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

ELABORÓ
GLORIA ELENA GIL PEMBERTY

ANDRES ALFONSO VILLA CASTRO

GERENTE

DONMATÍAS 2026

INTRODUCCIÓN

En observación del marco normativo restablecido en el Modelo Integrado de Planeación y Gestión y específicamente de acuerdo con el Decreto 612 de 2018, las entidades del estado deben desarrollar políticas para gestión de la seguridad y privacidad de la información, así como para el cumplimiento de las directrices de Gobierno Digital.

La E.S.E Hospital Francisco Eladio Barrera de Donmatías formula el presente Plan, en desarrollo del Modelo Integrado de Planeación y Gestión y con el propósito de fortalecer la gestión de las Tecnologías de la Información y las Comunicaciones, las demás políticas relacionadas con las directrices de Gobierno Digital, así como la seguridad privacidad de la información.

El Plan de tratamiento de riesgos de seguridad y privacidad de la información de la E.S.E Hospital Francisco Eladio Barrera de Donmatías establece las acciones para reducir la afectación de la entidad en caso de materialización, desarrollando estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos, basado en el inventario de activos de información.

ALCANCE

El Plan de tratamiento de riesgos seguridad y privacidad de la información de la E.S.E Hospital Francisco Eladio Barrera, se proyecta para la vigencia 2026 y se aplica a todos los activos de información identificados en las diferentes dependencias de la entidad.

DEFINICIONES

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

•Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

OBJETIVO

Establecer las actividades para el tratamiento de riesgos la Seguridad y Privacidad de la Información de la E.S.E Hospital Francisco Eladio Barrera del municipio de Donmatías, alineadas con las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

CONTEXTO ESTRATÉGICO DE LA ENTIDAD

La EMPRESA SOCIAL DEL ESTADO HOSPITAL FRANCISCO ELADIO BARRERA del Municipio de Donmatías, obtuvo su personería jurídica por medio de la Resolución No. 0916 del 18 de abril de 1955, emanada de la Gobernación de Antioquia y publicada en la Gaceta departamental. Es una entidad sin ánimo de lucro dedicada a prestar servicios de salud a la comunidad.
Mediante Acuerdo 013 del 27 de agosto de 1994, el Honorable Concejo Municipal del Municipio de Donmatías, reestructuro la entidad transformándola en una EMPRESA SOCIAL DEL ESTADO, descentralizada del orden municipal, dotada de personería jurídica, patrimonio propio y autonomía administrativa, sometida al régimen jurídico previsto en el Capítulo III, Titulo II. Libro segundo de la Ley 100 del 23 de diciembre de 1993.
La representación legal la tiene el Gerente de la E.S.E. Hospital Francisco Eladio Barrera, cargo que en la actualidad ocupa el doctor ANDRES ALFONSO VILLA CASTRO, nombrado mediante decreto Municipal No. 066 del 01 de abril de 2024.
La Empresa Social del Estado Hospital Francisco Eladio Barrera es un Hospital de Primer Nivel de Atención que se encarga de la atención de baja complejidad en el Municipio de Donmatías. Es una IPS con una sede única ubicada en la cabecera municipal.
Oferta servicios de: urgencias, laboratorio clínico, medicina general, odontología general, Rayos X general y odontológica, servicio farmacéutico, vacunación, servicios de promoción y prevención, terapia física, transporte asistencial básico TAB, nutrición, psicología, proceso de esterilización.
Cuenta con capacidad instalada para los servicios de hospitalización general adultos, pediatría y obstetricia y sala de partos, además, se realizan actividades extramurales, que se ejecutan para brindar atención en salud pública contempladas como actividades de promoción y prevención en la resolución 2003 y brigadas de salud a poblaciones remotas.

MISIÓN

Garantizar la prestación de servicios de salud de primer nivel de atención a los habitantes del municipio de Donmatías y demás usuarios, mediante un modelo de atención integral orientado en la promoción y mantenimiento de la salud, contando con tecnología adecuada y talento humano idóneo y comprometido en brindar atención de excelente calidad.

