Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023

INTRODUCCIÓN

Las tecnologías de la información han generado un cambio significativo en la cultura y en las estrategias de comunicación de la sociedad. Por tanto, el SETP MONTERÍA AMABLE SAS ha desarrollado el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023, que tiene como objetivo y finalidad la protección de los equipos de cómputo, la información de la empresa (como activo de gran valor), tanto en Hardware como en Software.

OBJETIVOS

Fortalecer la infraestructura tecnológica, con un plan de contingencia que garantice la protección de los equipos de cómputo y la información de las diferentes dependencias de la empresa.

OBJETIVOS ESTRATÉGICOS

- Adoptar un Plan de Contingencia Tecnológica para el SETP TRANSFEDERAL SAS.
- Establecer los lineamientos y estrategias a utilizar en cada caso.
- Salvaguardar la información de la empresa como uno de los principales activos de la misma.

OBJETIVOS ESPECÍFICOS

- Levantar un inventario de la información de cada una de las dependencias
- Realizar acciones que conlleven a la protección de la información
- Socializar en todo el personal, la importancia del Plan de Contingencia Tecnológica, y las acciones que cada uno debe tener en cuenta para la protección de la misma.
- Vigilancia en el servicio de servidores en la nube donde se salvaguarde la información y se encuentre protegida frente a terrorismo, asonadas, catástrofes o incendios.
- Proceder y levantar los procesos de generación de Backups (copias e seguridad).

ACCIONES POR DESARROLLAR

1. **MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS DE EQUIPOS DE COMPUTO**

- **Mantenimiento Preventivo:**

Es aquel mantenimiento que se lleva a cabo cada cuatro (4) meses de parte de Ingeniero de Sistemas capacitado para esta tarea, mantenimiento que incluye:

- Limpieza externa e interna del equipo (físico)
- Actualización y revisión del software
- Revisión contra virus informáticos, spam, pishing entre otros softwares que puedan ocasionar daño o pérdida de la información.
- Eliminación de archivos temporales u otros que relenticen el funcionamiento del

equipo
- Para esta tarea se lleva una ficha técnica u hoja de vida de cada equipo.

- **Mantenimiento Correctivo:**

Mantenimiento que se realiza en un periodo de tiempo corto, ante la solicitud y llamado del usuario operador del mismo equipo; este mantenimiento es atendido por un Ingeniero de Sistemas.

Pasos para el desarrollo de esta tarea:

1. Se realiza la solicitud por parte del funcionario o contratista al proveedor de manejar el mantenimiento de los equipos de cómputo o los programas.
2. El ingeniero de sistemas se desplaza atender la solicitud, teniendo en cuenta de la importancia de salvaguardar la información de este como prioridad.
3. En caso de tener que retirar el equipo, se le suministra un equipo provisional al usuario final de manera temporal, mientras se soluciona lo de su equipo asignado.
4. De acuerdo con el diagnóstico realizado por el ingeniero, se hacen los correctivos, y se retorna al usuario final el mismo.
5. Se hacen las recomendaciones si viene al caso.
6. Se hace cierre del caso correctivo.

2. RESPALDO DE LA INFORMACIÓN

a) En cada unidad de trabajo:

Cada usuario debe generar Backup de la información de su importancia de acuerdo a sus funciones y cargos que le corresponda.
Esta copia de seguridad puede ser, dentro del mismo equipo, en discos duros externos, drive o en la nube.
Debe de existir un ingeniero de sistemas, que generara Backup completo del equipo, y este será almacenado en discos duros externos, diferentes a los que maneje el usuario.
Así mismo el usuario puede solicitar soporte y apoyo al ingeniero de sistemas, cuando lo requiera, para la protección de su información.

b) Portal web www.monteriaamable.gov.co

El portal web debe generar copia de seguridad periódica, dependiendo del flujo de la información que maneje, ya sea diaria o semanal.
Este backup quedará en el PC asignado para tal tarea, disco duro externo y en el servidor de hosting contratado por la empresa.
El ingeniero responsable de la administración y alimentación del portal es el responsable de la generación y protección del mismo.

c) Información de cada una de las dependencias

Se tiene un disco o unidad compartida en el servidor donde cada dependencia maneja

una carpeta y ahí debe guardar su copia de seguridad.
A parte de que cada dependencia puede solicitar al ingeniero de soporte el recaudo de la información en discos duros externos.

d) Seguridad Perimetral

Se debe de instalar un sistema de Seguridad Perimetral, donde se salvaguarde la información de la dependencia de Administrativa y Financiera, esta información debe ser salvaguardada de manera diaria.
Por lo tanto, esta información queda en el disco duro del servidor de la empresa y en el servidor VPS contratado por la empresa, fuera de la ciudad de Neiva.
Se contrata dos servidores de hosting en la nube:

1. Uno para alojar el Sistemas de Gestión Documental (con sistema Windows server especializado)
2. Otro para la copia de seguridad diaria del sistema financiero de la empresa Suministros y Servicios TECH S.A.S, con eso garantizamos que la información del sistema financiero quede alojada externamente a las instalaciones de la empresa, garantizando su protección frente a asonadas, incendios y vandalismos entre otros.

3. CONTINGENCIA EN HARDWARE (EQUIPOS TECNOLOGICOS)

Se debe adquirir una póliza que ampare los equipos de cómputo ante:

- Robo
- Vandalismo
- Terrorismo
- Catástrofes
- Y daños eléctricos.

Lo cual nos garantice la recuperación física de los mismos sin incurrir en costos extras para la empresa.