MANUAL CORPORATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA

COPIA CONTROLADA

TABLA DE CONTENIDO

FIGURAS

TABLAS

ANEXOS

INTRODUCCIÓN

La Cooperativa Médica del Valle y de Profesionales de Colombia, COOMEVA, sus unidades de negocio y las empresas que conforman el **GRUPO EMPRESARIAL COOPERATIVO COOMEVA (**en adelante **GECC)**, desarrollan sus actividades con sujeción a las normas legales y a los más altos principios éticos; por tal motivo, en cumplimiento de lo establecido en las normas emitidas por la Superintendencia de la Economía Solidaria, la Superintendencia Financiera de Colombia, la Superintendencia de Industria y Comercio, la Superintendencia Nacional de Salud, la Superintendencia de Sociedades y demás entidades y organismos de vigilancia y control, el Consejo de Administración de **COOMEVA** aprueba el marco general del **SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL GECC (**en adelante **SGSI)**, el cual es de obligatoria aplicación por parte de todas las unidades y empresas que lo conforman y de obligatorio cumplimiento por parte de los dirigentes cooperativos, de los administradores, directivos y en general de todos los colaboradores, contratistas y proveedores**.**

1.OBJETIVO

Definir el marco de referencia, instrumentos y metodologías generales para la implementación y funcionamiento del **SGSI** para Coomeva, sus unidades de negocio y las empresas que conforman el **GECC** y el Conglomerado en su conjunto, con el fin de contextualizar, identificar, valorar (analizar y evaluar), tratar, comunicar, monitorear y revisar los riesgos implicados en toda su cadena de valor.

En lo sucesivo, cuando en este Manual se haga referencia al **GECC** y a las disposiciones, obligaciones y en general a los requerimientos que este debe cumplir, se entenderá que estas se refieren a todas y cada una de las entidades y unidades que lo conforman y cuando se haga referencia al **Nivel Corporativo**, se entenderá que se refiere al conjunto del grupo visto como conglomerado.

2.ALCANCE

El presente Manual tiene carácter vinculante y alcance para todo el **GECC**, y para todas las áreas y procesos que conforman el Grupo y el Nivel Corporativo, incluyendo los procesos que las empresas y unidades decidan tercerizar.

Adicionalmente interactúa con los demás sistemas y subsistemas que conviven en la organización, tales como: Sistema de Gestión Integral, Control Interno, Gestión de la Calidad, el Sistema de Sostenibilidad y Responsabilidad Social y el Sistema de Gestión del Riesgo, entre otros.

Las políticas, directrices, metodologías y lineamientos corporativos plasmados en este Manual, complementan la normatividad para la implantación y funcionamiento del **SGSI** al interior del **GECC**. Se trata de un marco general y básico, el cual debe ser complementado por cada sector, empresa y unidad de negocio, a fin de cumplir plenamente con la normatividad que a cada entidad le es aplicable.

Supervisión Directa Corporativo	Acogen Lineamientos Corporativos
Coomeva	Bancoomeva
Club Los Andes	Fiduciaria Coomeva
Fundación Coomeva	Corredor de Seguros
	Coomeva EPS
	Coomeva Medicina Prepagada
	Conectamos Financiera
	Conecta Salud
	Fondo de Empleados

Tabla 1. Alcance del Manual a Nivel Corporativo en Seguridad y Privacidad de la Información

3.TÉRMINOS Y DEFINICIONES

Además de los términos y definiciones incluidos en el **Manual Corporativo del Sistema de Gestión del Riesgo del GECC,** aprobado por el Consejo de Administración de COOMEVA, se establecen los siguientes términos y definiciones específicos para el **SGSI**:

Activo de Información: 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.

Activo Primario: Corresponde a la categoría de Información o Datos. Es todo activo que corresponde a actividades, procesos del negocio e información. De forma más general la información primaria comprende principalmente: información vital para la ejecución de la misión, información personal, información estratégica e información cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición.

Activo de Soporte: Es todo activo de los cuales dependen los elementos primarios del alcance (por ejemplo: hardware, software, redes, personal, instalaciones y estructura de la organización).

