PLAN INSTITUCIONAL 2021

TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Empresa de Servicios Públicos del Distrito de Santa Marta ESSMAR E.S.P.

ELABORÓ Y REVISÓ

CARLOS FELIPE SANABRIA
P.E. Adscrito a Secretaría General

RAFAEL PINEDA
P.U. Adscrito a Secretaría General

CARLOS ENRIQUE PAEZ CANTILLO
Gerente (E) ESSMAR E.S.P.

TABLA DE CONTENIDO

LISTA DE TABLAS

1 OBJETIVO

El objetivo se divide en dos partes: primera, tomar las medidas necesarias para minimizar la probabilidad de los riesgos se conviertan en una realidad. Segunda, si ocurre, posibilitar que el sistema pueda responder sin que ello suponga un grave impacto para su integridad.

2 ALCANCE

Aplica para la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P., garantizando al máximo la protección de los activos tecnológicos y de información, logrando brindar un servicio continuo y oportuno y sin interrupciones.

3 FINALIDAD

Mantener un plan para el tratamiento de riesgos de seguridad y privacidad de la información lo más completo y global posible. Definir procedimientos necesarios para afrontar cualquier eventualidad que se produzca en los Sistemas de Información y Comunicación de la empresa, de modo que se asegure la continuidad, seguridad y confiabilidad de estos.

4 RESPONSABILIDAD

El personal del área TIC's es encargado de hacer cumplir dicho plan y socializar con las áreas la mecánica de este.

5 ACTIVIDADES PARA REALIZAR

5.1 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de tratamiento de riesgos de seguridad y privacidad de la información está diseñado para ser aplicado tanto en la Sede principal de la empresa como en las sedes externas, involucrando al personal y equipos que intervienen en el mantenimiento de la función informática y contemplen el software base y las aplicaciones informáticas, así como controlar los accesos a áreas de uso restringido y el hardware. Como resultados esperados son establecer los controles necesarios en la función informática y en el uso de las aplicaciones garantizando la integridad y confidencialidad de la información y el soporte informático ante cualquier siniestro que pudiera ocurrir.

5.2 ESQUEMA GENERAL

Este plan de riesgo implica un análisis de los posibles riesgos a los cuales pueden estar expuestos las instalaciones, equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que se hará un análisis de los riesgos (Antes), cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso de que se presentará el problema (Durante). Pese a todas las medidas se seguridad con las que cuenta la empresa puede ocurrir un desastre, por tanto, es necesario un Plan de Recuperación ante un desastre. El cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Identificaremos los tipos de riesgos y factores para proceder a un plan de recuperación de desastres.

5.2.1 Análisis e Identificación de Riesgos

Tabla 1. Relación riesgos y factor del riesgo

Tipo de Riesgos	Factor de Riesgo
Fallas en el Equipo	Alto
Fallas por Tensión	Alto
Accesos no autorizados	Alto
Acción de Virus	Medio
Fuego	Medio
Terremoto	Medio

En la empresa, se ha identificado los siguientes tipos y factores de riesgo:

5.2.2 En fallas por tensión y en el equipo (tipo de riesgo – alto)

Son fallas que se presentan como parpadeos constantes, de la energía, causando problemas en las instalaciones internas, llegando a malograr equipos de cómputo si no se tiene las siguientes precauciones:

Si hubiere fluctuaciones constantes y prolongadas, se procederá a apagar los equipos, previo aviso a los usuarios. Como medidas de seguridad, se deberá contar con UPS, estabilizadores, polo a tierra, etc.

Llamar a Servicios Administrativos para identificar si la falla es del sistema en general, o es un problema aislado en el tablero de alimentación del área.

Si no se detecta la falla, ubicar si están realizando algún trabajo con equipos de alto consumo, como son máquinas soldadoras, etc. y que se hayan conectado a la red de los equipos de cómputo por equivocación.

En casos de corte intempestivo del suministro de la energía eléctrica, ocasionado por algún factor externo, como son (corte de la línea de transmisión, accidentes, falla en los sistemas de protección, etc.). Esta falla, tanto en el origen como al final (retorno de la energía) puede causar daños a los equipos de cómputo por lo que se debe de seguir el siguiente procedimiento:

Revisar la carga del UPS que alimentan los equipos, para los casos de corte de energía y determinar el tiempo que queda de energía auxiliar.
Por seguridad utilizar la energía que se tiene en los UPS para apagar los equipos en forma correcta.
Si la falla es originada en el sistema general, se debe esperar a que se normalice, (siempre en coordinación), para proceder a encender los equipos y conectar a los usuarios.
Si la falla es originada por algún factor local, deberá, proceder a revisar, los elementos del tablero de la sala de cómputo como son: fusibles, térmicos, cables flojos, o revisar si existe algún equipo que este ocasionando la falla
Si la falla es local proceder a la reparación, o reemplazo, de los componentes que causaron la falla, para esto se debe de solicitar el apoyo de Servicios Generales.