VISIÓN

En el año 2028 nos reconocemos por el compromiso hacia la seguridad y la humanización en la prestación de servicios de salud, el mejoramiento continuo de los procesos, la integridad del recurso humano, la sostenibilidad empresarial y la contribución al bienestar de los usuarios.

POLÍTICA DE CALIDAD

La E.S.E Hospital Francisco Eladio Barrera de Donmatías, se compromete a orientar su gestión a la obtención de beneficios y resultados de calidad para la comunidad, mediante la innovación, el control constante a la prestación de los servicios de salud y el mejoramiento de la calidad de vida de sus usuarios, la selección objetiva de sus proveedores, el continuo mejoramiento de las habilidades, competencias de sus servidores públicos, la aplicación de logística y tecnología apropiadas.

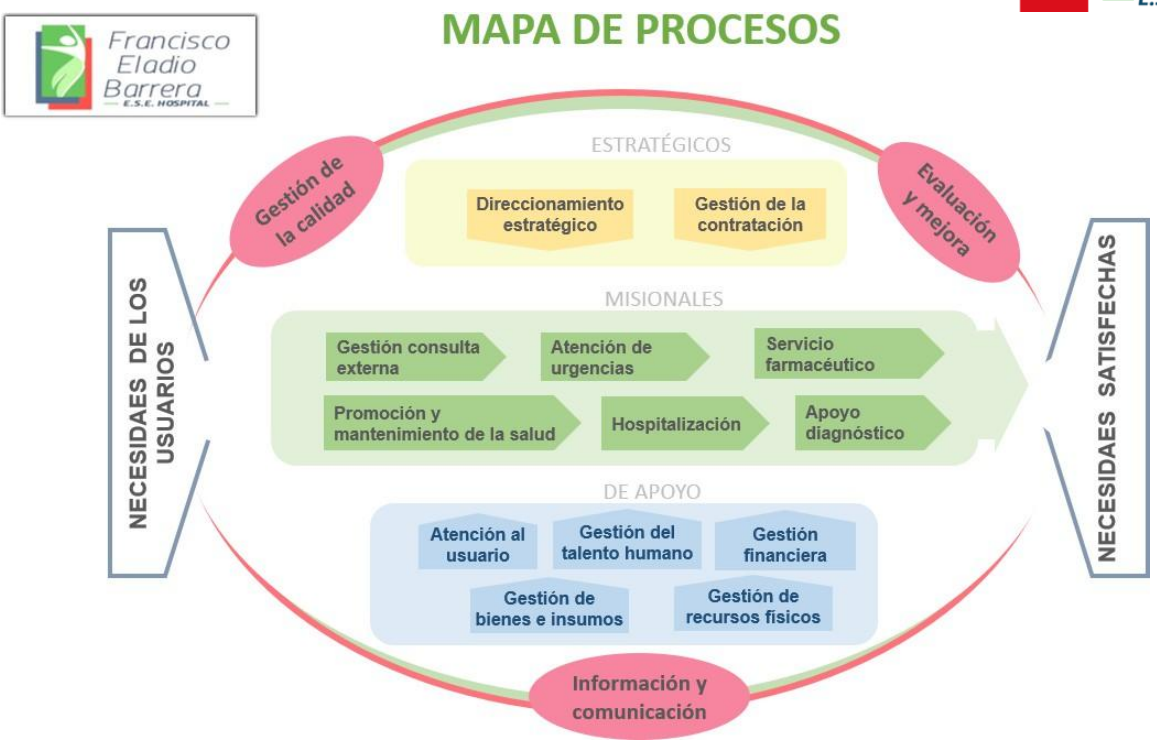
Somos un equipo humano interdisciplinario comprometido con lograr la satisfacción y seguridad de nuestros usuarios internos y externos, con personal idóneo, capacitado y entrenado en el manejo de tecnologías biomédicas, que garantiza la responsabilidad social, la mejora continua y la oportuna prestación de servicios de salud en cumplimiento de la normatividad vigente.