Amenaza: Causa potencial de un incidente no deseado que implica un daño a un sistema o a la organización.

Autorización: Consentimiento previo, expreso e informado del titular del dato personal para llevar a cabo el tratamiento de datos personales.

Base de datos: Todo conjunto organizado de datos personales que sea objeto de tratamiento, sin importar que se trate de una base de datos manual o automatizada.

Cadena de Custodia: La cadena de custodia de la prueba se define como el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones.

Ciberseguridad: Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: Medio para mitigar o gestionar un riesgo o amenaza identificada.

Contratistas: Colaboradores de Coomeva, administrados y contratados en Misión por las empresas del Grupo.

Cumplimiento: Es el proceso que registra y monitorea las políticas, los procedimientos y controles necesarios para garantizar que las políticas y los estándares se adhieran a él. Fuente: www.isaca.org.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables; Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.

Dato personal público: Dato que no es semiprivado, privado o sensible (Por ejemplo, datos relativos al estado civil de las personas, su profesión u oficio, su calidad de comerciante o servidor público, datos de ubicación de una persona en la empresa es público, correo electrónico de la empresa, la extensión asignada y aquellos que pueden obtenerse sin reserva alguna). 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.

Dato personal semiprivado: Dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento interesa al titular y a cierto sector o grupo de personas o a la sociedad en general (Por ejemplo, datos financieros y crediticios, dirección de residencia, teléfonos personales, correo electrónico personal, etc.).

Dato personal privado: Dato que solo es relevante para su titular (Por ejemplo, fotografías, videos, datos relacionados con su estilo de vida, datos de salud, resultado de exámenes de laboratorio, gustos personales, orientación sexual, etc.).

Dato personal sensible: Dato 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, los datos biométricos y los datos de niños, niñas y adolescentes.
Directriz: Especificación que aclara lo que debe hacerse y el cómo hacerlo, para alcanzar los objetivos definidos en las normas y políticas.

Disponibilidad: Garantizar que la información y los recursos relacionados con la misma estén accesibles, siempre que el personal autorizado a ello lo requiera.

Equipo de Respuesta a Incidentes de Seguridad y Privacidad de la Información: Equipo conformado por miembros confiables de la organización, que cuentan con las habilidades y competencias para tratar los incidentes de seguridad y privacidad de la información, durante el ciclo de vida de éstos.

Evaluación de Riesgos: Proceso de análisis y valoración del riesgo para evaluar las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la organización.

Evento de Seguridad y Privacidad de la Información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad y privacidad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Exposición al Riesgo: El grado al cual una vulnerabilidad puede resultar en consecuencias desfavorables; la pérdida potencial para una organización como resultado de un evento adverso que ha ocurrido.

GCR: Gerencia Corporativa de Riesgo.

GECC: Grupo Empresarial Cooperativo Coomeva.

Gobierno de Seguridad de la Información: La estructura y naturaleza del Gobierno de Seguridad de la Información es la misma definida en el Manual Corporativo del SGR para la Gestión del Riesgo en el **GECC**.

GRC: Gestión del Riesgo y Cumplimiento.

GTC-ISO/IEC 27035: Tecnología de la Información. Técnicas de Seguridad. Gestión de Incidentes de Seguridad de la Información.

Incidente de Seguridad de la Información: Evento adverso en un sistema informático que compromete la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. Causado generalmente mediante la explotación de alguna vulnerabilidad mediante una amenaza. También se define como evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Conjunto de datos ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado.

Integridad: Garantizar la exactitud y totalidad de la información y los métodos de procesamiento.

Investigación Forense de Seguridad de la Información: Aplicación de técnicas de investigación y análisis para recolectar, registrar y analizar información de incidentes de seguridad de la información.

ISO/IEC 27001:2013: Estándar internacional para la seguridad de la información de la Organización Internacional de Estandarización (ISO) y de la Comisión Internacional Electrotécnica.

ISO/IEC 27005:2018: Estándar internacional para proporcionar directrices en la Gestión del Riesgo de la Seguridad de la Información, apoyando así los conceptos generales especificados en la norma ISO/IEC 27001:2013.

