Emsercota S.A.

EMPRESA DE SERVICIOS PÚBLICOS

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

2026

INTRODUCCIÓN

En la gestión de riesgos de seguridad de la información se tratan aquellos procesos que ayudan a reducir las pérdidas y proporcionan protección a los datos en información y permiten dar a conocer las falencias y debilidades que se tienen en los ciclos de los servicios.

Por esta razón en importante contar con un plan de riesgos que permita dar continuidad al funcionamiento de la administración, debido a esto se desarrolla un análisis de riesgo de seguridad de la información aplicado en la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP.

Se busca identificar las respectivas amenazas, medir los riesgos existentes y sugerir las acciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

Este plan da una proyección que permite identificar los niveles de riesgo de la información y como está la seguridad existente, buscando incentivar a las personas involucradas a continuar con el uso de las normas y procedimientos pertinentes a la seguridad de la información y recursos.

1. OBJETIVOS

1.1 Objetivo General

Desarrollar un plan de gestión de seguridad y privacidad de la información que tenga como resultado la disminución de los riesgos de pérdida de información en la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP.

1.2 Objetivos Especificos

Identificar e implementar los medios y mecanismos técnicos, administrativos y organizacionales necesarios para proteger los activos de información digital de EMSERCOTA S.A. E.S.P., garantizando su confidencialidad, integridad y disponibilidad.

- Administrar de manera adecuada los riesgos asociados a la seguridad y privacidad de la información, con el fin de mantenerlos controlados dentro de niveles aceptables y minimizar su impacto en los procesos institucionales.

- Sensibilizar y capacitar al personal administrativo, contratistas y demás partes interesadas de EMSERCOTA S.A. E.S.P. sobre el Plan de Seguridad y Privacidad de la Información, fortaleciendo la cultura de protección y uso responsable de los activos de información.

- Realizar seguimiento permanente al cumplimiento de los estándares de seguridad de la información, mediante el uso de herramientas de diagnóstico, autoevaluaciones y controles definidos.

- Identificar, implementar y documentar acciones correctivas y de mejora continua que permitan fortalecer el Plan de Seguridad y Privacidad de la Información de la Entidad.

- Evaluar y comparar periódicamente el nivel de riesgo inicial y residual, con el fin de medir el impacto de los controles implementados dentro del Plan de Gestión de Seguridad y Privacidad de la Información.

2. ALCANCE

La implementación del Plan de Tratamiento del Riesgos de Seguridad y Privacidad de la Información está orientada al fortalecimiento de la protección de los activos de información de EMSERCOTA S.A. E.S.P., garantizando su confidencialidad, integridad y disponibilidad.

Este plan aplica a los procesos misionales, estratégicos y de apoyo de la Entidad, así como a los funcionarios, contratistas y terceros que tengan acceso a la información institucional, y se desarrolla de conformidad con la normatividad y los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en el marco de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI) vigente.

3. DEFINICIONES

- **Riesgo:** Posibilidad de que un evento o situación incierta ocurra y afecte negativamente el cumplimiento de los objetivos institucionales.
- **Gestión del riesgo:** Proceso desarrollado por la alta dirección y el personal de la Entidad, orientado a identificar, analizar, evaluar y tratar los riesgos, con el fin de proporcionar un aseguramiento razonable sobre el logro de los objetivos institucionales.
- **Riesgo estratégico:** Riesgo asociado a la forma en que se direcciona y administra la Entidad. Está relacionado con la misión, la visión, el cumplimiento de los objetivos estratégicos, la definición de políticas y la toma de decisiones por parte de la alta dirección.
- **Riesgo de imagen:** Riesgo relacionado con la percepción, reputación y nivel de confianza que tienen los usuarios, ciudadanos y demás partes interesadas frente a la gestión y servicios prestados por la Entidad.
- **Riesgo operativo:** Riesgo derivado del funcionamiento de los procesos, la operación de los sistemas de información, la infraestructura tecnológica, la estructura organizacional y la articulación entre las dependencias de la Entidad.
- **Riesgo financiero:** Riesgo relacionado con la administración de los recursos financieros de la Entidad, incluyendo la ejecución presupuestal, los estados financieros, los pagos, la gestión de tesorería y el manejo de los bienes institucionales.