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

“La Dirección de la Empresa Social del Estado Hospital Francisco Eladio Barrera del Municipio de Donmatías, en coherencia con su misión, visión, políticas y objetivos, se compromete a proteger los usuarios, colaboradores y bienes de la entidad, de los potenciales riesgos que puedan afectar el desempeño de las funciones y el logro de los propósitos institucionales; estableciendo y promoviendo la aplicación de los mecanismos necesarios para evitar, reducir, compartir, transferir y/o asumir los riesgos relacionados con el desarrollo de sus procesos tanto a nivel de riesgos de gestión como de corrupción y seguridad digital. Para tal efecto realizará la identificación, análisis, valoración e intervención de los riesgos inherentes al quehacer institucional, aplicando la metodología establecida en el marco del modelo integrado de planeación y gestión MIPG”.

MODELO DE OPERACIÓN DE LA ENTIDAD

La E.S.E Hospital Francisco Eladio Barrera adoptó su modelo de operación por procesos mediante la Resolución 080 de 2022. En este modelo se concibe el proceso de Gestión de la información y la comunicación, de acuerdo con el siguiente esquema:



POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

REGULACION
Las políticas contenidas en este documento deberán ser conocidas, aceptadas y cumplidas por todos los colaboradores de la E.S.E. El incumplimiento de estas, se considerará un incidente de seguridad que de acuerdo con el caso podrá dar lugar a un proceso disciplinario para los funcionarios de acuerdo con el manual y/o política de confidencialidad de la E.S.E

POLITICAS GENERALES DE SEGURIDAD DE LA INFORMACION

El uso aceptable de los activos informáticos de la E.S.E implica la aceptación implícita por parte de los usuarios de estos, de las normas, políticas y estándares establecidos para garantizar la seguridad informática y el buen uso de estos, así como de los compromisos y responsabilidades adquiridas.
Los siguientes se consideran actos de obligatorio cumplimiento para el uso de los activos informáticos y están expresamente prohibidos así:
El intento o violación de los controles de seguridad establecidos para la protección de los activos informáticos
El uso sin autorización de los activos informáticos.
El uso no autorizado o impropio de la conexión al sistema.
Intentar evadir o violar la seguridad o autenticación de usuario de cualquier host, red o cuenta. El uso indebido de las contraseñas, firmas digitales o dispositivos de autenticación.

Está prohibido a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios.
Está prohibido el uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos o vulnere la seguridad de los sistemas.
El hurto, robo, sustracción o uso no autorizado de: datos, información, materiales, equipos y otros elementos pertenecientes a los activos informáticos.
Está prohibido retirar de las instalaciones de la ESE o áreas bajo su administración o control, cualquier activo informático sin autorización previa.
El Servicio de Internet debe ser utilizado solamente con fines laborales. Se prohíbe toda transmisión de material obsceno o pornográfico, difamatorio, o que constituya una amenaza.
Los mensajes contenidos en los correos electrónicos no pueden ser contrarios a las disposiciones del orden Público, la moral, las buenas costumbres nacionales e internacionales y los usos y costumbres aplicables en Internet, y el respeto por los derechos de terceras personas.
Está prohibido el almacenamiento y reproducción de aplicaciones, programas o archivos de audio o vídeo que no están relacionados con las actividades propias de las funciones que cumple la dependencia o el usuario.
El usuario está de acuerdo en aceptar responsabilidad por todas las actividades a realizar con los activos informáticos bajo su responsabilidad y custodia o desde las cuentas asignadas para su acceso a los servicios informáticos.
Está prohibido el intento o el hecho de agregar, remover o modificar información identificadora o de contenido en la red, que engañe o confunda al sistema o al usuario destinatario o suplante a otro usuario utilizando su información identificadora.

DIRECTIVAS DE GRUPOS

REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACION

El área de Sistemas será responsable de garantizar que se realicen revisiones periódicas al Sistema de Gestión de Seguridad de la Información, para verificar su vigencia, su correcto funcionamiento y su efectividad.

