MANUAL

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ASEGURAMIENTO DE LA GESTIÓN / GESTIÓN INTEGRAL DE RIESGOS

Tabla de contenido

1. OBJETIVO 3
2. ALCANCE 3
3. DEFINICIONES 3
4. DESCRIPCIÓN DEL DOCUMENTO 4
4.1. CONTEXTO DE LA ORGANIZACIÓN 4
4.1.1. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS 5
4.1.2. ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 5
4.1.3. NORMATIVIDAD 5
4.2. LIDERAZGO 5
4.2.1. COMITÉ INTEGRAL DE RIESGOS DE COLPENSIONES 5
4.2.2. MESA DE MONITOREO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD. 7
4.2.3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 7
4.2.4. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN 7
4.3. PLANIFICACIÓN 8
4.3.1. ACCIONES PARA TRATAMIENTO RIESGOS Y OPORTUNIDADES DE MEJORA 8
4.3.2. DECLARACIÓN DE APLICABILIDAD 8
4.3.3. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 8
4.3.4. MEDICIÓN DEL SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 8
4.4. SOPORTE 9
4.4.1. RECURSOS 9
4.4.2. TOMA DE CONCIENCIA 9
4.4.3. COMUNICACIÓN 9
4.4.4. INFORMACIÓN DOCUMENTADA DEL SGSI 9
4.5. EVALUACIÓN DEL DESEMPEÑO DEL SGSI 9
4.5.1. AUDITORIA INTERNA 9
4.5.2. REVISIÓN POR LA DIRECCIÓN 10
4.6. MEJORA DEL SGSI 10
4.6.1. NO CONFORMIDADES Y ACCIONES CORRECTIVAS 10
4.6.2. MEJORA CONTINUA 10
5. ANEXOS 10
CONTROL DE CAMBIOS DEL DOCUMENTO 10

1. OBJETIVO

Establecer las directrices que permitan garantizar la confidencialidad, integridad y disponibilidad de los activos de información de acuerdo con el marco de la norma ISO 27001:2013 y la normativa vigente con el fin de implementar, mantener, revisar y mejorar el Sistema de Gestión de Seguridad de la Información y Ciberseguridad de COLPENSIONES.

2. ALCANCE

Este documento está dirigido al nivel directivo, los líderes de los procesos de COLPENSIONES y a todas las partes interesadas, con repercusión a los colaboradores de todas las áreas de la Entidad y los procesos correspondientes, que hacen parte del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

3. DEFINICIONES

- **Activo de Información:** cualquier elemento que contenga, datos que tienen valor para uno o más procesos de la Entidad y debe protegerse. (ISO/IEC 27001:2013).
- **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. (Archivo General de la Nación, 2006).
- **Confidencialidad:** propiedad de la información que garantiza no estar disponible o ser divulgada a personas, entidades o procesos no autorizados. (ISO/IEC 27000:2018).
- **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. (Ministerio de Tecnologías de la Información y las Comunicaciones - Modelo de Seguridad y Privacidad de la Información 2016).
- **Control de acceso:** Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos de negocio y de seguridad. (ISO/IEC 27000:2018).
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012).
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el 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 27000:2018).
- **Disponibilidad**: propiedad de la información que garantiza el ser accesible y usable de acuerdo con lo requerido por una entidad autorizada. (ISO/IEC 27000:2018).
- **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 27000:2018).
- **Integridad:** Propiedad de exactitud y completitud de los activos de información. (ISO/IEC 27000:2018).

- **ISO/IEC 27001:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.
- **Isotools**: Sistema de Información que permite administrar y controlar los documentos, indicadores, riesgos, requisitos legales, otros que hacen parte de los sistemas de gestión y marcos de referencia que componen el Modelo SIG - Sistema Integrado de Gestión.
- Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado - positivo o negativo. (ISO/IEC 27000:2018).
- **Servicios**: servicios de computación y comunicaciones, tales como los de consulta, correo electrónico, mensajería instantánea, videoconferencia, herramientas colaborativas y transmisión, entre otros que sean prestados por un tercero. (Adaptado de la Guía para la Gestión y Clasificación de Activos de Información,2016).
- **SGSI**: Sistema de Gestión de Seguridad de la Información. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **STAKEHOLDERS**: es una palabra del inglés que, en el ámbito empresarial, significa 'interesado' o 'parte interesada', y que se refiere a todas aquellas personas u organizaciones afectadas por las actividades y las decisiones de una entidad.

4. DESCRIPCIÓN DEL DOCUMENTO

4.1. CONTEXTO DE LA ORGANIZACIÓN

La Administradora Colombiana de Pensiones - COLPENSIONES, es una empresa industrial y comercial del Estado, organizada como entidad financiera de carácter especial, vinculada al Ministerio de Trabajo. Conforme al Decreto número 309 del 24 de febrero de 2017, adoptó un nuevo modelo de operación por procesos para mejorar la efectividad en el servicio al ciudadano, sus procesos de evaluación y control de la gestión y dar respuesta oportuna a las solicitudes o trámites de los ciudadanos.

El **Sistema de Gestión de Seguridad de la Información y Ciberseguridad** está "basado en estándares internacionales y buenas prácticas, cuyos requisitos están orientados a establecer, operar, hacer seguimiento, revisar, mantener la seguridad y los activos de información de la entidad, para gestionar adecuadamente la integridad, confidencialidad y disponibilidad de estos y hace parte del Modelo del Sistema Integrado de Gestión y tiene en cuenta los elementos transversales establecidos en el Manual del Modelo de Sistemas Integrados de Gestión - AGE-ASG-MAN-001.

COLPENSIONES determina los factores internos y externos que pueden comprometer el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad por medio del documento Diagnóstico de Contexto Interno y Externo - DIE-PLE-DIN-005.

Estrategia: COLPENSIONES establece la Misión, Visión y Objetivos estratégicos los cuales son revisados y actualizados periódicamente, y se consolidan bajo el Plan Estratégico Institucional: https://www.colpensiones.gov.co/publicaciones/115/marco-estrategico/.

Estructura. El proceso de Gestión de la selección, administración del talento humano y servicios laborales gestiona la estructura organizacional de COLPENSIONES. El nivel jerárquico más alto está asignado a la Junta Directiva de la cual depende la Presidencia de COLPENSIONES que establece la dirección para las Oficinas y Vicepresidencias. Esta información puede ser consultada a través de la página web de la entidad en el siguiente enlace: https://www.colpensiones.gov.co/publicaciones/116/organigrama-y-equipo-humano/.

4.1.1. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Mediante el documento caracterización de grupos de interés priorizados COLPENSIONES DIE-PLE-DIN-003 y la Identificación grupos de interés de COLPENSIONES "STAKEHOLDERS" DIE-PLE-DIN-004, se identifican las partes interesadas, sus necesidades y requerimientos. Frente al sistema de Gestión de seguridad de la información y Ciberseguridad se cuenta con el documento "AGE-GRI-DIN-008 - Grupos de Interés SGSI.

4.1.2. ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El Sistema de Gestión de seguridad de la información y Ciberseguridad de COLPENSIONES se ha implementado para que sea aplicable para todos los procesos y áreas que conforman la entidad y se alinea con el alcance definido en el Sistema de Gestión de Calidad, así:

La administración integral de los aportes del régimen de prima media (RPM) y los ahorros de los beneficios económicos periódicos (BEPS) y los servicios sociales complementarios soportados en la gestión comercial, la gestión del ciudadano y el empleador, la gestión del financiamiento e inversiones, la administración de la información, la determinación y cumplimiento de derechos, la gestión en educación y servicios extendidos y de bienestar.

Requisito no aplicable conforme lo establecido en la Declaración de Aplicabilidad: A 18.1.5 Reglamentación de controles criptográficos.

4.1.3. NORMATIVIDAD

El marco de referencia normativo bajo el cual se identifican los requerimientos legales relacionados con seguridad de la información para COLPENSIONES se establece en los requisitos legales controlados en Isotools y publicados en el Normograma, en la página web de la entidad en el siguiente enlace: https://normativa.colpensiones.gov.co/compilacion/herramientas_busqueda.html

4.2. LIDERAZGO

4.2.1. COMITÉ INTEGRAL DE RIESGOS DE COLPENSIONES

El comité integral de riesgos de COLPENSIONES fue creado mediante la resolución interna 014 de 2021, igualmente, se rige de acuerdo con el Manual del Sistema Integral de Administración de Riesgos AGE-GIR-MAN-009 con el fin de apoyar y asesorar en la definición, seguimiento, control e implementación de las políticas y procedimientos del Sistema Integral de Administración de Riesgos de la Organización. En dicho comité de manera periódica, se presentan los aspectos asociados al Sistema de Gestión de Seguridad de la Información y Ciberseguridad con el objetivo de proveer los recursos para el referido sistema, estableciendo el apetito de riesgo y tomando las medidas de alto nivel para corregir las desviaciones que se pudieran presentar en el cumplimiento de las políticas y objetivos de Seguridad de la Información y Ciberseguridad.