ISO/IEC 27032:2012: Estándar internacional para proporcionar directrices en la Gestión de la Seguridad Cibernética.

ISO/IEC 31000:2011: Estándar internacional para la Gestión de Riesgos. Principios y Directrices.

Legalidad: Se refiere al cumplimiento de leyes, normas, directrices, reglamentaciones y/o disposiciones a las que está sujeta la organización.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales y es reglamentada por el Decreto 1377 de 2013.

Magerit V3.0: Metodología de análisis y gestión de riesgos de los sistemas de información, elaborada inicialmente para las compañías de administración pública de España.

Manual Corporativo de Seguridad y Privacidad de la Información: Es el documento que contiene las políticas, objetivos, estructura organizacional y de gobierno, estrategias, procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento del SGSI.

Oficial de protección de datos personales: Es la persona que tiene como función la vigilancia y control de la aplicación de la Política de Protección de Datos Personales, bajo la orientación y lineamientos del **GECC**. Toda vez que el **GECC**, está conformado por una agrupación de empresas, cada una de ellas, tiene designado un oficial de protección.

PESI: Plan Estratégico de Seguridad y Privacidad de la Información del **GECC**.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Seguridad de la Información: Se entiende como la preservación de las características: confidencialidad, integridad y disponibilidad de la información. Pueden estar involucradas características adicionales: autenticidad, responsabilidad, no repudio y confiabilidad.

SGR: Sistema de Gestión del Riesgo del **GECC**.

SGSI: Sistema de Gestión de Seguridad y Privacidad de la Información del **GECC**.

Terceros: Personas que no tienen un vínculo laboral directo con las empresas que componen el **GECC**. Por ejemplo: asociados, proveedores, visitantes, clientes, usuarios, etc.

Titular de los datos personales: Persona natural cuyos datos personales sean objeto de tratamiento.

Tratamiento de información: Cualquier acción sobre la información como creación, captura, almacenamiento, tránsito, procesamiento y disposición final.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. MARCO DE REFERENCIA PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

4.1. DEFINICIÓN DE LA GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Gerencia Corporativa de Riesgo (en adelante **GCR**) adopta las buenas prácticas de las normas **ISO/IEC 27001:2013**, **ISO/IEC 27032:2012** y los requerimientos de la **Ley 1581 de 2012 y decretos reglamentarios** para soportar los procesos de establecimiento, implementación, mantenimiento y mejora continua del **SGSI** de las empresas del **GECC**; tomando como referencia las necesidades y objetivos de la organización, los requisitos de seguridad y privacidad de los negocios, los procesos organizacionales definidos y el tamaño y estructura de la organización. El **SGSI** adoptado, estará alineado con el Sistema de Gestión Integral del **GECC** con el fin de aprovechar la madurez de este último y así facilitar el proceso de implementación al interior de las empresas.

La Presidencia Ejecutiva/Gerencia General de las empresas del **GECC**, serán los responsables de la gestión ante el establecimiento, implementación, operación, seguimiento, mantenimiento y mejora continua del **SGSI** para su empresa, asignando y comunicando las funciones, responsabilidades, autoridades y recursos necesarios para que la seguridad y privacidad de la información se integre a los procesos de la organización.

4.2. POLÍTICAS PARA LA GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La metodología se complementa con las Políticas para la Gestión de Riesgo contenidas en el documento **GC-DC-487 Manual Corporativo del Sistema de Gestión del Riesgo del GECC**.

4.2.1. Política de Seguridad y Privacidad de la Información del GECC

El **GECC** mediante su política de seguridad y privacidad de la información reconoce la información como un activo fundamental y estratégico para el desarrollo de las actividades del grupo, en donde la seguridad, la privacidad, la ciberseguridad y el conocimiento generado de esta información tiene una importancia primordial en los objetivos estratégicos.

La política de seguridad y privacidad de la información tiene como objetivo principal demostrar que *"El **GECC** se compromete con la gestión de los riesgos de seguridad,*

privacidad y ciberseguridad a los que se expone la información de sus grupos de interés[1] *y del negocio; manteniendo siempre los criterios de confidencialidad, integridad y disponibilidad"*.