- **Riesgo de cumplimiento:** Riesgo asociado al incumplimiento de disposiciones legales, contractuales, normativas, éticas y compromisos adquiridos por la Entidad frente a la comunidad y los entes de control.
- **Riesgo de seguridad digital:** Combinación de amenazas y vulnerabilidades presentes en el entorno digital que pueden afectar la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento de los objetivos institucionales. Incluye factores relacionados con las personas, los procesos, la tecnología y el entorno físico.
- **Riesgo inherente:** Nivel de riesgo existente antes de la implementación de controles o acciones de tratamiento.
- **Riesgo residual:** Nivel de riesgo que permanece después de aplicar los controles y acciones de tratamiento definidos.
- **Probabilidad:** Posibilidad de que un riesgo se materialice, la cual puede ser estimada con base en la frecuencia histórica o la factibilidad de ocurrencia.
- **Impacto:** Consecuencias que puede generar la materialización de un riesgo sobre los procesos, la operación, la información, la imagen o los recursos de la Entidad.
- **Causa:** Factores internos o externos que, de manera individual o combinada, pueden dar origen a la materialización de un riesgo.
- **Consecuencia:** Efectos o situaciones que se producen como resultado de la materialización de un riesgo y que afectan a la Entidad, sus procesos y grupos de interés.
- **Mapa de riesgos:** Documento que consolida la identificación, análisis, evaluación y tratamiento de los riesgos de la Entidad.
- **Activo:** Elemento que tiene valor para la Entidad y que es necesario para su operación, tales como información física o digital, aplicaciones, sistemas, redes, equipos, servicios tecnológicos y recurso humano.
- **Control:** Medida administrativa, técnica u organizacional que permite prevenir, detectar o corregir un riesgo, reduciendo su probabilidad o impacto.
- **Vulnerabilidad:** Debilidad o ausencia de controles que puede ser explotada por una amenaza y afectar los activos de la Entidad.
- **Amenaza:** Evento o situación potencial que puede generar un incidente de seguridad y causar daño a los activos de información o a la operación institucional.

4. MARCO NORMATIVO

MARCO NORMATIVO	AÑO	DESCRIPCIÓN
Constitución Política – Art. 15	1991	Garantiza el derecho a la intimidad, habeas data y protección de datos personales.
Ley Estatutaria 1581	2012	Establece el régimen general de protección de datos personales.
LEY 1712	2014	Regula la transparencia y el acceso a la información pública.
Decreto 1078	2015	Decreto Único Reglamentario del Sector TIC.
CONPES 3854	2016	Política Nacional de Seguridad Digital.
Ley 1928	2018	Aprueba el Convenio de Budapest sobre ciberdelincuencia.
Resolución 500	2021	Adopta el Modelo de Seguridad y Privacidad de la Información (MSPI).
Decreto 767	2022	Lineamientos de la Política de Gobierno Digital.
NTC ISO/IEC 27001	2022	Estándar para la gestión de la seguridad de la información y el tratamiento de riesgos.

5. AUTODIAGNÓSTICO ACTIVOS DE INFORMACIÓN, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El autodiagnóstico realizado en EMSERCOTA S.A. E.S.P. permitió comprender de manera clara cómo se están gestionando actualmente los activos de información y el nivel de avance en materia de seguridad y privacidad de la información. A continuación, se presenta un cuadro resumen en el que se relaciona la información obtenida, la cual sirve como base para la identificación de riesgos y la definición de acciones dentro del Plan de Tratamiento de Riesgos.

