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

E.S.E. HOSPITAL DE LA CEJA

2023

Código: PL-MC-02 Versión: 03
Fecha de actualización: 01/2023

CONTENIDO

1. 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 ESE Hospital De La Ceja 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 ESE Hospital De La Ceja 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.

2. ALCANCE

El Plan de tratamiento de riesgos seguridad y privacidad de la información de la ESE Hospital de La Ceja, se proyecta para las vigencias 2022-2023 y se aplica a todos los activos de información identificados en las diferentes dependencias de la entidad.

3. 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.

4. OBJETIVO

Establecer las actividades para el tratamiento de riesgos la Seguridad y Privacidad de la Información de la ESE Hospital de La Ceja, alineadas con las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

5. CONTEXTO ESTRATÉGICO DE LA ENTIDAD

MISIÓN

Somos una empresa con un equipo ético, que brinda servicios de calidad, seguros e integrales en salud, donde la humanización e innovación se convierten en nuestras principales estrategias para el sostenimiento financiero y la responsabilidad social con nuestra comunidad.

VISIÓN

En el año 2024, seremos una institución reconocida en el departamento de Antioquia por la innovación en la prestación de servicios de salud, con enfoque humanizado y de seguridad del paciente, aplicando estándares para el mejoramiento continuo, con un equipo altamente comprometido y una comunidad participativa, para asegurar sostenibilidad financiera, rentabilidad social y desarrollo empresarial.

VALORES CORPORATIVOS:

- Compromiso: Entregando todas nuestras capacidades para el logro de los objetivos de la institución.
- Responsabilidad: Con el usuario, su familia y la comunidad, garantizando el beneficio de todas las partes relacionadas con el proceso de atención.
- Respeto: Reconociendo, apreciando y aceptando las condiciones del otro frente a la prestación del servicio.

- Honestidad: Actuando con rectitud, transparencia e integridad, anteponiendo el respecto por la institución, el usuario, y la comunidad en general.

- Solidaridad: Trabajando en equipo para aportar al bienestar de todas las partes interesadas y relacionadas con el proceso de atención.

PRINCIPIOS CORPORATIVOS:

- Sentido de pertenencia: Con equipo de trabajo comprometido con los objetivos institucionales, aportando al crecimiento de la organización.

- Transparencia: Frente a cada una de las actividades y procesos que se realicen, garantizando la confianza frente a los grupos de interés y la comunidad en general.

- Amor: Garantizando una atención compasiva y respetuosa, centrada en el ser, sus necesidades y expectativas.

- Humanización: Garantizando una comunicación efectiva y cálida que satisfaga las necesidades de los usuarios en un ambiente que le brinde seguridad y confianza frente a la atención.

LÍNEAS ESTRATÉGICAS:

El plan de desarrollo de la ESE Hospital de La Ceja está compuesto por las siguientes líneas estratégicas, las cuales se convierten en los conductores principales para el cumplimiento de los objetivos institucionales:

- Salud Cercana para todos
- Amor por lo que hacemos
- Nuestro Equipo, nuestro compromiso
- Recursos seguros
- Innovamos para ti
- Compromiso Social

OBJETIVOS ESTRATÉGICOS:

Los objetivos serán los inductores que permiten materializar las líneas estratégicas:

Salud Cercana para todos:

Fortalecer los programas de promoción de la salud y prevención de la enfermedad a través de estrategias que mejoren las condiciones de accesibilidad para la población.

Amor por lo que hacemos:

Prestar servicios de salud con atributos de calidad y calidez, garantizando un trato humanizado y un servicio seguro que satisfaga las necesidades de nuestros usuarios.

Nuestro Equipo, nuestro compromiso:

Contar con un talento humano competente, comprometido y satisfecho, como aliado principal para el cumplimiento de los objetivos de la institución, en donde se garantizará la seguridad frente a la labor que desempeñe.

Recursos seguros:

Garantizar la sostenibilidad financiera de la institución, a través de la gestión eficiente de los recursos.

Innovamos para ti:

Gestionar proyectos que permitan la modernización tecnológica y de la infraestructura de la institución, garantizando la prestación de servicios con estándares de calidad.