INVENTARIO DE ACTIVOS DE INFORMACIÓN
El área Administrativa e inventarios, mantendrá un inventario actualizado de los activos informáticos, donde se registrarán y controlarán, desde su ingreso a la institución hasta el momento que se requiera prescindir de los mismos, siguiendo el procedimiento “Inventario y clasificación de activos”.

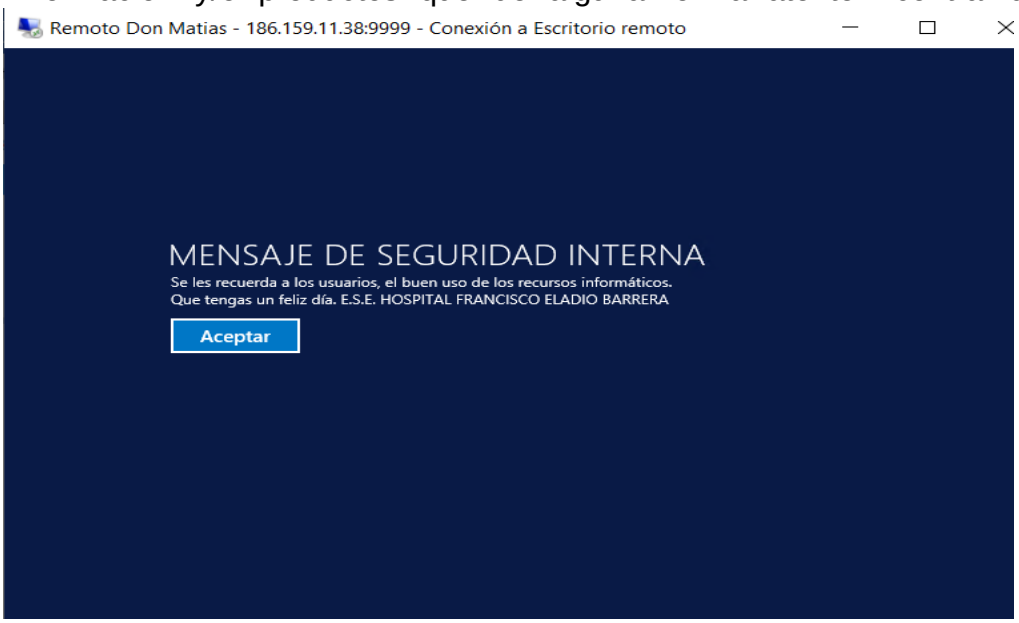
USO ADECUADO DE LOS ACTIVOS Y RECURSOS DE INFORMACION
Toda la información de la ESE será procesada y almacenada de acuerdo con su nivel de clasificación, de manera que se garanticen los criterios de confidencialidad, integridad y disponibilidad.

USO DE INTERNET

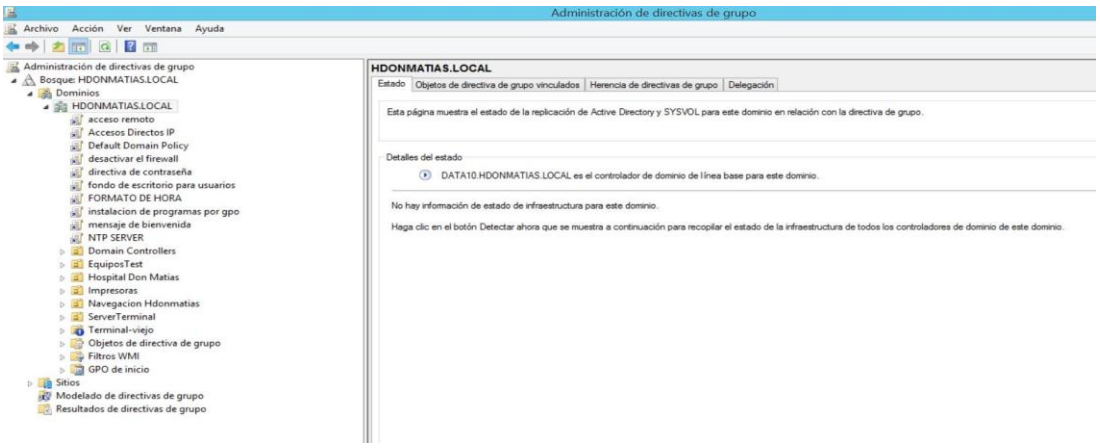
Dado que Internet es una herramienta de trabajo que ofrece múltiples sitios y páginas Web para investigar y aprender, y que además permite navegar en muchos otros sitios no relacionados con las actividades propias de la E.S.E, se controlará, verificará y monitoreará el uso adecuado este recurso, considerando para todos los casos las restricciones definidas en las siguientes políticas:

No se permitirá el acceso a páginas relacionadas con pornografía, música, videos, concursos, entre otros.

No se permitirá la descarga, uso, intercambio y/o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la



propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros. No se permitirá el intercambio no autorizado de información de propiedad de la E.S.E de sus usuarios y/o de sus funcionarios, con terceros.



Cada uno de los funcionarios será responsable de dar un uso adecuado de este recurso y en ningún momento podrá ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, entre otros.

CORREO ELECTRONICO

La E.S.E asignará una cuenta de correo electrónico institucional como herramienta de trabajo para cada una de las áreas o dependencias, la cual será usada para el desempeño de las funciones asignadas.

Los mensajes y la información contenida en los buzones de correo son de propiedad de la E.S.E.

SEGURIDAD DE LOS EQUIPOS

La infraestructura de procesamiento de información (equipos de hardware, software, elementos de red y comunicaciones, instalaciones físicas) La ese cuenta con un sistema de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Los dispositivos y mecanismos de protección estarán alienados con los resultados del análisis de riesgos. Así mismo, se protegerá la disponibilidad e integridad de la infraestructura de procesamiento de información mediante acciones de mantenimiento y soporte.

ELIMINACION Y/O REUTILIZACION SEGURA DE EQUIPOS

Cuando un equipo sea reasignado o dado de baja, se deberá realizar una copia de respaldo de la información de la organización que allí se encuentre almacenada. Luego el equipo deberá ser sometido a un proceso de eliminación segura de la información sensible almacenada y del software instalado, con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma.

ADMINISTRACION DE OPERACIONES Y COMUNICACIONES

PROCEDIMIENTOS Y RESPONSABILIDADES

Se definirán procedimientos, registros e instructivos de trabajo debidamente documentados (reportes-hoja de vida), con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica Cada procedimiento tendrá un responsable para su definición y mantenimiento.

PROTECCIÓN CONTRA CODIGO MALICIOSO

La infraestructura de procesamiento de información contará con sistema de detección de intrusos, sistema anti-spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos. Así mismo, se restringirá la ejecución de aplicaciones y se mantendrá instalado y actualizado un sistema de antivirus, en todas las estaciones de trabajo y servidores de la E.S.E.

COPIAS DE RESPALDO

La información contenida en los servidores se respaldará de forma periódica y automática, es decir se harán copia de respaldo y Backup de Información y se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo, incendio, humedad, y mecanismos de control de acceso físico. Adicionalmente, se realizarán pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

Para garantizar que la información de los usuarios sea respaldada, es responsabilidad de cada uno mantener copia de la información en el disco local D de su estación de trabajo y en el servidor de archivos definido para cada área y/o usuario.

CONTROLES DE RED

Se establecerá un conjunto de controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de garantizar el buen uso de estos y mantener los niveles de seguridad establecidos de acuerdo con los resultados del análisis de riesgos sobre los activos de información. El acceso remoto a la red de datos se permitirá para acceder a recursos como el correo electrónico y servidores de monitoreo, pero únicamente a los funcionarios o terceros autorizados.

CONTROL DE ACCESO

POLÍTICA DE CONTROL DE ACCESO

Los sistemas de información de la E.S.E, cuenta con mecanismos de identificación de usuarios y procedimientos para la autenticación y el control de acceso a los mismos.