A continuación, se relacionan los aspectos del sistema de gestión de seguridad de la información y ciberseguridad que se presentan en el comité:

a) Establecer el apetito de riesgo, tomando las medidas de alto nivel para corregir las desviaciones que se pudieran presentar en el cumplimiento de los objetivos de Seguridad de la Información.
b) Asegurar que la política de Seguridad de la Información y ciberseguridad y los objetivos de ésta, estén alineados con la planeación estratégica de la Entidad.
c) Recomendar al vicepresidente de Seguridad y Riesgos Empresariales la aprobación de las políticas de Seguridad de la Información y Ciberseguridad.
d) Validar el alcance y las interfaces del SGSI, de acuerdo con el contexto y los intereses de las partes interesadas. Las interfaces son los puntos de entrada y salida de información del SGSI, estableciendo los límites, así como el alcance de la responsabilidad y los controles para este sistema.
e) Recomendar al vicepresidente de Seguridad y Riesgos Empresariales la aprobación de los objetivos de seguridad de la información.
f) Proponer acciones de alto nivel para apoyar el cumplimiento de los planes y proyectos de seguridad de la información, validando presupuestos, cambio en la prioridad de los proyectos y los esfuerzos corporativos, recomendando alianzas estratégicas, acogiéndose a programas gubernamentales, impulsando programas de formación y capacitación, promoviendo desarrollo de nuevas tecnologías y marcos de referencia.
g) Facilitar y promover el desarrollo de iniciativas de Seguridad de la Información.
h) Promover en COLPENSIONES la importancia de cumplir los objetivos de Seguridad de la Información definidos en el SGSI, estableciendo planes de trabajo que permitan evaluar su compromiso frente al cumplimiento de estos objetivos.
i) Analizar los incidentes de alto impacto de seguridad de la información para COLPENSIONES.
j) Hacer un seguimiento periódico para la aplicación del marco legal y regulatorio aplicable.
k) Validar la aplicación de la metodología corporativa de riesgos de seguridad de la información y ciberseguridad, a través del seguimiento de los planes de tratamiento de riesgos y oportunidades de mejora, contribuyendo con el proceso permanente de identificación, análisis, valoración y tratamiento de riesgos de seguridad de la información.
l) Liderar los planes de trabajo para que la responsabilidad de la gestión de los riesgos sea asignada a los propietarios y no quede en las áreas de soporte.
m) Validar que los reportes de los análisis de riesgos de seguridad de la información estén acordes con la metodología de riesgos de la Entidad, corroborando la alineación con los objetivos de los procesos y la planeación estratégica de COLPENSIONES.

n) Realizar seguimiento al cumplimiento de los indicadores de Seguridad de la Información y Ciberseguridad.
o) Promover que el personal con responsabilidades de Seguridad de la Información cuente con las competencias y conocimientos necesarios para el desempeño de sus funciones.
p) Verificar las revisiones regulares de la eficacia del SGSI, basados en el resultado de las auditorías al SGSI, los incidentes de Seguridad de la Información y la retroalimentación de las partes interesadas.
q) Asegurar que se actualice la documentación del SGSI con base en la responsabilidad de cada cargo.

4.2.2. MESA DE MONITOREO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

La Mesa de Monitoreo de Riesgos de Seguridad de la Información y Ciberseguridad de COLPENSIONES se estableció conforme al Memorando Interno No. 02 de 2022, emitido por el Vicepresidente de Seguridad y Riesgos Empresariales. La mesa está adscrita al Comité Integral de Riesgos y allí se tratan los temas asociados al Sistema de Gestión de Seguridad de la Información y Ciberseguridad con el propósito de enfrentar los retos que tiene la Administradora Colombiana de Pensiones - COLPENSIONES en materia de los riesgos relacionados con la seguridad de la información y la ciberseguridad.

A continuación, se relacionan los temas a tratar que se presentan en la mesa de monitoreo:

- Realizar seguimiento al comportamiento de los riesgos de Seguridad de la Información y Ciberseguridad y promover la implementación de los planes de tratamiento de los riesgos que se encuentren por fuera del apetito de riesgo.
- Evaluar el comportamiento de los eventos e incidentes de seguridad que se presenten en la entidad y realizar seguimiento a los planes de mejoramiento establecidos para mitigarlos.
- Acompañar y realizar seguimiento al desarrollo de proyectos de seguridad de la información y ciberseguridad.
- Recomendar al Comité Integral de Riesgos, propuestas de mejora sobre el Sistema de Gestión de Seguridad de la Información y Ciberseguridad.
- Los demás acordes con la naturaleza y el objetivo de la mesa de trabajo.

4.2.3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La Política General de Seguridad de la Información y Ciberseguridad se describe en el documento interno Política General de Seguridad de la Información y Ciberseguridad AGE-GRI-DIN-005.

Para el cumplimiento del Sistema de Seguridad de la Información, se cuenta con un Manual de Políticas y Lineamientos de Seguridad de la Información y Ciberseguridad AGE-GRI-MAN-015 anexo al presente manual, aprobado por la Alta dirección para la aplicación de controles necesarios para garantizar la protección de los activos de Información.

4.2.4. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

4.2.4.1. ROLES Y RESPONSABILIDADES FRENTE AL MODELO SIG

COLPENSIONES define los roles y responsabilidades para asegurar una adecuada mejora continua al sistema integrado de Gestión, en el documento interno denominado "Manual del Modelo de Sistemas Integrados de Gestión" - AGE-ASG-MAN-001 Numeral 4.2.8. Compromiso, roles y responsabilidades frente al modelo SIG.

4.2.4.2. ROLES, RESPONSABILIDADES PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

COLPENSIONES define los roles y responsabilidades para asegurar una adecuada mejora continua al sistema de Gestión de Seguridad de la Información bajo el documento Interno "Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información y Ciberseguridad" - AGE-GRI-DIN-004.

4.3. PLANIFICACIÓN

4.3.1. ACCIONES PARA TRATAMIENTO RIESGOS Y OPORTUNIDADES DE MEJORA

COLPENSIONES cuenta con una metodología integral para la identificación, análisis, evaluación, tratamiento, monitoreo de los riesgos e información y comunicación descrita en el Manual del Sistema Integral de Administración de Riesgos AGE-GRI-MAN-009. Adicionalmente se establecen las particularidades de la metodología para seguridad de la información y ciberseguridad en el Manual Parte V Sistema de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad AGE-GRI-MAN-013, en el que se define la identificación de riesgos sobre la toma de decisiones y la priorización de las acciones sobre los mismos, contando con planes de tratamiento que permitan la mejora continua del Sistema de Gestión de Seguridad de la Información.

4.3.2. DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad se desarrolla durante el análisis de riesgos de seguridad de la información y ciberseguridad y se actualiza anualmente en el módulo de Declaración de Aplicabilidad en el sistema ISOTOOLS.

4.3.3. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Los objetivos de seguridad de la información y ciberseguridad se describen en el documento interno Objetivos de seguridad de la información y ciberseguridad AGE-GRI-DIN-006.

4.3.4. MEDICIÓN DEL SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La medición del Sistema de Gestión de Seguridad de la Información y Ciberseguridad se describe en el documento interno medición del Sistema de Gestión de Seguridad de la Información y Ciberseguridad AGE-GRI-DIN-007.

4.4. SOPORTE

4.4.1. RECURSOS

COLPENSIONES provee los recursos necesarios para la implementación y mantenimiento del Sistema de Gestión de seguridad de la información y ciberseguridad, por medio de un presupuesto anual aprobado por la Junta Directiva generado para los requerimientos necesarios tanto técnicos como administrativos que se requieren para la mejora continua del sistema.

4.4.2. TOMA DE CONCIENCIA

El sistema de seguridad de la información y ciberseguridad cuenta con un plan anual de comunicación, sensibilización y capacitación revisado y aprobado por la Vicepresidencia de Seguridad y Riesgos Empresariales, que se ejecuta, junto con la Gerencia de Talento Humano y Relaciones Laborales y se articula con el plan de transformación organizacional del modelo SIG, de acuerdo con las necesidades y cumplimiento de cada una de las temáticas propuestas.

4.4.3. COMUNICACIÓN

La entidad a través del proceso de Gestión de Comunicaciones cuenta con la Política de Comunicaciones y Relacionamiento Institucional DIE-COM-MAN-001, la cual establece las pautas para el manejo de la comunicación, la información y el relacionamiento institucional con los grupos de interés, tanto internos como externos.

4.4.4. INFORMACIÓN DOCUMENTADA DEL SGSI

COLPENSIONES cuenta con información documentada conforme los lineamientos del sistema de gestión de calidad.

4.5. EVALUACIÓN DEL DESEMPEÑO DEL SGSI

4.5.1. AUDITORIA INTERNA

Para el seguimiento, cumplimiento y monitoreo del sistema de Seguridad de la información, se realizan auditorías por lo menos una vez al año, dando cumplimiento al documento Lineamientos para auditorías internas del sistema integrado de Gestión ECG-EVI-LIN-001, en el cual se encuentra definido el programa de auditorías, la selección del equipo auditor y el plan de auditoría entre otros. Generando como resultado de la ejecución de la auditoría, un informe donde se incluyen las fortalezas, oportunidades de mejora y no

conformidades, que permitan generar planes de mejoramiento para el fortalecimiento del sistema de seguridad de la información y ciberseguridad.

4.5.2. REVISIÓN POR LA DIRECCIÓN

La Alta Dirección de COLPENSIONES está comprometida con la revisión del sistema de gestión de seguridad de la información y ciberseguridad, como mínimo una vez al año para asegurar las normas y buenas prácticas del SGSI. En el documento de Lineamientos para la evaluación y seguimiento al Modelo SIG AGE-ASG-LIN-002 se detallan los lineamientos relacionados al respecto.

4.6. MEJORA DEL SGSI

4.6.1. NO CONFORMIDADES Y ACCIONES CORRECTIVAS

La gestión de las no conformidades y la definición de las acciones correctivas, se rigen por el documento "Lineamientos, Formulación, Seguimiento y Evaluación de Planes de Mejoramiento" AGE-GPR-LIN-001 donde se relaciona el seguimiento y evaluación de los planes de mejoramiento que permitan solucionar, controla y mejorar las situaciones identificadas por fuentes internas o externas a COLPENSIONES.

4.6.2. MEJORA CONTINUA

A partir de los resultados de los indicadores del Sistema de Gestión de seguridad de la información y Ciberseguridad, auditorías realizadas y la revisión por la dirección, entre otros, se formulan planes de mejoramiento que contribuyen con la mejora continua y aseguran el cumplimiento de los dominios, objetivos y controles de la Norma ISO 27001, leyes y buenas prácticas del sistema.

5. ANEXOS

5.1. Política General de Seguridad de la Información y Ciberseguridad - AGE-GRI-DIN-005
5.2. Documento Interno Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información y Ciberseguridad - AGE-GRI-DIN-004.
5.3. Manual de Políticas y Lineamientos de SI y Ciberseguridad - AGE-GRI-MAN-015

CONTROL DE CAMBIOS DEL DOCUMENTO

FECHA	VERSIÓN	MODIFICACIÓN	ELABORÓ	REVISÓ	APROBÓ
Febrero 2022	1	Creación	Nombre: Stiven Parra Córdoba Cargo: Profesional Máster, Código 320, Grado 08 Nombre: Liliana Serrano Forero Cargo: Asesor, Código 200, Grado 01	Nombre: Antonio José Coral Triana Cargo: Gerente, Código 150, Grado 08 Nombre: Miembros Comité Integral de Riesgos del 13 de Febrero de 2022	Nombre: Fabián Mauricio Arias Cargo: Vicepresidente, Código 160, Grado 09 Nombre: Junta Acuerdo 004 de 28 de Febrero de 2022
Abril 2023	2	Revisión	Nombre: Stiven Parra Córdoba Cargo: Profesional Máster, Código 320, Grado 08 Nombre: Liliana Serrano Forero Cargo: Asesor, Código 200, Grado 01	Nombre: Paola Palmariny Peñaranda, Vicepresidente de Seguridad y Riesgos Empresariales Nombre: Antonio José Coral Triana, Gerente de Riesgos y Seguridad de la Información	Nombre: Junta Directiva abril de 2023 Acuerdo 004 de 2023