Compromiso Social:

Asegurar la responsabilidad social y ambiental, contribuyendo al bienestar del usuario, la familia y la comunidad en general.

4. MARCO NORMATIVO

- **Ley 57 de 1985** - Publicidad de los actos y documentos oficiales.
- **Decreto Ley 2150 de 1995** - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.

- **Ley 527 de 1999** - Ley de Comercio Electrónico.
- **Ley 594 de 2000** - Ley General de Archivos.
- **Decreto 1747 de 2000** - Entidades de certificación, los certificados y las firmas digitales.
- **Ley 962 de 2005** - Racionalización de trámites y procedimientos administrativos procedimientos administrativos.
- **Ley 1266 de 2008** - Disposiciones generales de habeas data y se regula el manejo de la información.
- **Ley 1437 de 2011** - Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Decreto 2364 de 2012** - Firma electrónica.
- **Decreto 019 de 2012** - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- **Ley Estatutaria 1581 de 2012** - Protección de datos personales.
- **Ley estatutaria 1618 de 2013** - Ejercicio pleno de las personas con discapacidad.
- **Ley 1712 de 2014** - Ley de Transparencia y acceso a la información pública.
- **Decreto Reglamentario Único 1081 de 2015** - Reglamento sobre la gestión de la información pública.
- **Acuerdo 03 de 2015** del Archivo General de la Nación - Lineamientos generales sobre la gestión de documentos electrónicos.
- **Anexo 1** - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la

Ley 1712 de 20214 - Ley de Transparencia y Acceso a la Información Pública.

- **Título 9 - Decreto 1078 de 2015** - Decreto Único Reglamentario del Sector de

Tecnologías de la Información y las Comunicaciones.

- **Ley Estatutaria 1757 de 2015:** Promoción y protección del derecho a la participación democrática.

- **Decreto 2641 de 2012** - Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011.

- **Decreto 124 de 2016** - Por el cual se sustituye el Título 4 de la Parte 1 del Libro 2 del decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano".

- **Decreto 1499 de 2017 -** Por medio del cual se actualiza el Modelo Integrado de Planeación y Gestión.

- **Decreto 612 de 2018** -directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado

5. MARCO CONCEPTUAL (DEFINICIONES RELEVANTES)

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura (Ley 594 de 2000 art 3).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privados que cumplen con funciones publicas y que son puestas a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014 art 6).

- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012 art 3).
- **Datos Personales Públicos**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la

información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

6. METODOLOGIA

La metodología utilizada para la formulación del plan se realizó usando como guía el Modelo Plan de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones, ajustando los componentes de acuerdo la situación que presenta la institución, describiendo las actividades y acciones que se desarrollarán para el logro de los objetivos.

7. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACIÓN

COPIAS DE SEGURIDAD

- Los usuarios del sistema que por el desarrollo de sus funciones requieren tener copias de seguridad de información relevante (que su pérdida puede perjudicar en algún momento el funcionamiento de la misma, presentar inconvenientes para la realización de las actividades laborales o alterar la toma de decisiones), realizarán una copia de su información en el disco alterno de su equipo (disco D, E, F, G, J) de acuerdo con el “Instructivo para la realización de copias de seguridad IN-AI-002”. La realización de

las copias de seguridad de los datos críticos que se manejan en cada computador de escritorio son responsabilidad de cada usuario.

- Los datos, la información, las aplicaciones y la documentación deben contar con copias de respaldo suficientes y actualizados, que garanticen la recuperación de los sistemas críticos, de tal manera que no se afecten en forma sustancial la operación del hospital frente a un evento catastrófico. Estas copias de respaldo son responsabilidad del área de sistemas y se realizan de la siguiente manera:

  AUTOMÁTICAS: El software Dinámica Gerencial realiza automáticamente copias de seguridad de toda la base de datos con la siguiente periodicidad 12 h, 8h, 10h, 12h 15h, 17h y 20h, estas copias se realizan en el mismo servidor, pero en una partición diferente del disco duro y se almacenaran en medio externo las copias de 12 horas.

  DIARIAS: El personal de sistemas realiza copia diaria de las bases de datos de Dinámica Gerencial en disco duro extraíble.

- La oficina de sistemas debe capacitar y entregar los instructivos necesarios a los usuarios para que realicen las copias de seguridad reglamentadas.

CONTROL DE ANTIVIRUS

- Cada equipo de la institución deberá tener instalado el antivirus que permita la verificación de toda información externa que pueda llegar a los mismos para evitar daño en los archivos y equipos de cómputo.

- En caso de detectarse algún virus en un equipo de la institución, debe informarse oportunamente al área de sistemas.

- El administrador del sistema elegirá el antivirus más adecuado para la entidad de acuerdo a los criterios de costo y efectividad.

- El administrador del sistema verificará la actualización automática del antivirus.

- La institución garantiza el licenciamiento del antivirus en forma continua.

CONTROL DE CAMBIOS

- Todo cambio que se requiera en el sistema de información debe ser autorizado por el líder del proceso y será realizado, siempre y cuando no vulnere la seguridad existente en el sistema, lo cual será validado por los administradores del sistema.
- Cualquier modificación a los programas o a las estructuras de datos debe ser analizada y puesta en marcha de acuerdo a su magnitud por el administrador del sistema.

ASIGNACIÓN DE USUARIOS Y CONTRASEÑAS

- Los usuarios de los recursos informáticos de la ESE deben contar con unas contraseñas que les permitan cumplir con el desempeño normal de sus funciones y que garanticen un nivel de acceso acorde a las funciones asignadas. Estos usuarios a su vez pertenecen a unos grupos definidos que tienen asociados unos perfiles de acceso a la información de la Institución de la siguiente manera:

  Los usuarios del sistema de información institucional están clasificados para que el personal pueda tener acceso a la estación de trabajo (PC), al software institucional, a la Intranet, a las carpetas de trabajo en red, e Impresoras de red, de acuerdo con el perfil según sus funciones:

  El perfil asignado a estos usuarios puede ser:

- Administrador: corresponde al administrador del sistema (Técnico Administrativo - Sistemas) y cuenta con todos los privilegios.
- Usuario administrativo: Usuarios que desarrollan labores administrativas, pero que no son administradores del sistema de información.
- Usuario asistencial: Usuario que desarrollan actividades en el área asistencial y que sus funciones son propias de la actividad misional de la institución.

La asignación de usuarios y contraseñas para ingresar a las diversas aplicaciones de la institución para usuarios nuevos debe ser solicitada por correo electrónico al área de sistemas por el jefe inmediato del nuevo funcionario, especificando área de trabajo y requerimientos específicos de uso de los programas. Para la asignación de usuarios y claves es necesario que al nuevo empleado ya se le haya realizado la inducción en el "Manual para el manejo de la información".

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

COMPONENTE	ACTIVIDAD	TAREAS	RESPONSABLE	INICIA	FINALIZA
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 2023	Junio de 2023
	Socializar los lineamientos para la gestión de riesgos de seguridad y	Socializar la metodología para la Gestión de Riesgos de Seguridad y privacidad de la	Líder del proceso de gestión de la información	Abril de 2023	Junio de 2023

	privacidad de la información.	Información, Seguridad Digital y Continuidad de la Operación.			
	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 2023	Diciembre de 2023
	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 2023	Diciembre de 2023
	Publicación de riesgos.	Publicar el mapa de riesgos de seguridad y privacidad de la información, Seguridad Digital y Continuidad de la Operación.	Líder comunicaciones	Julio de 2023	Diciembre de 2023
	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 2023	Diciembre de 2023
	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 2023	Diciembre de 2023
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 2023	Diciembre de 2023
		Socializar a los colaboradores el procedimiento de	Líder del proceso de	Julio de 2023	Diciembre de 2023

		incidentes de seguridad de la información.	gestión de la información		
	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 2023	Diciembre de 2023

9. CONTROL DE CAMBIOS

Versión	Descripción	Elaboró	Revisó	Aprobó
01	Elaboración del Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Mónica Araque Soto Técnica administrativa Martin Alvarez Montoya Asesor calidad	Comité de gestión y desempeño	Claudia Barrera Gerente