5.2.3 En caso de infección por acción de virus o acceso no autorizado (tipo de riesgo – medio).

La empresa cuenta con la protección de antivirus con consola central web para los equipos en las diferentes áreas; asimismo a través de la red se hacen las actualizaciones del antivirus hacia las máquinas correspondientes.

Sin embargo, en caso de infección masiva de virus se debe de seguir el siguiente plan de tratamiento de riesgos de seguridad y privacidad de la información.

Si la infección es vía red a los equipos de cómputo, proceder de la siguiente forma:

Revisar las alertas que envía el antivirus y ver el tipo de virus que se está propagando, detectando el origen del virus. A su vez desconectar de la red el equipo que está infectado y que está reenviando el virus.
Comprobar si tiene carpetas compartidas en forma total y proceder a no compartirlas.
Si no se lograra limpiar en forma satisfactoria, el equipo, porque los archivos del sistema operativo han sido dañados se procederá a formatear el disco reinstalándole el sistema operativo y transfiriendo la data de seguridad.

Si la infección es por lista de correo, se procede de la siguiente forma:

Entrar al Servidor donde está instalado el Correo a los servicios y deshabilitar el Servicio de Mensaje Transferencia para que no siga reenviando los correos.
Proceder a eliminar el mensaje que se encuentra en cola y que está infectado.
Proceder a pasar el antivirus con las opciones indicadas.

5.2.4 En caso de fuego, terremoto o cualquier otra eventualidad externa (tipo de riesgo –medio)

La empresa, a pesar de que cuenta con sistemas de protección, contra incendios, como son, extintores manuales, "conexiones alternas de energía" (en algunas áreas), equipos de bajo consumo, vías de acceso y de evacuación, amplias, etc., no está exenta de que algún incidente involuntario, puede ocasionar, el inicio de un Incendio para lo cual se deberá proceder de la siguiente manera:

Desconectar las fuentes de alimentación eléctricas (sin riesgo de exponer la vida).

Si el tiempo lo permite y si la fuente del siniestro está lejos, pero se puede propagar hacia los equipos principales de cómputo deberá retirar los equipos hacia un lugar seguro, discos o ultimas copias que tenga a la mano evitando exponer la vida.

5.3 ASPECTO DE SEGURIDAD EN LAS REDES

5.3.1 Control de acceso físico en las áreas

Solo personal autorizado deberá ingresar a las áreas donde se encuentren los equipos informáticos; si otras personan ingresan debe ser con autorización y coordinación de la jefatura inmediata con previa programación si es el caso.

Se recomienda contar con cámaras de seguridad en las áreas consideradas clave y en caso no se encuentre personal deberá estar cerrado por motivos de seguridad; o si es el caso dicha persona que está a cargo de las llaves se tendría que ausentar por un tiempo considerable, darle a otra persona a fin de que se encargará de velar por el mismo.

5.3.2 Control de acceso a la red vía PC

- ✓ Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves o bloqueos de las PC.
- ✓ Solicitar clave de ingreso en el área TIC's a la red y a los sistemas que están en red.
- ✓ Registrar toda la actividad de la estación de trabajo con el visor de sucesos.

6 ANÁLISIS DE RIESGOS

Identificar y evaluar los objetos que deben ser protegidos, los daños que éste pueda sufrir, sus posibles fuentes de daño, su impacto dentro de la entidad y su importancia dentro del mecanismo de funcionamiento.

6.1 BIENES SUSCEPTIBLES DE UN DAÑO

1. Hardware.
2. Software.
3. Datos e información.
4. Documentación.
5. Suministro de energía eléctrica.
6. Suministro de telecomunicaciones.

Los posibles daños a lo que puedan estar expuestos:

- ✓ Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o por causas humanas.
- ✓ Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, sean cambios de claves de acceso, eliminación o borrado físico/lógico de información o proceso no deseado ejecutado.
- ✓ Acceso no Autorizado: por vulneración de los sistemas de seguridad en operación, ruptura de las claves de acceso a los sistemas computacionales, instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales
- ✓ Desastres Naturales: movimientos telúricos que afecten directa o indirectamente a las instalaciones, por fallas causadas por la agresividad del ambiente o inundaciones causadas por falla en los suministros de agua.