Las actividades y determinaciones objeto de la política de seguridad y privacidad de la información serán revisadas ante cambios en la organización por la Presidencia Ejecutiva/Gerencia General de las empresas del **GECC**, para garantizar la adecuación y el continuo cumplimiento de los objetivos de seguridad y privacidad de la información, los cuales son gestionados a través de riesgos, controles y planes de seguridad y privacidad.

Los planes de seguridad y privacidad de la información deben ser desarrollados, implementados, continuamente ejercitados y mantenidos, atendiendo las necesidades y gestionando las responsabilidades con *asociados, colaboradores, contratistas, clientes, afiliados, usuarios y proveedores*, para el cumplimiento de objetivos, requisitos, obligaciones y responsabilidades de seguridad y privacidad de la información.

El establecimiento de los objetivos de seguridad y privacidad de la información estará ligado a las necesidades que, desde los procesos del **GECC**, se expresen con relación a los riesgos y oportunidades a los que está expuesta la información del alcance del **SGSI**.

De manera detallada las políticas de seguridad y privacidad de la información corporativas se definen y establecen en el documento **GC-DC-504 Políticas y Responsabilidades de Seguridad y Privacidad de la Información del GECC**. La Presidencia Ejecutiva será la responsable de la aprobación de las **Políticas y Responsabilidades de Seguridad y Privacidad de la Información del GECC**.

4.2.2. Política de protección de datos personales del GECC

La Política aplicará a todas las bases de datos y/o archivos que contengan datos personales que sean objeto de tratamiento por parte del **GECC**, incluida toda aquella información que haya sido obtenida o recolectada con anterioridad a la Ley 1581 del 2012 y cualquier otro dato que sea susceptible de ser tratado por las empresas del **GECC** en desarrollo de su objeto social o con ocasión de cualquier tipo de relación civil, laboral o comercial que llegue a surgir en virtud de sus actividades conexas o propias de su naturaleza societaria.

De manera detallada la política de protección de datos personales del **GECC** se define y establece en el documento **GC-DC-532 Política de Protección de Datos Personales**

[1] Grupos de interés: asociados, colaboradores, contratistas, clientes, afiliados, usuarios y proveedores

del GECC. La Presidencia Ejecutiva será la responsable de la aprobación de la **Política de Protección de Datos Personales** del **GECC**.

4.3. MECANISMOS DE COMUNICACIÓN INTERNA Y EXTERNA

Son los establecidos en el Manual Corporativo del **SISTEMA DE GESTIÓN DEL RIESGO DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA** (en adelante **SGR**), Capítulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO. Mecanismos de comunicación interna y externa y Capítulo 6. PROCESO PARA LA GESTIÓN DEL RIESGO. Comunicación y Consulta, como también los definidos en el presente manual Capítulo 5.6 COMUNICACIÓN Y CONSULTA DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

4.4. MECANISMOS DE CAPACITACIÓN

Son los establecidos en el Manual Corporativo del **SGR**, Capítulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO. Mecanismos de capacitación.

4.5. GOBIERNO Y ROLES PARA LA GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL GECC

La Estructura de Gobierno del **SGSI** en el **GECC** forma parte de la estructura general del Sistema de Gestión del Riesgo del **GECC** que se establece en el Manual Corporativo del **SGR**, Capitulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO. Gobierno para la Gestión del Riesgo en el **GECC.**

Las unidades y empresas del **GECC** aplicarán el modelo de Gobierno establecido en el Manual del **SGR** del **GECC**, mencionado en el párrafo anterior, y realizarán los ajustes necesarios según las normas empresariales o sectoriales y de organismos de vigilancia y control que les sean aplicables, cumpliendo como mínimo las siguientes funciones:

4.5.1. Consejo de Administración - Juntas Directivas

a) Aprobar la política de seguridad y privacidad de la información del **GECC**.
b) Garantizar la alineación entre la planeación estratégica del negocio (objetivos estratégicos) y el **SGSI**.
c) Aprobar el nivel de riesgo aceptable para el negocio, el apetito de riesgo (evaluación anual).
d) Supervisar el cumplimiento de las políticas y el cumplimiento de las exigencias regulatorias en seguridad y privacidad de la información.

e) Supervisar la utilización adecuada de los recursos de seguridad y garantizar la integración de la seguridad y privacidad de la información en los procesos de negocio.

f) Velar por la ejecución de acciones encaminadas a mitigar los riesgos a los que se encuentran expuestos los activos de información.

g) Conocer los activos de información y procesos críticos del negocio.

h) Apoyar la integración de las distintas iniciativas de seguridad y privacidad de la información para garantizar que los procesos operen de la forma planeada.

i) Garantizar la integración del Gobierno de Seguridad y Privacidad de la Información dentro del Gobierno Corporativo.

j) Apoyar el cumplimiento de los requerimientos legales y regulatorios relacionados con la seguridad y privacidad de la información y el control interno.

k) Definir y aprobar una estructura organizacional de seguridad y privacidad de la información con autoridad suficiente y recursos económicos adecuados.

l) Definir el régimen de sanciones por incumplimiento de las políticas de seguridad y privacidad del **GECC**.

4.5.2. Comité Corporativo de Auditoría y Riesgos de COOMEVA

La composición, funciones y demás aspectos relacionados con este Comité, son los establecidos en el Acuerdo No. 459 (CA-AC-2015.459) de abril 24 de 2015 aprobado por el Consejo de Administración de Coomeva y en el Manual Corporativo del **SGR**, Capitulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO.

4.5.3. Presidente Ejecutivo del GECC, Presidentes, Gerentes Generales o quienes hagan sus veces

a) Garantizar el compromiso de la alta dirección frente a las estrategias de seguridad y privacidad de la información.

b) Difundir la política de seguridad y privacidad del **GECC** y supervisar su aplicación.

c) Aprobar las políticas y responsabilidades de seguridad y privacidad de la información del **GECC** y supervisar su implementación, difusión y aplicación.

d) Aprobar y difundir la política de protección de datos personales del **GECC** y supervisar aplicación.

e) Aprobar los procedimientos de seguridad y privacidad de la información definidos para el **GECC**.

f) Aprobar y difundir la estrategia de seguridad y privacidad de la información.

g) Formalizar procesos para integrar la seguridad y privacidad de la información en los objetivos del negocio.

h) Verificar que los roles y responsabilidades de los cargos incluyan la gestión de riesgos en todas sus actividades, al igual que la seguridad y privacidad de la información.

i) Apoyar las iniciativas de sensibilización, capacitación y generación de cultura en seguridad y privacidad de la información para todos los colaboradores y contratistas del **GECC**.

j) Supervisar y garantizar el cumplimiento de las normas legales y regulaciones vigentes asociadas a la seguridad y privacidad de la información.

k) Exigir el desarrollo de casos de negocio que justifiquen las iniciativas e inversiones en seguridad y privacidad de la información.

l) Seguimiento de indicadores que midan la eficiencia de la estrategia de seguridad y privacidad de la información.

m) Asignar recursos adecuados y delegar autoridad para implementar y mantener el **SGSI**.

n) Apoyar el mejoramiento continuo de la seguridad y privacidad de la información.

4.5.4. Comité Corporativo de Gestión del Riesgo

Corresponde al Comité creado en el Manual Corporativo del **SGR**, Capitulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO.

4.5.5. Gerencia Corporativa de Riesgo (GCR)

La composición, funciones y demás aspectos relacionados con la GCR, son los establecidos en el Manual Corporativo del **SGR**, Capitulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO.

4.5.5.1. Jefatura Corporativa de Seguridad de la Información

Tendrá a su cargo las siguientes responsabilidades:

a) Proponer, implementar y mantener el Modelo de Gobierno, Gestión del Riesgo y Cumplimiento (**GRC**) que soporte la estrategia de seguridad y privacidad de la información del **GECC**.

b) Definir, socializar y ejecutar el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), garantizando su alineación con el Plan Estratégico del **GECC**.

c) Proponer, implantar y documentar las políticas, normas y procedimientos de seguridad y privacidad de la información aplicables al **GECC**.

d) Proponer, implantar y documentar la política de protección de datos personales del **GECC**.

e) Liderar el desarrollo de los proyectos de seguridad y privacidad de la información en las empresas del **GECC** que están bajo la supervisión de la **GCR**.

f) Facilitar y coordinar esfuerzos en el desarrollo de los proyectos de Seguridad y privacidad de la información en las demás empresas del **GECC.**

g) Proponer al Consejo de Administración y/o Juntas Directivas a través de la **GCR**, la política y las funciones generales en materia de seguridad y privacidad de la información para que sean sometidas a aprobación por parte de las instancias correspondientes.

h) Monitorear frecuentemente la implementación del **SGSI** en las empresas del **GECC**.

i) Monitorear el cumplimiento de los indicadores establecidos dentro del **SGSI**.

j) Diseñar, definir, implementar y monitorear el plan y actividades de seguridad y privacidad de la información, y supervisar su eficacia.

k) Garantizar la alineación constante de las iniciativas de seguridad y privacidad de la información con los procesos del negocio.

l) Monitorear los procesos de seguridad y privacidad de la información para garantizar que se alcancen los objetivos definidos.

m) Definir estrategias de capacitación y sensibilización en seguridad y privacidad de la información, al igual que la medición de la eficiencia y efectividad de las mismas.

n) Monitorear y evaluar de manera periódica los controles de seguridad y privacidad de la información para mitigar el riesgo a niveles aceptables en las empresas del **GECC**.

o) Conocer y consolidar las exposiciones, incidencias y el comportamiento de indicadores relativos a la seguridad y privacidad de la información dentro del **GECC**.

p) Definir procesos para la adecuada gestión de incidentes de seguridad y privacidad de la información.

4.5.5.2. Comité Técnico Corporativo de Seguridad y Privacidad de la Información

Es un Comité Técnico no decisorio que se rige por lo establecido en el Manual Corporativo de Gestión del Riesgo, por las Resoluciones reglamentarias suscritas por la Presidencia Ejecutiva del **GECC** y por las reglamentaciones emanadas de la **GCR**. Es liderado por el Jefe Corporativo Seguridad de la Información, con el apoyo de los representantes designados por cada una de las empresas del **GECC**. El Comité sesionará trimestralmente, pudiendo celebrar sesiones extraordinarias, y tendrá las siguientes responsabilidades específicas, además de las establecidas en las normas mencionadas:

a) Revisar y proponer actualizaciones periódicas al **Manual Corporativo de Seguridad y Privacidad de la Información del GECC** siempre que se vea impactado por cambios al interior de la organización o nuevas regulaciones.
b) Revisar, analizar y activamente propender por la alineación de las políticas, normas, procedimientos, controles y estrategias implementadas por las empresas del **GECC** para cumplir estándares y normativas (internas y externas) de seguridad y privacidad de la información.
c) Asegurar el cumplimiento del Gobierno de Seguridad y Privacidad de la Información en cada una de las empresas del **GECC**.
d) Revisar y apoyar la estrategia de seguridad y privacidad de la Información, al igual que su integración con los procesos de negocio.
e) Analizar el riesgo residual y promover prácticas de seguridad y privacidad de la información en cada una de las empresas.
f) Retroalimentar sobre la eficacia de los controles de seguridad y privacidad de la información que apoyan las funciones del negocio.
g) Revisar el avance de los procesos de capacitación y sensibilización en seguridad y privacidad de la información diseñados para el **GECC**.
h) Discutir las problemáticas de seguridad y privacidad de la información que atañen al **GECC** y propender por la solución de las mismas.
i) Socializar el seguimiento, supervisión y monitoreo de los incidentes de seguridad y privacidad de la información.
j) Realizar seguimiento a los proyectos de seguridad y privacidad de la información que sean ejecutados por el **GECC**, analizar la viabilidad de nuevos proyectos y su alineación con el Plan Estratégico de Seguridad y Privacidad de la Información definido.
k) Compartir experiencias obtenidas desde cada uno de los sectores en materia de seguridad y privacidad de la información, así como también analizar nuevas disposiciones regulatorias y mejores prácticas.

l) Revisar la exposición al riesgo de seguridad y privacidad de la información de los procesos analizados en el **GECC**.

m) Definir los lineamientos que contribuyan a la implementación del **SGSI**, así como colaborar en la unificación de criterios y resolución de problemáticas que afecten a las empresas del **GECC**.

n) Todas las demás que le sean asignadas por acuerdos del Consejo de Coomeva, resoluciones de la Presidencia Ejecutiva y reglamentaciones de la **GCR**.

4.5.5.3. Coordinador Regional / Zonal de riesgo

Es un rol que tiene la responsabilidad de orientar, acompañar, resolver dudas e inquietudes y promover junto con el Gerente corporativo regional o quien haga sus veces, la toma de consciencia en seguridad y privacidad de la información. Además, tendrá las siguientes responsabilidades específicas:

a) Apoyar a que se establezcan, implementen y mantengan los procesos necesarios para el **SGSI** (activos de información, riesgos e incidentes de seguridad y privacidad de la información).

b) Apoyar la gestión y mejoramiento del **SGSI** en la regional.

c) Capacitar a los colaboradores en los temas relacionados con la seguridad y privacidad de la información.

d) Implementar campañas de refuerzo e interiorización del **SGSI**.

e) Apoyar la realización de jornadas para impulsar el logro de los objetivos del **SGSI**.

f) Apoyar la realización de auditorías del **SGSI** y apoyar el seguimiento a la programación de auditorías internas.

g) Aplicar todo lo referente a los procedimientos fundamentales: control de documentos y registros, acciones preventivas, acciones correctivas, auditorías internas.

4.5.6. Áreas de Gestión del Riesgo de Seguridad y Privacidad de la Información en el GECC

Empresa	Responsables Directos	Apoyo
Coomeva	• Presidente Ejecutivo • Gerente Corporativa de Riesgo • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Fundación	• Gerente Nacional • Gerente Corporativa de Riesgo	• Jefe, coordinador y analista corporativo seguridad de la

Empresa	Responsables Directos	Apoyo
	• Líderes de los procesos	información
Club Los Andes	• Gerente General • Gerente Corporativa de Riesgo • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Financiero: • **Bancoomeva**	• Presidente • Vicepresidente de Riesgo y Gestión • Gerente Riesgo Operativo y Gestión • Oficial Seguridad y Ciberseguridad • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Financiero: • **Fiduciaria Coomeva**	• Gerente • Director de Riesgo de Operaciones • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Financiero: • **Conectamos Financiera**	• Gerente • Asistente de Riesgo y Tecnología • Líderes de los Procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Protección: • **Corredor de Seguros**	• Gerente Sector Protección • Gerente General • Jefe de Riesgo • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Salud: • **EPS**	• Gerente General • Gerente Nacional de Riesgo • Oficial de Privacidad y Seguridad de la Información • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Salud: • **Medicina Prepagada**	• Gerente General • Jefe Nacional de Riesgo • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Salud: • **Conecta Salud**	• Gerente • Coordinador de Proyectos • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Fondo de Empleados	• Gerente General • Coordinador Nacional de Riesgo Operativo y Financiero • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información

Tabla 2. Responsables de Seguridad y Privacidad de la Información

Empresa	Cargo
Coomeva e Integradas	• Jefe/A Corporativo Seguridad de la Información **Apoyo** • Coordinador/A Seguridad de la Información • Analista Seguridad de la Información
Bancoomeva	• Oficial Seguridad y Ciberseguridad • Analista Senior Seguridad Información
Fiduciaria Coomeva	• Director de Riesgo de Operaciones
Conectamos Financiera	• Asistente de Riesgo y Tecnología
Corredor de Seguros	• Jefe de Riesgo
Coomeva EPS	• Oficial de Privacidad y Seguridad de la Información

Empresa	Cargo
Coomeva MP	• Jefe Nacional de Riesgo
Conecta Salud	• Coordinador de Proyectos
Fondo de Empleados	• Coordinador Nacional de Riesgo Operativo y Financiero

Tabla 3. Oficiales de Protección de Datos Personales

4.5.7. Auditoria Corporativa

Sus funciones corresponden a las establecidas en el **MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DEL RIESGO DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA,** Capitulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO.

