“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 2026 - 2027

ELABORÓ Y REVISÓ

ALFONSO ELIECER OROZCO DIAZ
Subgerente Corporativa

OSWALDO ENRIQUE ROJAS MANOTAS
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

EDWIN ANTONIO PARADA CABRERA
Agente Especial ESSMAR E.S.P.

Tabla de contenido

1. Introducción

La privacidad y la seguridad de la información constituyen pilares esenciales para el funcionamiento adecuado y la generación de confianza en cualquier organización. A medida que las tecnologías evolucionan y los procesos se digitalizan, aumentan también los riesgos asociados a la protección de los datos personales y corporativos. Esto hace indispensable establecer un plan de tratamiento de riesgos que permita identificar, evaluar y mitigar las amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.

Un plan de tratamiento de riesgos en privacidad y seguridad tiene como propósito gestionar de manera sistemática los riesgos derivados de situaciones como ataques cibernéticos, accesos no autorizados, pérdidas de información, fallas operativas y el incumplimiento de normativas legales vigentes, entre ellas el Reglamento General de Protección de Datos (GDPR) en la Unión Europea. Asimismo, contempla la implementación de controles técnicos y organizacionales, la capacitación continua del personal y la preparación para la atención oportuna de incidentes de seguridad.

La formulación de este plan requiere una evaluación constante y dinámica de los riesgos, adaptándose a los cambios tecnológicos y a la aparición de nuevas amenazas. Su efectividad depende del compromiso de todos los niveles de la organización, desde la alta dirección hasta cada uno de los colaboradores, quienes desempeñan un papel fundamental en la protección de la información que gestionan.

En conclusión, un plan de tratamiento de riesgos de privacidad y seguridad de la información es esencial para prevenir y reducir los impactos derivados de posibles incidentes, asegurar el cumplimiento normativo y salvaguardar uno de 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 y afecten la confidencialidad, integridad y disponibilidad de la información, garantizando fortalecer el sistema de información de la entidad, para responder sin que ello suponga un grave impacto para su 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. POLITICA DE SEGURIDAD DIGITAL

La Empresa de Servicios Públicos del Distrito de Santa Marta ESSMAR E.S.P., como entidad prestadora de servicios públicos de acueducto, alcantarillado, alumbrado público e interventoría a la empresa prestadora del servicio de aseo, establece que, la información es vital para el desarrollo de los procesos y de las actividades misionales e institucional, motivo por el cual, el área de TIC está comprometida con la protección de los activos de información de la Entidad (Empleados, información y entorno laboral), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones de gobernabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad de la información en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información de la empresa, tomando como base que la efectividad de esta política depende finalmente del comportamiento de las personas y los controles establecidos en las políticas de seguridad digital descritas en el presente documento.

El objetivo de la política es Establecer un marco integral de Seguridad de la Información en la ESSMAR E.S.P. que permita definir directrices, lineamientos, roles y responsabilidades para proteger los activos de información y las tecnologías de la entidad, garantizando su integridad, confidencialidad y disponibilidad; así como diseñar y ejecutar procedimientos orientados a minimizar riesgos, eventos e incidentes,

promoviendo a su vez una cultura organizacional de protección y uso adecuado de la información.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Transferir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

6.2. 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.

6.3. 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.

6.3.1. Análisis e Identificación de Riesgos

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 grupo 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.

ID	ESCENARIO DE RIESGO	PROBABILIDAD
R1_Tic´s	Uso indebido o inadecuado de la información empresarial.	Media
R2_Tic´s	Pérdida o alteración de la información crítica por acceso no autorizado.	Alta
R3_Tic´s	Insuficiencia de equipos, herramientas e infraestructura tecnológica.	Alta
R4_Tic´s	Daños, deterioro o pérdida de recursos tecnológicos.	Alta

6.3.2. Uso indebido o inadecuado de la información empresarial (R1_Tic´s)

6.3.2.1. Análisis e Identificación

Descripción: Acceso no autorizado que modifica o elimina información crítica.