6.2 6.2. MEDIDAS PREVENTIVAS

6.2.1 Control de Accesos

Se debe definir medidas efectivas para controlar los diferentes accesos a los activos computacionales:

- ✓ Acceso físico de personas no autorizadas.
- ✓ Acceso a la Red de los PC's.
- ✓ Acceso restringido a las librerías, programas, datos, logs de auditoria, etc.

6.2.2 Previsión de desastres naturales

La previsión de desastres naturales sólo se puede hacer desde el punto de vista de minimizar los riesgos innecesarios en las distintas áreas de cómputo, tener la medida de no dejar objetos en una posición tal que ante un movimiento telúrico de cierta magnitud pueda generar mediante su caída y/o destrucción, la interrupción del proceso de operación normal. Además, desde el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, CD, discos externos, discos con información vital de respaldo de aquellos que se encuentren aún en las instalaciones.

6.2.3 Seguridad de la información

La información y programas de los Sistemas de Información que se encuentran en los equipos de cómputo deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado. Proceso contemplado en el documento plan de seguridad y privacidad de la información.

7 PLAN DE RESPALDO

El Plan de Respaldo trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento. Todos los nuevos diseños de sistemas, proyectos o ambientes tendrán sus propios Planes de Respaldo.

7.1 RESPALDO DE DATOS VITALES

Identificar las áreas para realizar respaldos:

Sistemas en Red.
Sistemas no conectados a Red.
Sitio WEB.
Correos electrónicos institucionales

7.2 ANÁLISIS DE CRITICIDAD

Esta tarea deberá ser realizada conjuntamente por Soporte técnico, Desarrollo y Administración de Sistemas, realizarse periódicamente, con el objetivo de revisar la criticidad, al menos dos veces por año o por demanda cuando se pone en producción un nuevo sistema de información o servicio de red y éste debe ser incluido en el plan de respaldos.

Normalmente la información que es respaldada por las empresas son archivos creados por aplicaciones, como, por ejemplo: .DOC, .DOCX .ODT, .XLS, .XLSX .MDB, .PDF, .PPT, PPD, PPDX, PPTX, entre otros.

7.2.1 Nivel de criticidad

Nivel con la cual se ha establecido la criticidad, este puede ser:

- ✓ ALTA: El sistema y/o servicio posee información altamente crítica, por lo que debe ser respaldada al menos de forma diaria y una vez al mes.
- ✓ MEDIA: El sistema y/o servicio posee información medianamente crítica, por lo que debe ser respaldada al menos una vez por semana y una vez al mes.
- ✓ BAJA: El sistema y/o servicio posee información que no es crítica y por lo que debe ser respaldada al menos una vez por mes.

7.3 PLAN DE RESPALDO Y RESPONSABLES

El plan de respaldos contiene información de que sistemas de información y servicios de red serán respaldados, por lo que su periodicidad, tipo de respaldo, etc., estará determinado por la criticidad del sistema de información y/o servicio de red. Por otro lado, se realizarán las tareas de obtención de respaldos tomado en cuenta los horarios en los que el tráfico de datos de la

red sea bajo; es decir, cuando no represente. Proceso contemplado en el documento plan de copias de seguridad (Backups).

El cronograma deberá contemplar claramente los siguientes campos:

Responsable/s: Persona/s quien/es realizo/aron el plan.
Fecha del plan: La fecha en la cual entra en vigor el plan.
Operador de Respaldos: Nombre y cargo de la persona que asume el rol.
Revisor de Respaldos: Nombre y cargo de la persona que asume el rol.

7.3.1 Periodicidad

Es la frecuencia con la que se deberán realizar los respaldos, esta puede ser:

- ✓ DIARIO: Realización de la copia de respaldo diariamente a disco duro.
- ✓ SEMANAL: Realización de la copia de respaldo semanalmente a disco duro.
- ✓ MENSUAL: Realización de la copia de respaldo mensual a cinta con las copias diarias y semanales acumuladas (HISTÓRICO).

Por requerimiento: Realización de la copia de respaldo a requerimiento por una sola vez o por un tiempo determinado y puede ser temporal-diario o temporal-mensual normalmente a requerimiento especial, a menudo usado para ambientes de prueba.