5.1 Activos de información

1. ACTIVOS DE INFORMACIÓN	ESTADO ACTUAL
HARDWARE	EMSERCOTA S.A. E.S.P. cuenta con un total de veintiséis (26) equipos de cómputo, los cuales se encuentran asignados a las diferentes áreas de la entidad y a cargo de funcionarios responsables para la ejecución de sus labores diarias. A continuación, se relacionan los equipos de cómputo con su respectiva ubicación y área, conforme a lo registrado en el inventario institucional: Los equipos de cómputo se encuentran ubicados en las siguientes áreas: PQR, Viabilidades, Auxiliar Comercial, Siso, Facturación, Gerencia, Prensa, Auxiliar PGIRS, Almacén, Contador, Subgerencia Técnica, Auxiliar Jurídico, Rack, Subgerente Corporativo, director Financiero, Jurídico, Archivo, Profesional Universitario del área operativa, Técnico de Aseo, Técnico de Acueducto, Talento Humano, Control Interno y Sistemas. Adicionalmente, la entidad cuenta con dos (02) servidores ubicados en el data center. Uno de los servidores está destinado al funcionamiento del sistema de información financiero y administrativo, el cual soporta los procesos contables y financieros de la empresa; mientras que el segundo servidor se utiliza para el almacenamiento y gestión de la información institucional de EMSERCOTA S.A. E.S.P. En cuanto a la conectividad inalámbrica, la empresa dispone de tres (03) routers para la distribución de la red WiFi. Uno de ellos se encuentra ubicado en el área administrativa, otro en el área operativa y el tercero en el área comercial, la conectividad necesaria para el desarrollo de las actividades administrativas, técnicas y operativas de la entidad. EMSERCOTA S.A. E.S.P. cuenta también con cuatro (04) impresoras distribuidas de la siguiente manera: Dos (02) impresoras Ricoh MP 320, de tamaño pequeño, una ubicada en el área administrativa y otra en el área operativa. Debido al alto volumen de impresión y los costos asociados a insumos como tóner y mantenimiento, se ha tomado la decisión de contratar en alquiler dos impresoras más robustas para estas áreas. Una (01) impresora HP LaserJet MFP M426fdw, ubicada en el área Jurídica y Control Interno, la cual presenta fallas en su funcionamiento. Una (01) impresora ECOSYS M3550idn, ubicada en el área comercial, la cual funciona normalmente.

	El data center cuenta con equipos destinados a la distribución de la red LAN y a las telecomunicaciones de la empresa. Actualmente, estos equipos están funcionando correctamente, asegurando la conectividad interna y el soporte de los servicios de red. No obstante, se ha identificado la necesidad de verificar la posible actualización del rack y sus componentes, con el fin de optimizar su rendimiento y garantizar una infraestructura más robusta a mediano y largo plazo, aunque a la fecha sigue funcionando de manera operativa. Si bien algunos equipos presentan mayor antigüedad, actualmente se encuentran en correcto funcionamiento y cumplen de manera adecuada con las labores asignadas, garantizando la continuidad de los procesos y el normal desarrollo de las actividades institucionales.
SOFTWARE	EMSERCOTA S.A. E.S.P. cuenta con equipos de cómputo que operan con sistemas operativos Windows 10 y Windows 11 debidamente licenciados, configurados de manera adecuada para su óptimo funcionamiento como plataformas de trabajo institucional. Los equipos disponen de software de ofimática con licencias activas de Microsoft Office, correspondientes a las versiones Office 2021 y Office 2016, las cuales cumplen con los requerimientos tecnológicos actuales de la entidad. Adicionalmente, los equipos cuentan con programas de licencia abierta y de uso general, tales como descompresores de archivos, herramientas de conexión remota y navegadores web, necesarios para el desarrollo de las actividades administrativas y operativas. Para los procesos financieros y administrativos, la entidad utiliza el Sistema de Información financiero y Administrativo, cuyas terminales se encuentran instaladas en cada equipo de cómputo que lo requiere. Este software cuenta con licenciamiento vigente por parte del contratista proveedor, garantizando su uso legal y funcionamiento adecuado. La entidad cuenta igualmente con escáneres, los cuales tienen sus respectivos controladores e instaladores activos, encontrándose en correcto estado de funcionamiento para la digitalización de documentos institucionales. En todos los equipos se dispone de software antivirus activo, contribuyendo a la protección de la información y a la seguridad de los sistemas. Asimismo, los equipos cuentan con utilitarios para la apertura y lectura de documentos PDF, reproducción de archivos multimedia y demás aplicaciones necesarias para el normal desarrollo de las labores. A nivel de sistema operativo, los equipos cuentan con configuraciones adecuadas, y el software instalado se encuentra sujeto a soporte técnico, garantizando la continuidad y estabilidad de los servicios tecnológicos

5.2 Seguridad y privacidad de la información

2. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	ESTADO ACTUAL
PROTECCIÓN DE ADENTRO HACIA AFUERA	EMSERCOTA S.A. E.S.P. cuenta con medidas de seguridad implementadas en sus equipos de cómputo a nivel de sistema operativo, mediante el uso de usuarios y contraseñas que permiten el control de acceso y el inicio de sesión únicamente a personal autorizado. Así mismo, los equipos disponen de configuraciones básicas de seguridad y mecanismos de respaldo de la información que contribuyen a la protección de los datos institucionales. De igual manera, se cuenta con controles de seguridad en la red interna, orientados a prevenir accesos no autorizados y minimizar los riesgos asociados a la pérdida, alteración o uso indebido de la información. Cabe resaltar que los equipos de cómputo y la información que en ellos se administra son manipulados exclusivamente por el personal autorizado de EMSERCOTA S.A. E.S.P. El mantenimiento preventivo y correctivo de los equipos se realiza dentro de las instalaciones de la entidad, garantizando el control, la confidencialidad y la integridad de la información institucional
PROTECCIÓN DE AFUERA HACIA ADENTRO	En EMSERCOTA S.A. E.S.P. ningún equipo de cómputo es manipulado por agentes externos no autorizados. El manejo de los equipos y de la información que en ellos se administra está a cargo exclusivamente del personal de la Entidad y del personal de soporte técnico debidamente autorizado. En los casos en que se requiera la conexión de unidades de almacenamiento externas, los equipos cuentan con sistemas operativos protegidos mediante antivirus actualizados, lo que permite la detección y prevención de posibles amenazas informáticas.
ANTIVIRUS	Los equipos de cómputo de EMSERCOTA S.A. E.S.P. cuentan con herramientas de protección antivirus como Kaspersky, debidamente configuradas y con sus escudos de seguridad activos, con el propósito de prevenir el robo de información y la infección por virus informáticos que puedan afectar la integridad, confidencialidad y disponibilidad de los datos institucionales. El antivirus Kaspersky se administra de manera centralizada a través de una consola de gestión, desde la cual se controlan y supervisan todas sus funcionalidades, tales como la actualización permanente de firmas, la configuración de políticas de seguridad, el monitoreo de amenazas, el análisis de equipos y la generación de alertas ante posibles incidentes de seguridad.

	Esta administración centralizada permite garantizar que todos los equipos se mantengan protegidos de forma homogénea y oportuna. Adicionalmente, el sistema antivirus bloquea automáticamente páginas web, enlaces y software malicioso que intenten acceder a los equipos o vulnerar la información administrada por la Entidad, fortaleciendo así las medidas de seguridad informática y la protección de los activos de información de EMSERCOTA S.A. E.S.P.
LICENCIAMIENTO	Todos los equipos de cómputo de EMSERCOTA S.A. E.S.P. cuentan con software debidamente licenciado, incluyendo los sistemas operativos Windows 10 y Windows 11, así como los paquetes Microsoft Office 2016 y 2021, garantizando su correcto funcionamiento y el cumplimiento de la normativa vigente en materia de uso legal de software. Adicionalmente, algunos programas instalados corresponden a software de uso o licencia gratuita, los cuales son necesarios para apoyar las actividades operativas y administrativas de la Entidad y no representan riesgos legales ni técnicos. El licenciamiento del sistema operativo y del paquete de ofimática es un aspecto primordial, ya que permite el acceso permanente a las actualizaciones de seguridad, mejoras de rendimiento y nuevas funcionalidades, contribuyendo a la protección de la información, la estabilidad de los equipos y la continuidad de los servicios que presta EMSERCOTA S.A. E.S.P..
BACK UP	Uno de los servidores de EMSERCOTA S.A. E.S.P. dispone de un espacio de almacenamiento conformado por cuatro (4) discos duros de 1 TB cada uno, los cuales se utilizan para realizar las copias de seguridad de la información más relevante y crítica de la Entidad. No obstante, es importante resaltar que la capacidad de almacenamiento actualmente disponible resulta limitada frente a las necesidades reales de la empresa, teniendo en cuenta el crecimiento constante de la información, los respaldos históricos y los requerimientos operativos y administrativos. Esta situación hace necesario evaluar, a mediano plazo, la ampliación o fortalecimiento de la infraestructura de almacenamiento, con el fin de garantizar la continuidad del servicio, la integridad de la información y una gestión adecuada de los respaldos institucionales.