El acceso a los activos de información estará permitido únicamente a los usuarios autorizados, por esta razón, todo funcionario tendrá asignado un identificador único de usuario, el cual deberá utilizar durante el proceso de autenticación, previo al acceso de los activos de información autorizados según su perfil (Rol).

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la Infraestructura de Procesamiento, sea por Internet, o por otro medio, siempre estará autenticado.

ADMINISTRACION DE CONTRASEÑAS DE USUARIOS

Los usuarios deberán seguir las siguientes políticas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados.

Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.

Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

Las contraseñas no se deberán escribir en ningún medio, excepto cuando son entregadas en custodia de acuerdo con el procedimiento

Reportar cualquier sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.

Las contraseñas se deberán cambiar según los requerimientos de la infraestructura de procesamiento de información.

POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Los usuarios deberán bloquear su estación cada vez que se retiren de su sitio de trabajo y sólo se podrán desbloquear con la contraseña del usuario. Al finalizar sus actividades diarias, deberán salir de todas las aplicaciones y apagar la estación de trabajo. Los usuarios deberán retirar de forma inmediata todos los documentos confidenciales que envíen a las impresoras. Así mismo, no se deberá reutilizar papel que contenga información confidencial.

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

COMPONENTE	ACTIVIDAD	TAREAS	RESPONSABLE	PLAZO	
				Fecha Inicio	Fecha Final
Gestión de Riesgos	Revisar y ajustar si se requiere, los lineamientos para la gestión de riesgos de seguridad y privacidad de la información.	Revisar la metodología para la Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación.	Líder del proceso de gestión de la información	Abril de 2026	Junio de 2026
	Socializar los lineamientos para la gestión de riesgos de seguridad y privacidad de la información.	Socializar la metodología para la Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación.	Líder del proceso de gestión de la información	Abril de 2026	Junio de 2026
	Actualizar la identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Actualizar la metodología: Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.	Líder del proceso y líberes de procesos	Julio de 2026	Diciembre de 2026
	Actualizar la aceptación de Riesgos Identificados.	Actualizar la aceptación, aprobación riesgos identificados y planes de tratamiento.	Líder del proceso y líderes de procesos	Julio de 2026	Diciembre de 2026
	Publicación de riesgos.	Publicar el mapa de riesgos de seguridad y privacidad de la información, Seguridad Digital y Continuidad de la Operación.	Subgerente administrativa	Julio de 2026	Diciembre de 2026
	Realizar seguimiento al tratamiento de riesgos.	Realizar seguimiento controles y planes de tratamiento de riesgos identificados (verificación de evidencias).	Asesor de control interno	Julio de 2026	Diciembre de 2026
	Monitoreo y Revisión	Realizar la medición, presentación y reporte de indicadores de la gestión de riesgos de seguridad y privacidad de la información.	Asesor de control interno	Julio de 2026	Diciembre de 2026
Gestión de Incidentes de Seguridad y Privacidad de la Información	Formular y socializar el procedimiento para la gestión de incidentes de seguridad de la información	Documentar el procedimiento de incidentes de seguridad de la información.	Líder del proceso de gestión de la información	Julio de 2026	Diciembre de 2026
		Socializar a los colaboradores el procedimiento de incidentes de seguridad de la información.	Líder del proceso de gestión de la información	Julio de 2026	Diciembre de 2026
	Gestionar los incidentes de Seguridad de la Información identificados.	Analizar y gestionar los incidentes de seguridad de la información reportados.	Líder del proceso y líberes de procesos	Julio de 2026	Diciembre de 2026

CONTROL DE CAMBIOS

Versión	Descripción	Elaboró	Revisó	Aprobó
04	Actualización del documento en el componente de programación de las actividades del Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Gloria Gil Pemberthy Subgerente Administrativa Martin Alvarez Montoya Asesor control interno	Comité de gestión y desempeño	Andrés Alfredo Villa Castro Gerente