7.3.2 Respaldos

7.3.2.1 Respaldo local

El respaldo local puede hacerse de varias formas en varios tipos de dispositivos. Pero actualmente el método más usado es utilizando discos duros externos. Estos discos no suelen ser muy costosos y hay de todas las capacidades, lo ideal sería tener dos de estos en espejo en caso de que alguno falle. En caso de ser un disco duro USB se tiene que compartir en Red entre las PC de la empresa.

Las desventajas de utilizar un medio de respaldo local es que en caso de desastre o robo se verán igual de afectados que nuestros demás equipos, normalmente la información más crítica se respalda en un medio como un DVD y se puede guardar en una caja fuerte si se tiene alguna en la empresa de esta manera si hay algún incendio o inundación no se verá

7.3.2.2 Respaldo remoto

El respaldo remoto nos ayuda a protegernos contra desastres como incendios e inundaciones, contra robos y otras eventualidades que puedan ocurrir en el sitio principal de nuestra empresa. Sí nuestra empresa tiene varias sedes separadas geográficamente podemos colocar uno o varios servidores distribuidos entre las sedes para respaldar nuestra información a través de la red con

una conexión segura. Así si pasa una eventualidad en alguna de nuestras sedes podemos recuperar la información fácilmente.

El respaldo remoto trae como ventaja la distancia geográfica que disminuye el riesgo de perder los datos, como desventaja tenemos que si se llega a perder la comunicación por períodos largos de tiempo no se puede realizar el respaldo con regularidad. La mejor solución es utilizar un respaldo local y remoto, así se tienen las ventajas de ambos y se compensan las desventajas de uno con el otro.

8 PLAN DE RECUPERACIÓN

8.1 8.1. LISTA DE VERIFICACIÓN PARA UN PLAN DE RECUPERACIÓN

Cuando hablamos de ejecutar una Recuperación ante una eventualidad de nuestra red o de la Continuidad de la organización el tiempo y la precisión son de alta importancia. Las metas de una recuperación de desastres y la continuidad del negocio son sensitivas en el tiempo y bastante críticos, por lo que el uso de una Lista de Verificación se convierte en una herramienta ideal cuando nos afrontamos a una situación en donde esos planes son requeridos.

Las siguientes actividades definen una seria de acciones o actividades que deben entrar en juego cuando se requiere ejecutar una recuperación de desastres:

Detectar una falla y efectos de desastres lo más rápido posible.
Notificar a los responsables que deben tomar acción.
Aislar los sistemas afectados para limitar el alcance de las fallas y daños.
Reparar o reemplazar sistemas críticos, y trabajar hacia una continuidad en las operaciones normales, si es que las circunstancias lo permiten.

El Plan de Recuperación viene de la mano del Plan de Respaldo, pues de la información respaldada se realiza la recuperación en caso de algún inconveniente.

8.2 ACTIVACIÓN DEL PLAN

La decisión queda a juicio de la Dirección General, determinando la activación del Plan de Desastres, y además indicar el lugar alternativo de ejecución del Respaldo y operación de emergencia, basándose en las recomendaciones indicadas por éste.

8.3 APLICACIÓN DEL PLAN

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en los casos que no sea un fin de mes, y un período mayor a 24 horas durante los fines de mes (durante los cierres contables).

8.4 RECURSOS DE CONTINGENCIA GENERALES

Se debe tener recursos de contingencia tales como:

- ✓ Router (Proveído por el proveedor de Internet y WAN).
- ✓ Tarjeta de Red, Conector RJ45, Jack RJ-45, Testeadores.
- ✓ Servidores y Equipos de Comunicación (Switchs, Antenas, Fibra, etc.).
- ✓ Gabinete de Comunicaciones y Servidores.
- ✓ Materiales Y herramientas para cableado Estructurado.
- ✓ UPS y Equipos de aire acondicionado.

- ✓ Backups diario de la información de los Sistemas.
- ✓ Instaladores de las aplicaciones, de Software Base, Sistema Operativo, etc.
- ✓ Componente de Remplazo (Memoria, Disco Duro, UPS, etc.).

9 REFERENCIAS

MINTIC. (2016). Modelo de Seguridad y Privacidad de la Información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Obtenido del siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC. (2016). Guía de gestión de riesgos. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Obtenido del siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MINTIC. (2016). Guía para la preparación de las TIC para la continuidad del negocio. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Obtenido del siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

MINTIC. (2016). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Obtenido del siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf