“Somos un equipo comprometido con nuestro hogar. Trabajamos con pasión por servir, estamos avanzando y tenemos la esperanza de ser cada vez mejores por el bienestar de nuestra comunidad y la convicción de sumar voluntades para un desarrollo ambiental, social y económico.”

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

ESSMAR 2025

ELABORÓ Y REVISÓ

ISMAEL ANTONIO MOLINA GIRALDO
Subgerente Corporativa

CRISTIAN PAUL SILVA USAQUEN
Profesional Especializado Grupo TIC
Subgerencia Corporativa

RAFAEL MAURICIO PINEDA GARCIA
Profesional Universitario Grupo TIC
Subgerencia Corporativa

GERMAN IGUARÁN ROMERO
Técnico Administrativo Grupo TIC
Subgerencia Corporativa

ERNEY VELÁSQUEZ TORRES
Agente Especial ESSMAR E.S.P.

Tabla de contenido

1. Introducción

La privacidad y la seguridad de la información son elementos fundamentales para el buen funcionamiento y la confianza en cualquier organización. A medida que las tecnologías avanzan y la digitalización crece, los riesgos asociados a la protección de los datos personales y corporativos se incrementan, lo que hace necesario establecer un plan de tratamiento adecuado para mitigar estos riesgos. Un plan de tratamiento de riesgos de la privacidad y seguridad de la información tiene como objetivo identificar, evaluar y gestionar los riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad de la información sensible, tanto en su almacenamiento como en su transmisión.

Este plan debe abordar las amenazas que puedan surgir de diversos factores, tales como ataques cibernéticos, acceso no autorizado, pérdida de datos, y la falta de cumplimiento de las normativas legales vigentes (por ejemplo, el GDPR en la Unión Europea). Además, debe incluir estrategias para la formación continua del personal, la implementación de controles técnicos y organizacionales, así como la respuesta ante incidentes de seguridad.

La creación de un plan de tratamiento de riesgos de privacidad y seguridad debe basarse en una evaluación continua y dinámica de los riesgos, adaptándose a los cambios tecnológicos y a las nuevas amenazas. La efectividad de este plan depende del compromiso de toda la organización, desde los altos directivos hasta los empleados en la base, para proteger la información que maneja y asegurar la confianza de sus clientes y usuarios.

En resumen, un plan de tratamiento de riesgos de privacidad y seguridad de la información es crucial para prevenir y mitigar los impactos negativos de posibles incidentes, garantizar el cumplimiento de las normativas y proteger los activos más valiosos de la organización: los datos.

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. Objetivo

3.1. Objetivo General

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.

3.2. Objetivos Especifico

- Realizar una evaluación exhaustiva de los riesgos que puedan afectar la privacidad y seguridad de la información dentro de la organización, teniendo en cuenta amenazas internas y externas, vulnerabilidades, y el impacto potencial sobre la confidencialidad, integridad y disponibilidad de los datos.
- Diseñar e implementar controles técnicos, administrativos y físicos adecuados para mitigar los riesgos identificados. Esto puede incluir la encriptación de datos, el control de accesos, auditorías periódicas y políticas de seguridad de la información.
- Desarrollar programas de capacitación y concientización en materia de seguridad de la información y protección de la privacidad para todos los niveles de la organización.
- Establecer un proceso de monitoreo y revisión constante de los riesgos, controles y protocolos implementados.
- Garantizar que la información confidencial, tanto personal como corporativa, sea protegida adecuadamente a lo largo de su ciclo de vida, desde su recopilación hasta su eliminación segura.

4. Marco legal

Norma	Descripción
Decreto 103 de 2015	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1494 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1008	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto 2573 de 2014	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 1377 de 2013	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2609 de 2012.	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Ley estatutaria 1581 de 2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley 1474 de 2011	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención,

Norma	Descripción
	investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 23 de 1982	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
Ley 527 de 1999	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 1581	Por la cual se dictan disposiciones generales para la protección de datos personales.
Norma técnica colombiana NTC - ISO/IEC 27001	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa

5.Definiciones

Riesgo: Probabilidad de que ocurra un evento que pueda afectar la confidencialidad, integridad o disponibilidad de la información, con una consecuencia negativa para la organización.

Confidencialidad: Propiedad de la información que asegura que solo las personas autorizadas tengan acceso a determinados datos o recursos.

Integridad: Propiedad de la información que garantiza que los datos se mantengan completos, precisos y sin alteraciones no autorizadas.

Disponibilidad: Propiedad de la información que asegura que los datos y sistemas estén accesibles y utilizables cuando sea necesario.

Amenaza: Cualquier circunstancia o evento con el potencial de causar daño a la seguridad o privacidad de la información, como ataques cibernéticos, desastres naturales, errores humanos, etc.

Vulnerabilidad: Debilidad en un sistema, proceso o control que puede ser explotada por una amenaza, lo que podría comprometer la seguridad de la información.

Control de seguridad: Medidas o mecanismos implementados para reducir o mitigar los riesgos relacionados con la seguridad y la privacidad de la información. Pueden ser controles técnicos (como firewalls) o administrativos (como políticas de acceso).

Gestión de riesgos: Proceso continuo de identificar, evaluar, tratar y monitorear los riesgos, con el objetivo de reducir la probabilidad y el impacto de eventos adversos relacionados con la privacidad y seguridad de la información.

Incidente de seguridad: Cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información, o que afecte la operación de los sistemas de la organización.

Plan de respuesta a incidentes: Conjunto de procedimientos predefinidos y acciones a seguir cuando ocurre un incidente de seguridad, con el fin de minimizar el impacto y restaurar las operaciones normales de manera rápida.

Cifrado: Técnica que convierte la información en un formato ilegible para aquellos que no tienen la clave de descifrado, con el fin de proteger su confidencialidad.

Acceso autorizado: El permiso dado a individuos o sistemas para acceder a datos o recursos, basándose en su rol o necesidad de conocer la información.

Evaluación de impacto: Proceso de determinar las consecuencias o efectos potenciales de un riesgo o incidente de seguridad sobre la organización, sus operaciones y sus stakeholders.

Cumplimiento normativo: Asegurar que las prácticas y políticas de la organización estén alineadas con las leyes, regulaciones y estándares aplicables en cuanto a la privacidad y seguridad de la información, como el GDPR, HIPAA, o ISO 27001.

Protección de datos personales: Conjunto de medidas y prácticas diseñadas para proteger los datos personales de individuos, asegurando su confidencialidad, integridad y disponibilidad.

Auditoría de seguridad: Proceso de revisión y evaluación de los sistemas y controles de seguridad, con el fin de verificar su eficacia y asegurar el cumplimiento de las políticas y normativas de seguridad.

Análisis de riesgos: Proceso de identificar, evaluar y priorizar los riesgos para la seguridad y privacidad de la información, con el fin de implementar las medidas adecuadas para su tratamiento.

Protección contra accesos no autorizados: Medidas implementadas para evitar que personas o sistemas sin permisos accedan a información o recursos protegidos.

Seguridad perimetral: Conjunto de controles y tecnologías diseñadas para proteger los sistemas y redes de la organización contra accesos no autorizados o ataques provenientes del exterior.

6. Generalidades

6.1. 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.

6.2. 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.

6.2.1. 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**

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

Son fallas que se presentan como parpadeos constantes de la energía 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.
- En el caso de que se den tormentas eléctricas fundamentalmente en las oficinas ubicadas en la planta de tratamiento de agua de MAMATOCO, se procede a apagar los equipos de cómputo, impresoras y demás dispositivos que puedan verse afectados por una súbita de tensión generada por descargas eléctricas de los rayos.

6.2.3. 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.

6.2.4. 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, 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.

6.3. Aspecto de Seguridad en las Redes

6.3.1. 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.

6.3.2. 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.

6.4. 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.

6.4.1. 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.

6.5. Medidas preventivas

6.5.1. 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.

6.5.2. 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.

6.5.3. 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.

6.6. 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.

6.6.1. Respaldo de datos vitales

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

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

6.6.2. 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.

6.6.3. 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.

6.6.4. 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.

6.6.5. 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.

6.6.6. Respaldos

6.6.6.1. 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.

6.6.6.2. 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.

6.7. PLAN DE RECUPERACIÓN

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.

6.7.1. 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.

6.7.2. 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.

6.7.3. 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.).

6.8. ESTRATEGIAS TIC'S

6.8.1. Actividades

ACTIVIDAD	OBJETIVOS	TIEMPO (ejecución)	SEGUIMIENTO	CONTROL	PRIORIDAD
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 Oficina de planeación y regulación	ELEVADO
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	MEDIO
Actualizar las 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	ELEVADO
Realizar revisiones periódicas a procesos de seguridad 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	MEDIO
Control de acceso a los puertos USB de los equipos de cómputo de la empresa ESSMAR E.S.P.	Evitar fuga de datos, Introducción de malware a los equipos y reducir el riesgo de pérdida de información confidencial	Largo plazo	Semestral	Grupo TIC	MEDIO

Tabla 1 (Elaboración propia)

6.8.2. Indiciadores

ACTIVIDAD	TAREAS	INDICADORES	META
Realizar controles establecidos en la matriz de riesgo del proceso TIC	Establecer trimestralmente los controles. Hacer seguimiento y evaluar riesgos.	(N° de controles realizados/ N° de controles programados *100%	100%
Actualizar servidores de la seguridad de la información de la ESSMAR E.S.P.	Realiza un inventario detallado de todos los servidores, incluyendo su hardware, software y configuración. Realiza copias de seguridad completas de todos los datos antes de comenzar la actualización.	(N° actualizaciones servidores realizadas / N° actualizaciones servidores programada) *100%	100%
Actualizar las licencias de software originales para los equipos de cómputo de la ESSMAR E.S.P.	Identificación de las licencias, hacer un inventario de cada una. Contacto con el proveedor, solicitudes de cotización y actualización de licencias. Evaluación de las opciones	(Licencias de software instaladas / Licencias de software programados) *100%	100%
Realizar revisiones periódicas a procesos de seguridad en los sistemas de información y correos institucionales.	Establecer un cronograma para las correspondientes revisiones periódicas. Evaluar la eficacia de las medidas de seguridad. Verificar la frecuencia y eficacia de los respaldos. Concientización de los usuarios sobre las amenazas cibernéticas y las medidas de seguridad	(Revisiones periódicas ejecutadas / Revisiones periódicas programadas) *100%	100%
Control de acceso a los puertos USB de los equipos de cómputo de la empresa ESSMAR E.S.P.	Crear política del uso de dispositivos USB. Definir y comunicar de manera clara las políticas de uso de dispositivos USB a todos los funcionarios. Establecer un proceso para solicitar autorización para utilizar dispositivos USB en casos excepcionales. Restringir puertos USB todos los equipos de computo	(Total equipos de cómputo/equipos con USB restringido) *100	100%

Tabla 2 (Elaboración propia)

7. Control de cambios

Ítem que cambió	Descripción del cambio	Año de modificación
Elaboró y Revisó	Se hizo cambio de los responsables	2022
Alcance	Se modifica la descripción.	2022
Elaboró y Revisó	Se hizo cambio de los responsables	2023
Generalidades	Se hizo ajustes en el contenido	2023
Generalidades	Se hizo ajustes en el contenido	2024
Introducción	Se hizo ajustes en el contenido	2024
Definiciones	Se hizo ajustes en el contenido	2024
Generalidades	Se hizo ajustes en el contenido	2025
Introducción	Se hizo ajustes en el contenido	2025
Definiciones	Se hizo ajustes en el contenido	2025

8. Anexos

N.A.