Impacto: Alto (sanciones legales, pérdida de confianza, daño reputacional).

Probabilidad: Media.

Activos afectados: Bases de datos de los sistemas de información implementados, información comercial y operativa.

6.3.2.2. Controles Preventivos Existentes

- Políticas de seguridad y privacidad de la información formalizadas.
- Acuerdos de confidencialidad para empleados y contratistas.
- Control de accesos basado en roles.
- Capacitación periódica en protección de datos y ética de la información.
- Clasificación de la información (pública, interna, confidencial).

6.3.2.3. Controles Correctivos Existentes

- Procedimiento disciplinario ante incumplimientos.
- Revocación inmediata de accesos ante incidentes.
- Investigación y análisis forense sobre incidente.

6.3.2.4. Acciones de Mejora Existentes

- Programas de concientización continua sobre manejo de la información.
- Revisión permanente de perfiles de acceso y credenciales.
- Auditorías internas sobre uso de la información.

6.3.2.5. Entregables para el seguimiento

- Registro de capacitaciones.
- Matriz de control de accesos.
- Informes de auditoría interna.

- Registro de incidentes de uso indebido.

6.4. Pérdida o alteración de la información crítica por acceso no autorizado. (R2_Tic´s)

6.4.1. Análisis e Identificación

Descripción: Uso de la información por parte de funcionarios o terceros para fines no autorizados.

Impacto: Muy alto (interrupción del servicio, decisiones erróneas, sanciones).

Probabilidad: Alta.

Activos afectados: Sistemas de facturación, SCADA, bases de datos críticas.

6.4.2. Controles Preventivos Existentes

- Políticas Autenticación fuerte (MFA).
- Copias de seguridad automáticas y verificadas.
- Segmentación de redes.

6.4.3. Controles Correctivos Existentes

- Restauración de información desde respaldos.
- Bloqueo de cuentas comprometidas.

6.4.4. Acciones de Mejora Existentes

- Pruebas periódicas de restauración de backups.
- Mejora de la arquitectura de seguridad.
- Sistemas de detección de intrusos (IDS/IPS).
- Activación del plan de respuesta a incidentes.

6.4.5. Entregables para el seguimiento

- Plan de copias de seguridad.
- Registros de respaldos y restauraciones.
- Plan de respuesta a incidentes.
- Bitácora de accesos y eventos de seguridad.

6.5. Insuficiencia de equipos, herramientas e infraestructura tecnológica. (R3_Tic´s)

6.5.1. Análisis e Identificación

Descripción: Infraestructura obsoleta o insuficiente para soportar la operación.

Impacto: Alto (caídas del sistema, baja eficiencia, riesgos de seguridad).

Probabilidad: Alta.

Activos afectados: Servidores, redes, software crítico.

6.5.2. Controles Preventivos Existentes

- Inventario actualizado de activos tecnológicos.
- Evaluación periódica del desempeño de la infraestructura.
- Presupuesto anual de renovación tecnológica.

6.5.3. Controles Correctivos Existentes

- Reasignación temporal de recursos.
- Migración a soluciones en la nube (si aplica).

6.5.4. Acciones de Mejora Existentes

- Plan de capacidad y crecimiento tecnológico.
- Adquisición urgente de recursos tecnológicos.
- Plan estratégico de TI a mediano y largo plazo.
- Evaluación de nuevas tecnologías.

6.5.5. Entregables para el seguimiento

- Inventario de activos tecnológicos.
- Informes de desempeño de infraestructura.
- Actas de mantenimiento y soporte.
- Contrataciones suministro de activos tecnológicos.

6.6. Daños, deterioro o pérdida de recursos tecnológicos (R4_Tic´s)

6.6.1. Análisis e Identificación

Descripción: Daños físicos, robos, incendios, fallas eléctricas o desastres naturales.

