PLAN INSTUTUCIONAL 2023

TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

ESSMAR E.S.P.
EMPRESA DE SERVICIOS PÚBLICOS
DEL DISTRITO DE SANTA MARTA

ELABORÓ Y REVISÓ

CARLOS SANABRIA
Profesional Especializado Grupo TIC
Secretaria General

RAFAEL PINEDA
Profesional Universitario Grupo TIC
Secretaria General

VÍCTOR RODRIGO VÉLEZ MARULANDA
Agente Especial ESSMAR E.S.P.

TABLA DE CONTENIDO

1 OBJETIVO

Establecer acciones y controles necesarios para minimizar y mitigar la probabilidad que los riesgos se materialicen, que permitan fortalecer el sistema de información de la entidad, para responder sin que ello suponga un grave impacto para su integridad y funcionamiento en los procesos.

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, oportuno y sin interrupciones.

3 RESPONSABLES

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

4 GENERALIDADES

4.1 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 en las áreas y sedes de la ESSMAR E.S.P, involucrando a los funcionarios y contratistas que están en contaste intervención y uso de equipos informáticos y manipulen algún software o aplicación informática, así como controlar los accesos a áreas de uso restringido donde exista hardware crítico. De igual forma se establecen los controles necesarios en el uso de las aplicaciones o softwares garantizando la integridad y confidencialidad de la información y el soporte informático ante cualquier siniestro que pudiera ocurrir.

4.2 Esquema General

Este plan de riesgo implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los 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). A pesar de contar con medidas de seguridad frente a riesgos, en la empresa puede ocurrir algún desastre de manera imprevista, por tanto, es necesario tener

el 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.

4.2.1. Análisis e Identificación de Riesgos

TIPO DE RIESGOS	FACTOR DE RIESGO
Fallas en el Equipo	Alto
Fallas por Tensión	Alto
Accesos no autorizados	Alto – Medio
Acción de Virus	Alto – Medio
Fuego	Medio
Terremoto	Medio

4.2.1.1. En Fallas por tensión y en el equipo (Tipo de Riesgo –Alto).

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

- Si existen 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.

- Informar de inmediato a Servicios Administrativos si la falla es del circuito en general, o es un problema aislado en el tablero de alimentación del área afectada.

- En caso de no detectar la falla a simple vista, identificar si están realizando algún trabajo con equipos de alto consumo, como son máquinas soldadoras, etc. y revisar si posiblemente está conectada al circuito de los equipos de cómputo por equivocación.

- En casos de algún corte repentino 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.). Se deberá seguir el siguiente procedimiento ante estas fallas, para evitar afectar los equipos de cómputo:

- Revisar la carga de la UPS que alimentan los equipos, en casos de corte de energía poder determinar el tiempo de reserva de la energía auxiliar.

- Si la falla es originada en el circuito principal, lo correcto es esperar a que se normalice la energía principal para proceder a encender los equipos.

- Si la falla es originada por algún factor local, se procede a revisar los elementos del tablero central como son: fusibles, térmicos, cables flojos, o revisar si existe algún equipo que este ocasionando la falla.

- Si la falla es local se procede a la reparación, o reemplazo, de los componentes que causaron la falla, se debe solicitar apoyo a Servicios Administrativos.

4.2.1.2. En caso de Infección por acción de virus o acceso no autorizado (Tipo de Riesgo– Alto – Medio).

La empresa cuenta con la protección de antivirus endpoint, el cual posee una consola central web para administrar y monitorear los equipos en las diferentes áreas; asimismo a través de la red se hacen las actualizaciones del antivirus hacia las máquinas correspondientes.

Cada equipo de cómputo cuenta con el usuario administrador del área TIC para evitar manipulación, alteración o perdida en los sistemas de información y prevenir instalaciones de software no autorizados.

Sin embargo, en caso de alteraciones por infección masiva de algún virus informático deberá seguirse el siguiente plan de tratamiento de riesgos de seguridad en la información.

Si la infección es ocasionada vía red a los equipos de cómputo, se procede a lo siguiente:

- Revisar las alertas que recibe la consola administradora del antivirus y ver el tipo de virus que se está propagando, haciendo la detención del origen del virus. A su vez se procede a desconectar la conexión del equipo que está infectado y que está reenviando el virus.

- Comprobar si tiene carpetas compartidas en forma total y proceder deshabilitar el uso compartido.

