden ser utilizados contra una persona o la compañía a la que pertenece y que abren brechas para conseguir datos. Con este conocimiento se debe adoptar una actitud proactiva que alerte y concienciar a los empleados que avisen de cualquier pregunta o actitud sospechosa. Eso sí, las políticas de seguridad deben ser realistas con reglas concisas y concretas que se puedan cumplir.

2.4.3 PROTECCIÓN PARA CORREO CORPORATIVO

Se recomienda el uso de una herramienta que permita implementar infraestructura de clave pública para proteger la comunicación por correo electrónico que implique el envío de información confidencial.

Unas de las herramientas recomendadas para este propósito es el Lotus Notes Domino para Windows.

2.5 RECOMENDACIONES SOBRE COMO REALIZAR LAS ACTUALIZACIONES DE PARCHES DE SEGURIDAD

Como complemento a las sugerencias anteriores, es recomendable estar al día con la instalación de los diferentes parches de seguridad para el software de la empresa.

Debido a que la mayoría de equipos funcionan bajo ambiente Microsoft, es conveniente instalar un servidor SUS[1], que realice las funciones de actualización de los parches de seguridad de los sistemas operativos Windows instalados en la red. Para esto se configuraría el servidor central para que descargue las actualizaciones y las almacene en disco duro, luego los clientes (estaciones de la red) automáticamente realizarían la actualización conectándose a este servidor. Este proceso se debería ejecutar en horarios que no afecten el desempeño de la red.

También se deben descargar los parches de seguridad para las demás aplicaciones que se utilizan en la empresa, como los productos Oracle, de

[1] SUS: Software Update Services (Servicios de Actualización de Software).

manera que sé este al día con las correcciones de las vulnerabilidades existentes.

Las recomendaciones de lo que debe realizarse en el caso de presentarse una contingencia como fuego, terremoto o un robo físico, se las podrá encontrar a continuación en el plan de contingencias.

2.6 PLAN DE CONTINGENCIAS

El Plan de Contingencias o Emergencias, constituye el instrumento principal para dar una respuesta oportuna, adecuada y coordinada a una situación de emergencia causada por fenómenos destructivos de origen natural o humano.

Sin embargo, es fundamental contar con la suma de esfuerzos, de todos, cuya composición permita fortalecer y cumplir en tiempo las acciones tendientes a prevenir y mitigar desastres en modo y tiempo las circunstancias señaladas y dar respuesta oportuna a las contingencias que se presenten.

Es por ello que se presenta en el siguiente plan, las actividades a tomar en cuenta por cada uno de los colaboradores de SASF, tanto antes, durante y después de la contingencia.

2.6.1 ACTIVIDADES PREVIAS AL DESASTRE

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, las cuales nos asegurarán un proceso de Recuperación para SASF con el menor costo posible. A continuación detallaremos las siguientes a realizar:

Establecimiento de plan de acción

En esta fase de planeamiento se debe de establecer los procedimientos y normas a seguir relativos a:

a) Instalaciones físicas de la empresa

En caso de que se pueda suscitar un robo, sismo o incendio se deberían tomar las siguientes medidas preventivas:

Robos:

- Al entrar y salir de las instalaciones se deberá observar previamente de que no exista ningún individuo sospechoso.

- Queda prohibido dar información personal de los empleados o información confidencial de la organización.
- Contar con personal para resguardo de las instalaciones de la empresa.
- Instalación de alarma.
- Contratar con pólizas de seguros

Sismos:

- Ubicar y revisar periódicamente, que se encuentren en buen estado las instalaciones de AGUA, y SISTEMA ELECTRICO.
- Fijar a la pared repisas, cuadros armarios, estantes, espejos y libreros. Evitar colocar objetos pesados en la parte superior de éstos, además asegurar al techo las lámparas.
- Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín, de ser posible un radio portátil y una linterna con pilas.
- Todo el personal debería portar siempre una identificación.
- Realizar simulacros de manera periódica.

Incendios:

- Estar siempre alerta. La mejor manera de evitar los incendios, es la prevención.
- Procurar no almacenar productos inflamables.
- Cuidar que los cables de los aparatos eléctricos se encuentren en perfectas condiciones.
- No se deben realizar demasiadas conexiones en contactos múltiples, para evitar la sobre carga de los circuitos eléctricos.
- Por ningún motivo mojar las instalaciones eléctricas. Recuerde que el agua es un buen conductor de la electricidad.
- Todo contacto o interruptor debe tener siempre su tapa debidamente aislada.
- Antes de salir de SASF la ultima persona en hacerlo, deberá revisar que los aparatos eléctricos estén apagados o perfectamente desconectados.
- Que prohibido fumar en las instalaciones de SASF debido a que este habito contaminante, no deja una buena impresión en los clientes y puede causar desagrado ante los no fumadores o puede causar un incendio.
- Bajo ningún motivo se debe sustituir los fusibles por alambre o monedas, ni usar cordones eléctricos dañados o parchados.
- Contar con una alarma de incendios.

- Tener en un lugar visible y accesible un extintor contra incendios.
- Realizar simulacros de manera periódica.
- Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín.

b) Sistemas e información

En SASF no se cuenta con sistemas de información que manejen los datos de la empresa. La información importante de la empresa se encuentra almacenada en un servidor central y detalla a continuación:

Nombre	Equipo	Path	Propósito	Tamaño
Sasf_corporativo	Desa11	C:\Sasf_compartido\Sasf_corporativo	Información administrativa	2 GB
Sasf_aplicaciones	Desa11	C:\Sasf_compartido\Sasf_aplicaciones	Información de productos desarrollados	2 GB
Manuales	Desa11	C:\Sasf_compartido\compartido\manuales	Manuales en general	2 GB

Cursos	Desa11	C:\Sasf_compartido\Curso	Cursos dictados	100 M
Users	Desa11	C:\Sasf_compartido\compartido\users	Información de los colaboradores	2GB

Tabla #10 Información crítica de la empresa

c) Equipos de cómputo

Inventario actualizado de los equipos de manejo de información (computadoras, impresoras, etc.), especificando su contenido (software que usa) y su ubicación.

SASF podría optar por la toma de una Póliza 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 podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.

Para revisar el inventario de hardware y software, revisar la sección “Situación Actual de la Empresa” tablas # 1, 2, 3, 4, 5, 6 y 7 respectivamente.

Se deberá realizar una 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 al Servidor, color amarillo a las computadoras con Información importante o estratégica y color verde a las computadoras de contenidos normales.

d) Obtención y almacenamiento de los respaldos de información (BACKUPS)

Se obtendrán copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

- Backups del Sistema Operativo.
- Backups del Software Base - Paquetes y/o Lenguajes de Programación.

- Backups de Productos Desarrollados (Considerando tanto los programas fuentes, como los programas objetos correspondientes)
- Backups de los Datos (Bases de Datos, Índices, y todo archivo necesario para la correcta ejecución de los Productos Desarrollados)
- Backups del Hardware, mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder continuar con las actividades para 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 ambiente y facilidades de trabajo.

Para realizar los respaldos se tendrá en consideración el uso de la herramientas de encriptación que vienen incluidas en el sistema operativo Windows 2000 para que la información pueda ser recuperada sola y exclusivamente por quién la generó. También se recomienda tener duplicidad en los respaldos, esto es, mantener un respaldo “in situ” para mayor facilidad de recuperación, y otro respaldo fuera de las instalaciones de la empresa.

e) Políticas (normas y procedimientos de Backups)

El valor que tiene la información y los datos es casi absoluto, si falla el disco duro, el daño puede ser irreversible, puede significar la pérdida total de nuestra información, por esta razón debemos respaldar la información importante. La pérdida de información provoca daño de fondo como los mencionados a continuación:

- Pérdida de oportunidades de negocio
- Clientes decepcionados
- Reputación perdida