Impacto: Alto.

Probabilidad: Alta.

Activos afectados: Equipos de cómputo, servidores, dispositivos de red.

6.6.2. Controles Preventivos Existentes

- Controles físicos de acceso.
- Seguros para activos tecnológicos.
- Almacenamiento seguro y etiquetado de activos.

6.6.3. Controles Correctivos Existentes

- Reemplazo o reparación de equipos.
- Uso de equipos de contingencia.

6.6.4. Acciones de Mejora Existentes

- UPS y sistemas de respaldo eléctrico.
- Simulacros de contingencia.
- Mejora de las condiciones físicas del CPD.
- Activación del plan de continuidad del negocio.
- Sistemas de monitoreo ambiental (temperatura, humedad).

6.6.5. Entregables para el seguimiento

- Inventario físico de activos.
- Plan de Continuidad del Negocio.
- Plan de Recuperación ante Desastres.
- Pólizas de seguros vigente.
- Informes de incidentes físicos.

6.7. Bienes susceptibles de un daño

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.

- 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.

6.8. GESTIÓN DEL RESPALDO

La gestión del 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 una gestión de respaldo.

6.9. Respaldo de datos vitales

Identificar los sistemas de información según su importancia en el suministro de datos para realizar respaldos:

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

6.10. 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 la gestión 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.

6.11. 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.

6.12. Responsables de la gestión de respaldos

La gestión 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.

6.13. 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.

6.14. Respaldos

6.14.1. 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.

6.14.2. 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.

6.15. GESTIÓN 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 esas gestiones 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.

La gestión de recuperación viene de la mano de la gestión de respaldo, pues de la información respaldada se realiza la recuperación en caso de algún inconveniente.

6.15.1. Activación de la gestión de recuperación

La activación de la gestión de recuperación se desarrolla acorde a las directrices definidas por el grupo TIC, determinado la activación en caso de una eventualidad, y además indicando el lugar alternativo de ejecución del respaldo y operación de emergencia, basándose en las recomendaciones indicadas por éste.

6.15.2. Aplicación de la gestión de recuperación

Se aplicará la gestión de recuperación 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.

6.15.3. 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.).

6.16. ESTRATEGIAS TIC'S

Dimensión de TI	Actividad	Entregable o Producto	Meta o Indicador	Fecha Inicio	Fecha Fin
Gestión administrativa, de alineamiento, organización y planeación de TI	Diseño de la matriz de riesgo de seguridad de la información	Matriz de riesgo de seguridad de la información	1 Documento creado	1/01/2026	31/03/2026
	Analizar los riesgos de manera estructurada	Informes de la matriz de tratamientos de riesgo de TIC con sus respectivos anexos	3 informes de seguimiento de la matriz de tratamientos de los	1/04/2026	31/12/2026

			riesgos TIC		
Administración de los datos	Inventario de activos de información	Documentar el inventario de los activos de información	1 informe de inventario de activos de la información	1/02/2026	31/07/2026
Administración de la seguridad y privacidad de la información	Programa de Capacitación y Formación en Seguridad de la Información	Diseñar un programa de capacitación en Seguridad de la Información.	1 capacitación realizada	1/03/2026	30/06/2026
	Diseño y Evaluación del Procedimiento de Respuesta a Incidentes	Procedimiento de respuestas a incidentes de seguridad de la información construido y aprobado	1 procedimiento implementado	1/04/2026	30/06/2026

Tabla 1 (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

Ítem que cambió	Descripción del cambio	Año de modificación
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
Introducción	Se hizo ajustes en el contenido	2025
Estrategias	Se hizo ajustes en el contenido	2025
Indicadores	Se hizo ajustes en el contenido	2025
Generalidades	Se hizo ajustes en el contenido	2026
Estrategias	Se hizo ajustes en el contenido	2026

8. Anexos

N/A