- Al no lograr limpiar satisfactoriamente el equipo, porque los archivos del sistema operativo han sido dañados se procede a formatear el disco reinstalándole el sistema operativo y transfiriendo la información de copias de seguridad realizadas.

Si la infección es ocasionada por lista de correo, se procede a lo siguiente:

- Entrar al servidor donde está instalado el correo institucional 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.

4.2.1.3. 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, pueda 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.

4.3 Aspecto de Seguridad en las Redes

4.3.1. 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 tener previa autorización por jefes del área de manera inmediata o debidamente programada.

- Contar con cámaras de seguridad en las áreas críticas y en caso de no encontrarse personal responsable deberá estar cerrada la oficina por motivos de seguridad; o si es el caso dicho responsable a cargo de las llaves se tendría que ausentar por un tiempo considerable, deberá delegar a otra persona a velar por el mismo.

4.3.2. Control de acceso a la red vía PC

- Acceso restringido a las áreas donde están ubicados lo equipos de cómputo mediante clave administrador o clave del responsable del equipo.

- Solicitar clave de ingreso a la red wifi, sistemas de información o equipos al área TIC.

- Registrar toda la actividad de los equipos de cómputo con el visor de sucesos.

4.4 ANÁLISIS DE RIESGOS

Identificar y evaluar los objetos e información que deban ser protegidos, los daños que éstos puedan sufrir, sus posibles fuentes de daño, su impacto dentro de la entidad y su importancia dentro de los procesos.

4.4.1. Bienes susceptibles de un daño

- Hardware.
- Software.
- Datos e información.
- Documentación.
- Suministro de energía eléctrica.
- 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 usados, sean 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 de información, instalación de software de comportamiento errático y/o dañino para la operación de los sistemas.

- 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.

4.4.2. Medidas preventivas

4.4.2.1. Control de Accesos

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

- ✓ Acceso físico de personas no autorizadas.
- ✓ Cambios o traspaso de contraseñas previamente autorizadas.
- ✓ Identificar vulnerabilidades en la red dirigido los equipos o sistemas.

4.4.2.2. 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 áreas donde se encuentren equipos de cómputo, evitando posiciones de tal manera que ante un movimiento telúrico de cierta magnitud pueda generar su caída y/o destrucción, con ello se genere la interrupción anormal del proceso. Además, desde el punto de vista de respaldo, se debe tener 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.

4.4.2.3. Seguridad de la información

La información y 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. Políticas de seguridad de la información contemplado en el documento plan de seguridad y privacidad de la información.

4.5 PLAN DE RESPALDO

El plan de respaldo define las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento. Cada sistema de información implementado o servicio TI tendrá su propio plan de respaldo.

4.5.1. Respaldo de datos vitales

Identificar las áreas según su importancia en el suministro de información para realizar respaldos:

- Sistemas de información en la nube.
- Sistemas de información no conectados a la Red.
- Sitio WEB.
- Correos electrónicos institucionales

4.5.2. Análisis de criticidad

Esta tarea deberá ser realizada juntamente con ayuda técnica, y el administrador del o los sistemas de información, de manera 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 TI y éste debe ser incluido en el plan de respaldos.

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

4.5.3. Nivel de criticidad

Nivel con la cual se ha establecido la criticidad de la información:

- ALTA: El sistema y/o servicio posee información altamente crítica, por lo que debe ser respaldada de manera trimestral o semanal si es requerida.

- MEDIA: El sistema y/o servicio posee información medianamente crítica, por lo que debe ser respaldada de manera trimestral o mensual si es requerida.

- BAJA: El sistema y/o servicio posee información que no es crítica y por lo que debe ser respaldada cada vez que sea requerida.

4.5.4. 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 copias de seguridad de la información teniendo en cuenta los horarios y debida programación del proceso. Dicho procedimiento está contemplado en el documento TIC-P01 Procedimiento Administración Copias de Respaldo.

4.5.5. Periodicidad

La frecuencia con la que se deberán realizarse los respaldos podría ser:

- SEMANAL: Si es solicitada, copia de respaldo semanal a disco(s) duro(s).
- MENSUAL: Se realiza copia de respaldo mensual a discos con las copias diarias y semanales acumuladas.
- TRIMESTRAL: Debidamente programado se realiza copia de respaldo a toda la información relevante de la entidad.

4.5.6. Respaldos

4.5.6.1 Respaldo local

El respaldo local puede hacerse de varias formas con varios tipos de dispositivos. Pero actualmente el método más usado es utilizando discos duros externos. Estos discos no suelen ser costosos y hay de todas las capacidades, lo ideal es contar con varios discos duros en caso de quedar sin espacio suficiente o se presente algún daño.

Una de las desventajas de utilizar un medio de respaldo local, es que en caso de desastre o hurto se verán afectados los procesos que respaldaron información sin poder recuperar datos parcialmente o total, la información más crítica debería contar con un respaldo extra en un medio como un DVD, el cual podría ser asegurado en otro sitio sea interno o externo.

4.5.6.2. Respaldo remoto

El respaldo remoto o virtual nos ayuda a protegernos contra desastres como terremotos, incendios e inundaciones, contra hurtos y otras eventualidades que puedan ocurrir en los diferentes sitios de nuestra empresa. Al tener varias sedes físicas de la empresa, se cuenta con servidores locales respaldados por servidores digitales, en caso de una eventualidad en alguna de nuestras sedes podemos recuperar la información fácilmente.

El respaldo remoto trae como ventaja el distanciamiento que disminuye el riesgo de perder los datos, como desventaja se podría perder la comunicación por períodos largos de tiempo sin poder 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.

4.6 PLAN DE RECUPERACIÓN

4.6.1. Lista de Verificación Para Un Plan de Recuperación

Cuando hablamos de ejecutar una recuperación ante una eventualidad de nuestra red o sistema o de la continuidad de la organización, el tiempo y la precisión son de alta importancia. Las metas de una recuperación ante el desastre y la continuidad del negocio son prioritarias en el tiempo y bastante críticas, por lo que el uso de una lista de verificación se convierte en una herramienta ideal cuando se nos presente una situación en donde esos planes son requeridos.

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

- Detectar la falla y efectos generados por el desastre lo más rápido posible.
- Notificar a los responsables que deben tomar acción respectivamente.
- 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.

4.6.2. Activación del plan

La activación del plan de recuperación se desarrolla acorde a las directrices definidas por el área TIC, determinado con la activación del Plan de Desastres, y además indicando el lugar alternativo de ejecución del respaldo y operación de emergencia, basándose en las recomendaciones indicadas por éste.

4.6.3. Aplicación del plan

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en cualquier que sea el caso, es lograr la continuidad del negocio sin retrasos y resolviendo positivamente la emergencia lo antes posible.

4.6.4 Recursos de contingencia generales

Se debe tener recursos de contingencia tales como:

- Conectividad respaldada por el prestador del servicio de Internet.
- 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.).

5. ESTRATEGIAS TIC'S

5.1. Actividades

ACTIVIDAD	OBJETIVOS	TIEMPO (ejecución)	SEGUIMIENTO	CONTROL
Realizar controles establecidos en la matriz de riesgo del proceso TIC	➢ Reducir y mitigar la materialización de los riesgos de seguridad y privacidad de la información.	Anual	Trimestral	Grupo TIC
Actualizar servidores de la seguridad de la información de la ESSMAR E.S.P.	➢ Supervisar las actualizaciones realizadas a los servidores utilizados.	Largo plazo	Trimestral	Grupo TIC
Actualizar licencias de software originales para los equipos de cómputo de la ESSMAR E.S.P.	➢ Mantener un adecuado funcionamiento de los recursos tecnológicos de software.	Mediano Plazo	Anual	Grupo TIC
Realizar revisiones periódicas a procesos de seguridad, IP locales, claves de equipos, usuarios administradores en los sistemas de información y correos institucionales.	➢ Garantizar el acceso seguro a los equipos de cómputos y sistema de información.	Mediano Plazo	Semestral	Grupo TIC

5.2. Indiciadores

ACTIVIDAD	INDICADORES	PRIORIDAD	META
Realizar controles establecidos en la matriz de riesgo del proceso TIC	(N° de controles realizados/ N° de controles programados *100%	ELEVADO	100%
Actualizar servidores de la seguridad de la información de la ESSMAR E.S.P.	(N° actualizaciones servidores realizadas / N° actualizaciones servidores programada) *100%	MEDIO	100%
Actualizar licencias de software originales para los equipos de cómputo de la ESSMAR E.S.P.	(Licencias de software instaladas / Licencias de software programados) *100%	ELEVADO	615 licencias instaladas
Realizar revisiones periódicas a procesos de seguridad, IP locales, claves de equipos, usuarios administradores en los sistemas de información y correos institucionales.	(revisiones periódicas ejecutadas / revisiones periódicas programadas) *100%	MEDIO	100%

6. 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