Las interrupciones se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones. Y aunque no se pueda prevenir cada una de estas interrupciones, SASF sí puede prepararse para evitar las consecuencias que éstas puedan tener ya que del tiempo que tarde en reaccionar SASF dependerá la gravedad de sus consecuencias. En parte para reducir el tiempo de recuperación del desastre se tendrán ciertas normas y procedimientos. Seguiremos las siguientes medidas técnicas para la realización de las copias de seguridad, condicionadas de acuerdo a los siguientes puntos:

Volumen de información a copiar

Sugerimos las siguientes estrategias con respecto a la forma de respaldar la información que puede ser:

- Copiar sólo los datos: poco recomendable, ya que en caso de incidencia, será preciso recuperar el entorno que proporcionan los programas para acceder a los mismos, influye negativamente en el plazo de recuperación del sistema.

- Copia completa: recomendable, si el soporte, tiempo de copia y frecuencia lo permiten, incluye una copia de datos y programas, restaurando el sistema al momento anterior a la copia.

- Copia incremental: solamente se almacenan las modificaciones realizadas desde la última copia de seguridad, con lo que es necesario mantener la copia original sobre la que restaurar el resto de copias. Utilizan un mínimo espacio de almacenamiento y minimizan el tipo de desarrollo, a costa de una recuperación más complicada.

- Copia diferencial: como la incremental, pero en vez de solamente modificaciones, se almacenan los ficheros completos que han sido modificados. También necesita la copia original.

Tiempo disponible para efectuar la copia

El tiempo disponible para efectuar la copia de seguridad es importante, ya que el soporte utilizado, unidad de grabación y volumen de datos a almacenar, puede hacer que el proceso de grabación de los datos dure horas, y teniendo en cuenta que mientras se efectúa el proceso es conveniente no realizar accesos o modificaciones sobre los datos objeto de la copia, por esta razón los respaldos se los deberá realizar fuera del horario laboral.

Soporte utilizado

Esta decisión estará condicionada por un conjunto de variables, tales como la frecuencia de realización, el volumen de datos a copiar, la disponibilidad de la copia, el tiempo de recuperación del sistema.

Tentativamente proponemos dos alternativas, a continuación:

- La utilización de una unidad de tape que será alimentada automáticamente mediante un software de respaldo el mismo que puede ser BrightStor® ARCserve® Backup r11.1 for Microsoft Small Business Server, el cual tiene un costo de $695,00 por servidor.

- Continuar con el esquema actual de respaldo utilizando un software de escritura de información a CD's de datos.

Frecuencia de realización de copias de seguridad

La realización de copias de seguridad han de ejecutarse diariamente, éste es el principio que debe regir la planificación de las copias.

Una alternativa basada en la frecuencia de ejecución que nos ayudará a tener una planificación en los respaldos es la que describimos a continuación:

Secuencia de respaldo GFS (Grandfather-Father-Son)

Esta secuencia de respaldo es una de las más utilizadas y consiste en Respaldos Completos cada semana y Respaldos de Incremento o Diferenciales cada día de la semana. Suponiendo la siguiente semana:

Domingo (1)	Lunes (2)	Martes (3)	Miércoles (4)	Jueves (5)	Viernes (6)	Sábado (7)
Diferencial/ de Incremento o NADA	Diferencial/ de Incremento	Diferencial/ de Incremento	Diferencial/ de Incremento	Diferencial/ de Incremento	Completo	Diferencial/ de Incremento o NADA
Domingo (8)	Lunes (9)	Martes (10)	Miércoles (11)	Jueves (12)	Viernes (13)	Sábado (14)
Diferencial/ de Incremento o NADA	Diferencial/ de Incremento	Diferencial/ de Incremento	Diferencial/ de Incremento	Diferencial/ de Incremento	Completo	Diferencial/ de Incremento o NADA

Tabla #11 Esquema de respaldo GFS

En caso de fallar el Sistema en Jueves(12):

Será necesario el Respaldo completo del Viernes(6) y si se utilizaron Respaldos Diferenciales: Sólo el Respaldo Diferencial del Miércoles(11).

Si se utilizaron Respaldos de Incremento: Se necesitaran todos los Respaldos de Incremento desde el Sábado(7) hasta el Miércoles(11).

Claro esta que los respaldos completos de cada Viernes pasan a formar parte del "Archivo" mensual de Información.

Mecanismos de comprobación

Se deben definir mecanismos de comprobación de las copias de seguridad, aunque los propios programas las efectúen, para verificar el estado de la copia, es conveniente planificar dentro de las tareas de seguridad la restauración de una parte de la copia o de la copia completa periódicamente cada 3 meses, como mecanismo de prueba y garantía.

Responsable del proceso

Se debe designar a una persona que incluya entre sus funciones la supervisión del proceso de copias de seguridad, el almacenamiento de los soportes empleados en un lugar designado a tal fin, e incluso de la verificación de que las copias se han realizado correctamente. Este rol será definido por el área administrativa de SASF.

El responsable del proceso deberá guardar las copias de seguridad en un lugar alejado, como, por ejemplo, una caja de seguridad o cualquier otro sitio asegurado contra incendios, para que, en caso de que se produzca algún desastre, los datos se encuentren protegidos. Además deberá formar equipos de evaluación (auditoria de cumplimiento de los procedimientos sobre Seguridad).

Cada una de las áreas operativas de Sudamericana de Software, que almacene información que sirva para la operatividad de la organización, deberá designar un responsable de la seguridad en su área, pudiendo ser el jefe de dicha área operativa. Sus labores serán:

- Ponerse en contacto con los miembros de su área para darles a conocer las políticas y procedimientos a seguir para la seguridad de la información
- Proporcionar soporte técnico para las copias de respaldo de los fuentes de los productos en desarrollo.
- Supervisar la carga de archivos de datos de los productos en desarrollo, y la creación de los respaldos incrementales.
- Verificar el funcionamiento óptimo de los componentes de red.
- Establecer procedimientos de seguridad en los sitios de recuperación.

- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Participar en las pruebas y simulacros de desastres.
- Revisar que las Normas y procedimientos con respecto a Backups, seguridad de equipos y data se cumpla.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.
- Los Jefes de las unidades operativas existentes en SASF deberán reportar el cumplimiento y mensualmente hacer la entrega de la información que ellos hayan respaldado al Administrador de la red de Sudamericana de Software con el fin de revisar y centralizar los backups realizados.

2.6.2 ACTIVIDADES DURANTE EL DESASTRE

Una vez presentada la Contingencia o Siniestro, se deberán ejecutar las siguientes actividades, planificadas previamente:

Plan de emergencias

En este plan se establecen las acciones que se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del Siniestro:

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

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

- Vías de salida o escape.
- Plan de Evacuación del Personal. Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)
- Ubicación y señalización de los elementos contra el siniestro (extintores, etc.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos /

Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

A continuación detallamos ciertas normar sugeridas para el caso que se presente un siniestro, sea este robo, sismo o incendio que son los más comunes.

Robos:

El personal de Sudamericana de Software con el fin de resguardar su integridad, deberá tener en cuenta las siguientes recomendaciones:

- Mantener la calma: No oponer resistencia, en especial si el criminal está armado o se nota que esté bajo el influjo de drogas.
- Inteligencia: Tratar de retener frases expresadas por el atacante y evitar mirarlo directo a los ojos para prevenir enfrentamientos.
- Memoria: Aprenderse el número de placas y características del automóvil en caso de que los agresores escapen en un vehículo.
- Sencillez: La gente debe evitar ser ostentosa y mantenerse atenta a lo que sucede a su alrededor.

Sismos:

Si el Sismo no es fuerte, tranquilícese, acabará pronto, si es fuerte, mantenga la calma, agudice la atención para evitar riesgos y recuerde las siguientes instrucciones:

- Si está dentro del edificio, quédese dentro, hasta poder salir calmadamente; si está fuera, permanezca fuera, buscando una área despejada.
- Dentro de un edificio busque estructuras fuertes: como por ejemplo una mesa, bajo el dintel de una puerta, junto a un pilar, pared maestra o en un rincón y proteja su cabeza.
- Apague todo fuego, con extintores. No utilice ningún tipo de llama (cerilla, encendedor, vela, etc.) durante o inmediatamente después del temblor.
- Fuera de un edificio ,aléjese de cables eléctricos, cornisas, cristales, pretiles, etc.
- No se acerque ni penetre al edificio para evitar ser alcanzado por la caída de objetos peligrosos (cristales, cornisas, etc.) Vaya hacia lugares abiertos, no corra y cuidado con el tráfico.