6. IDENTIFICACIÓN, ANÁLISIS, VALORACIÓN DE CONTROLES, SEGUIMIENTO Y DEFINICIÓN DEL MAPA DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

6.1 Identificación del Riesgo: Esta etapa permite establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias.

A continuación se referencian los riesgos identificados en la Corporación por concepto de seguridad y privacidad de la información, los cuales se relacionan así:

RIESGOS	Falla en los equipos de cómputo por obsolescencia
	Pérdida de información por fallas en el respaldo
	Interrupción en el servicio de internet
	Acceso no autorizado a información sensible
	Pérdida de información por malware
	Fuga de información confidencial
	Error humano en gestión de información

6.2 *Valoración del Riesgo*: Busca establecer la probabilidad de ocurrencia del riego y el nivel de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial

6.2.1 *Análisis del Riesgo:* Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

- *Impacto:* Es la consecuencia que puede ocasionar a la Corporación la materialización del Riesgo, valorado de la siguiente manera: Insignificante: 1, Menor: 2, Moderado: 3, Mayor: 4 y Catastrófico: 5.

- *Probabilidad: E*ntendida como la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia. Se valora de la siguiente forma: Rara vez: 1, Improbable: 2, Posible: 3, Probable: 4 y Casi seguro: 5.

6.2.2 *Evaluación del Riesgo:* Resultado obtenido en la Matriz de Calificación, Evaluación y Respuesta a los Riesgos.

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi seguro (5)	A	A	E	E	E
Probable (4)	M	A	A	E	E
Posible (3)	B	M	A	E	E
Improbable (2)	B	B	M	A	E
Rara vez (1)	B	B	M	A	A

E: ZONA DE RIESGOS EXTREMA: Reducir el riesgo, Evitar, Compartir o Transferir
A: ZONA DE RIESGO ALTA: Reducir el riesgo, Evitar, Compartir o transferir
M: ZONA DE RIESGO MODERADA: Asumir el riesgo, Reducir el riesgo
B: ZONA DE RIESGO BAJA: Asumir el riesgo.

Opciones de manejo: Son las posibles respuestas de manejo ante los riesgos tendientes a evitar, reducir, dispersar o transferir el riesgo, o asumir el riego residual.

• *Evitar el Riesgo*: tomar las medidas encaminadas a evitar su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

• *Reducir el Riesgo*: implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades, se consigue mediante la optimización de los procedimientos y la implementación de controles.

• *Compartir o transferir el Riesgo*: reduce su efecto a través del traspaso a otros procesos.
• *Asumir un Riesgo*: luego de que el riesgo ha sido reducido o transferido, puede quedar un riesgo residual que se mantiene, en este caso el líder del proceso simplemente acepta la pérdida Residual probable y elabora planes de contingencia para su manejo.

De esta forma; se presenta la matriz a través de la cual se adelanta el análisis y la valoración del riesgo:

No. DEL RIESGO	NOMBRE DEL RIESGO	CALIFICACION		TIPO IMPACTO		EVALUACIÓN		MEDIDAS DE RESPUESTA
		PROBABILIDAD (1-5)	IMPACTO (1-5)	CATEGORÍA	SUBCATEGORÍA	PERFIL DEL RIESGO (1-100)	ZONA RIESGO	MEDIDA
R1	Falla en los equipos de computo por obsolescencia	2	3	OPERATIVO	INTERMITENCIA EN EL SERVICIO	24	ZONA RIESGO MODERADA	REDUCIR EL RIESGO
R2	Perdida de información por fallas en el respaldo	2	4	OPERATIVO	CAMBIOS EN LA INTERACCION DE LOS PROCESOS	32	ZONA RIESGO ALTA	COMPARTIR O TRANSFERIR EL RIESGO
R3	Interrupcion en el servicio de internet	3	3	OPERATIVO	INTERMITENCIA EN EL SERVICIO	30	ZONA RIESGO ALTA	REDUCIR EL RIESGO
R4	Acceso no autorizado a información sensible	3	4	CONFIDENCIALIDAD	INSTITUCIONAL	48	ZONA RIESGO EXTREMA	REDUCIR EL RIESGO
R5	Pérdida de información por malware	3	4	OPERATIVO	INTERMITENCIA EN EL SERVICIO	48	ZONA RIESGO EXTREMA	REDUCIR EL RIESGO
R6	Fuga de información confidencial	3	4	CONFIDENCIALIDAD	INSTITUCIONAL	48	ZONA RIESGO EXTREMA	COMPARTIR O TRANSFERIR EL RIESGO
R7	Error humano en gestion de información	2	3	OPERATIVO	AJUSTES DE UNA ACTIVIDAD CONCRETA	36	ZONA RIESGO ALTA	REDUCIR EL RIESGO

6.3 Análisis y evaluación de los controles: La valoración del riesgo requiere de una evaluación de los controles existentes, lo cual implica:

- Determinar su naturaleza: Si se trata de un control preventivo o correctivo.
- Determinar si los controles están documentados, de forma tal que es posible conocer cómo se lleva a cabo el control, quién es el responsable de su ejecución y cuál es la periodicidad para su ejecución, lo cual determinará las evidencias que van a respaldar la ejecución del mismo.
- Establecer si el control que se implementa es automático o manual.
- Determinar si los controles se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo.
- Determinación de riesgo residual: Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

A continuación se presenta la matriz en la cual es posible evidenciar la definición de los controles para cada uno de los riesgos:

No. DEL RIESGO	NOMBRE DEL RIESGO	VALIDACION DE CONTROLES												CALIFICACIÓN DEL CONTROL	CONTROL DEL RIESGO	CONTROL DEL PROCESO
		DESCRIPCIÓN (Control al riesgo)	HERRAMIENTAS PARA EJERCER CONTROL			SEGUIMIENTO AL CONTROL		CALIFICACIÓN DEL ESTADO								
			HERRAMIENTAS	MANUALES O PROCEDIMIENTOS	NON EFECTIVOS	NO RESPONSABLES	ES NECESARIO									
R1	Falla en los equipos de computo por obsolescencia	1. Proponer un plan de renovacion tecnologica	N	M	NC	NC	NC	15	15	5	5	5	30			
		2. Destinar presupuesto especifico para actualizar los equipos de computo asignados a los Concejales	N	N	NC	NC	NC	15	15	5	5	5	N			
		3. Backup de información critica	M	M	NC	M	M	15	15	5	15	25	75			
R2	Perdida de información por fallas en el respaldo	1. Diseñar una politica formal de respaldo	M	M	NC	M	M	15	15	5	15	25	75			
		2. Implementar la politica formal de respaldo	N	M	NC	M	M	15	15	5	15	25	75			
		3. Validación periodica de respaldos	N	M	NC	M	M	15	15	5	15	25	75			
R3	Interrupción en el servicio de internet	1. Optimizar el canal de respaldo	N	M	NC	M	M	15	15	5	15	25	75			
		2. Evaluar la redundancia adicional	N	M	NC	M	M	15	15	5	15	25	75			
		3. Adquirir una red de respaldo para el servicio de internet	N	M	NC	M	M	15	15	5	15	25	75			
R4	Acceso no autorizado a información sensible	1. Diseñar una politica de control de acceso	N	M	NC	M	M	15	15	5	15	25	75			
		2. Implementar la politica de control de acceso	M	M	NC	M	M	15	15	5	15	25	75			
		3. Registrar los accesos	M	M	NC	M	M	15	15	5	15	25	75			
R5	Perdida de información por malware	1. Capacitar a Concejales y Equipo administrativo en "Seguridad y Privacidad de la información"	N	N	N	N	M	15	15	30	15	25	150			
								0	0	0	0	0	0			
								0	0	0	0	0	0			
R6	Fuga de información confidencial	1. Diseñar una politica de clasificación	N	M	NC	M	M	15	15	5	15	25	75			
		2. Control de dispositivos USB	M	M	NC	M	M	15	15	5	15	25	75			
		3. Realizar monitoreos de actividad	N	N	NC	M	M	15	15	5	15	25	75			
R7	Error humano en gestion de información	1. Disponer de procedimientos documentados	N	N	N	M	M	15	15	30	15	25	150			
		2. Capacitacion periodica	N	N	NC	M	M	15	15	5	15	25	75			
								0	0	0	0	0	0			

De otro lado; una vez evaluados los riesgos después de implementar los controles se observan los siguientes resultados:

No. DEL RIESGO	NOMBRE DEL RIESGO	CALIFICACION		ZONA RIESGO	CONTROL PARA MITIGAR	CONTROLES	CALIFICACIÓN			
		PROBABILIDAD (1-5)	IMPACTO (1-5)				PUNTAJE HERRAMIENTA	PUNTAJE SEGUIMIENTO CONTROL	PUNTAJE FINAL	CONTROL DEL PROCESO
R1	Falla en los equipos de computo por obsolescencia	2	2	ZONA RIESGO BAJA	IMPACTO	1. Proponer un plan de renovacion tecnologica 2. Destinar presupuesto especifico para actualizar los equipos de computo asignados a los Concejales 3. Backup de información critica	30	[illegible]	42	35,7
R2	Perdida de información por fallas en el respaldo	2	3	ZONA DE RIESGO MODERADA	IMPACTO	1. Diseñar una politica formal de respaldo 2. Implementar la politica formal de respaldo 3. Validación periodica de respaldos	30	40	70	
R3	Interrupción en el servicio de internet	2	3	ZONA DE RIESGO MODERADA	PROBABILIDAD	1. Optimizar el canal de respaldo 2. Evaluar la redundancia adicional3. Adquirir una red de respaldo para el servicio de internet	30	40	70	
R4	Acceso no autorizado a información sensible	2	4	ZONA DE RIESGO ALTA	PROBABILIDAD	1. Diseñar una politica de control de acceso 2. Implementar la politica de control de acceso 3. Registrar los accesos	30	40	70	
R5	Perdida de información por malware	2	4	ZONA DE RIESGO ALTA	PROBABILIDAD	1. Capacitar a Concejales y Equipo administrativo en "Seguridad y Privacidad de la información"	60	40	100	
R6	Fuga de información confidencial	2	4	ZONA DE RIESGO ALTA	PROBABILIDAD	1. Diseñar una politica de clasificación 2. Control de dispositivos USB 3. Realizar monitoreos de actividad	10	13	23	
R7	Error humano en gestion de información	2	3	ZONA DE RIESGO MODERADA	PROBABILIDAD	1. Disponer de procedimientos documentados 2. Capacitacion periodica	20	26,66666667	47	

6.4 Mapa de Riesgos: Es una representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa.

El mapa de riesgos correspondiente a la seguridad y privacidad de la información para el Concejo Municipal de Sopó quedó constituido así:

No. DEL RIESGO	NOMBRE DEL RIESGO	CALIFICACION		EVALUACIÓN Y CONTROLES			NUEVA CALIFICACIÓN			NUEVA EVALUACIÓN	OPCIONES MANEJO
		PROBABILIDAD (1-5)	IMPACTO (1-5)	EVALUACION RIESGO	CONTROLES	REDUCE	PROBABILIDAD	IMPACTO	PERFIL DEL RIESGO (1-100)		
R1	Falla en los equipos de computo por obsolescencia	3	3	ZONA RIESGO MODERADA	1. Proponer un plan de renovación tecnológica 2. Destinar presupuesto específico para actualizar los equipos de computo asignados a los Concejales 3. Backup de información crítica	IMPACTO	3	2	18	ZONA RIESGO BAJA	ASUMIR EL RIESGO
R2	Perdida de información por fallas en el equipo	3	4	ZONA RIESGO ALTA	1. Diseñar una política formal de respaldo 2. Implementar la política formal de respaldo 3. Validación periódica de respaldos	IMPACTO	3	3	24	ZONA RIESGO MODERADA	REDUCIR EL RIESGO
R3	Interrupción en el servicio de internet	3	3	ZONA RIESGO ALTA	1. Gestionar el canal de respaldo 2. Evaluar la redundancia adicional. 3. Adquirir una red de respaldo para el servicio de internet	PROBABILIDAD	3	3	24	ZONA RIESGO MODERADA	REDUCIR EL RIESGO
R4	Acceso no autorizado a información confidencial	3	4	ZONA RIESGO EXTREMA	1. Diseñar una política de control de acceso 2. Implementar la política de control de acceso 3. Registrar los accesos	PROBABILIDAD	3	4	32	ZONA RIESGO ALTA	REDUCIR EL RIESGO
R5	Perdida de información por malware	3	4	ZONA RIESGO EXTREMA	1. Capacitar a Concejales y Equipo administrativo en "Seguridad y Privacidad de la Información"	PROBABILIDAD	3	4	32	ZONA RIESGO ALTA	REDUCIR EL RIESGO
R6	Fuga de información confidencial	3	4	ZONA RIESGO EXTREMA	1. Diseñar una política de clasificación 2. Control de dispositivos USB 3. Realizar monitoreo de actividad	PROBABILIDAD	3	4	32	ZONA DE RIESGO ALTA	REDUCIR EL RIESGO
R7	Error humano en gestión de información	3	3	ZONA RIESGO ALTA	1. Disponer de procedimientos documentados 2. Capacitación periódica	PROBABILIDAD	3	3	24	ZONA DE RIESGO MODERADA	REDUCIR EL RIESGO

6.5 Seguimiento: A través de este mecanismo se debe asegurar que las acciones establecidas en el mapa de riesgos se están desarrollando y evaluar la eficiencia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo debe estar a cargo de la Secretaría Administrativa y Financiera de la Corporación.

TRATAMIENTO DE LOS RIESGOS						CONTROLES		TRIMESTRE				SEGUIMIENTO
No. DEL RIESGO	NOMBRE DEL RIESGO	PERFIL DEL RIESGO	CAUSAS	MEDIDAS DE MITIGACIÓN	RESPONSABLE IMPLEMENTACIÓN	CONTROLES	CALIFICACIÓN DEL CONTROL	I	II	III	IV	DESCRIPCION DEL SEGUIMIENTO
R1	Pérdida de información por falla en el equipo	OPERATIVO	1. Equipos que han superado su vida útil 2. Falta de renovación tecnológica 3. Presupuesto limitado	REDUCIR EL RIESGO	Mesa Directiva/ Contratista	1. Proponer un plan de renovación tecnológica. 2. Destinar presupuesto específico para actualizar los equipos de cómputo asignados a los Concejales 3. Backup de información crítica	40					
R2	Pérdida de información por falta de un respaldo	OPERATIVO	1. Capacidad limitada de almacenamiento 2. Falta de políticas de respaldo 3. No disponer de un manual de respaldo	COMPARTIR O TRANSFERIR EL RIESGO	Contratista	1. Diseñar una política formal de respaldo 2. Implementar la política formal de respaldo 3. Realizar verificación periódica de respaldos	70					
R3	Interrupción en el servicio de internet	OPERATIVO	1. Dependencia de un único proveedor 2. Infraestructura de red obsolescente	REDUCIR EL RIESGO	Mesa Directiva/ Contratista	1. Optimizar el canal de respaldo 2. Evaluar la redundancia adicional 3. Adquirir una red de respaldo para el servicio de internet	70					
R4	Acceso no autorizado a información sensible	CONFIDENCIALIDAD	1. Falta de políticas de acceso 2. Controles de seguridad débiles	REDUCIR EL RIESGO	Contratista	1. Diseñar una política de control de acceso 2. Implementar la política de control de acceso 3. Registrar los accesos	70					
R5	Pérdida de información por malware	INFORMÁTICA EN EL SERVICIO	1. Falta de actualización en la seguridad 2. Usuarios sin capacitación	REDUCIR EL RIESGO	Mesa Directiva/ Contratista	1. Capacitar a Concejales y Equipo administrativo en "Seguridad y Privacidad de la Información"	100					
R6	Fuga de información confidencial	INSTITUCIONAL	1. Falta de clasificación de información 2. Control inadecuado de dispositivos	COMPARTIR O TRANSFERIR EL RIESGO	Contratista	1. Diseñar una política de clasificación 2. Control de dispositivos USB 3. Realizar monitoreos de actividad	20					
R7	Error humano en gestión de información	AJUSTES DE UNA ACTIVIDAD CONCRETA	1. Falta de capacitación 2. Procesos no documentados	REDUCIR EL RIESGO	Equipo Administrativo/Contratistas	1. Disponer de procedimientos documentados 2. Capacitación periódica	47					

FUNCIONARIO	NOMBRE Y CARGO	FIRMA
PROYECTÓ	Yamir Geovanny Quevedo Agudelo – Técnico en Sistemas – EMSERCOTA S.A E.S.P.	
REVISÓ	Sandra Lorena Mondragón H- Jefe de Oficina de Control Interno- – EMSERCOTA S.A E.S.P.	
APROBÓ	Andrés Felipe Rincón Damián – Gerente- EMSERCOTA S.A E.S.P.	