Incendios:

- Conserve la calma: No Grite, No Corra, No Empuje. Puede provocar un pánico generalizado. A veces este tipo de situaciones causan más muertes que el mismo incendio.
- Busque el extintor más cercano y trate de combatir el fuego. Si no sabe manejar el extintor, busque a alguien que pueda hacerlo por usted.
- Si el fuego es de origen eléctrico no intente apagarlo con agua.
- Cierre puertas y ventanas para evitar que el fuego se extienda, a menos que éstas sean sus únicas vías de escape.
- Al momento de abrir una puerta, verifique que la chapa no esté caliente antes de abrirla; sí lo está, lo más probable es que haya fuego al otro lado de ella, no la abra.
- En caso de que el fuego obstruya las salidas, no se desespere y colóquese en el sitio más seguro. Espere a ser rescatado.
- Si hay humo colóquese lo más cerca posible del piso y desplácese "a gatas". Tápese la nariz y la boca con un trapo, de ser posible húmedo.
- Si se incendia su ropa, no corra: tírese al piso y ruede lentamente. De ser posible cúbrase con una manta para apagar el fuego.

Formación de equipos

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de prioridades, para salvar los equipos señalados en las actividades previas al desastre.

Entrenamiento

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, sismos, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos de Sudamericana de Software. Se llevará a cabo estos entrenamientos mediante la implementación de simulacros y charlas ante los posibles siniestros que pudiesen ocurrir en la empresa.

2.6.3 ACTIVIDADES DESPUÉS DEL DESASTRE

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan en el Plan de contingencias establecido previo a su ejecución se deben tomar en cuenta los puntos que se detallan a continuación.

Evaluación de daños

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

Para la evaluación de los daños se realizarán las preguntas o indagaciones necesarias por parte del equipo encargado de la vigilancia y/o supervisión del área en donde se produjo el siniestro.

El objetivo de establecer esta evaluación hace que los encargados de cada área puedan reconocer el tipo de desastre que se produjo sea este en el ámbito físico o lógico.

Cuando se obtengan los resultados de la evaluación realizada, el equipo encargado de la supervisión verificará en cuál de los puntos establecidos en el plan de contingencias encaja el siniestro.

Si se tratase de un desastre en el ámbito lógico se deben verificar los siguientes puntos:

- Para la información existente de SASF se debe verificar la calidad e integridad de la misma (hacer las pruebas sobre los programas que antes del desastre funcionaban correctamente)
- La calidad e integridad de la información de respaldo.
- En lo posible volver al estado original de la información antes del desastre.

Si se tratase de un desastre en el ámbito físico se deben verificar los siguientes puntos:

- Por una Suspensión o caída del suministro eléctrico, el estado del hardware (Equipos de cómputo, Equipos de telecomunicaciones)

- Si se trata de un siniestro de fuerza mayor como son: incendios, inundaciones, maremotos, tornados, robo a la empresa; se deben seguir los lineamientos establecidos en el plan de contingencias para desastres de gran magnitud.

Priorización de actividades del plan de acción

Con la evaluación de daños reales y su comparación contra el Plan de acción, tendremos la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Empresa.

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

Ejecución de actividades

Para la ejecución de actividades previamente planificadas en el Plan de acción se definen los siguientes equipos de trabajo:

- Equipo de Salvaguarda de información
- Equipo de Salvaguarda de hardware
- Equipo de Salvaguarda de la empresa

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

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

Evaluación de resultados

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar 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 y como se comportaron los equipos de trabajo.

De la Evaluación de resultados y del siniestro en si, darán como resultado dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionó el siniestro.

Retroalimentación del plan de acción

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

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