La Auditoría Corporativa tendrá las siguientes responsabilidades en materia de seguridad y privacidad de la información a nivel Corporativo.

a) Evaluar y reportar el grado de alineación de la estrategia de seguridad y privacidad de la información con los objetivos del **GECC**.
b) Evaluar y reportar acerca de los riesgos corporativos de seguridad y privacidad de la información en cuanto a la adopción de los marcos de gestión, así como frente a las prácticas de gestión de los mismos y sus resultados.
c) Evaluar y reportar acerca de los resultados del Plan Estratégico de Seguridad y Privacidad de la Información, y el uso adecuado de los recursos.
d) Evaluar y reportar sobre la eficiencia de los procesos de aseguramiento "controles" que se desarrollan en cada una de las empresas del **GECC**.
e) Realizar seguimiento a los planes de acción para salvaguardar los hallazgos de seguridad y privacidad de la información documentados en auditorías realizadas.
f) Realizar acompañamiento en la ejecución de nuevos proyectos con el fin de asesorar y brindar aseguramiento objetivo, evidenciando los riesgos que puedan surgir en el proceso.

4.5.8. Áreas de Responsabilidad de Dirección, Administración, Operación y Control

Además de las establecidas en el numeral 4.5.9 del presente Manual, sus funciones corresponden a las establecidas en el **MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DEL RIESGO DEL GRUPO EMPRESARIAL COOPERATIVO COOMEV**A, Capitulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO.

4.5.9. Áreas o Líderes Responsables de la Implementación del SGSI

Las áreas o líderes designados en cada una de las empresas del **GECC** para la implementación del **SGSI** deben:

a) Divulgar las políticas de seguridad y privacidad de la información a todo el personal y los cambios que en ellas se produzcan, y ejecutar las tareas de capacitación y sensibilización continua que sean necesarias.
b) Comunicar periódicamente a sus jefes inmediatos y a los responsables de las empresas y unidades de negocio del **GECC**, sobre las exposiciones, incidencias y el comportamiento de indicadores relativos a la seguridad y privacidad de la información.
c) Asesorar en materia de riesgos de seguridad y privacidad de la información a los líderes de procesos para alcanzar una adecuada implementación del **SGSI**.
d) Monitorear frecuentemente la implementación del **SGSI**.
e) Reportar periódicamente a la **GCR** o a quienes hagan sus veces en las empresas y unidades de negocio del **GECC**, los indicadores de seguridad y privacidad de la información acordados.
f) Verificar que se adopten las medidas tecnológicas y administrativas necesarias para evitar la adulteración, modificación, pérdida, consulta, uso o acceso no autorizado a los registros y repositorios del **GECC**, así como velar por la calidad y veracidad de la información por parte del Oficial de Protección de Datos Personales de las empresas del **GECC**, durante su uso, captura, recolección y tratamiento de datos personales y demás responsabilidades definidas en el documento **GC-DC-504 Políticas y responsabilidades de seguridad y privacidad de la información del GECC**.
g) Ejecutar todas las demás responsabilidades que les sean asignadas para el óptimo desarrollo del **SGSI**.

4.5.10. Líderes de Proceso

Los Líderes de proceso deben:

a) Identificar y mantener actualizado y valorado el inventario de activos de información de los procesos que lidera.
b) Realizar la identificación, medición y control de riesgos de seguridad y privacidad de la información cada vez que se cree o se realice un cambio en los procesos del negocio.

c) Definir e implementar planes de acción para reducir la exposición al riesgo hasta los niveles aceptados por la organización específicamente para los riesgos críticos y altos del mapa.

d) Reportar periódicamente a la **GCR** o a quienes hagan sus veces en las empresas y unidades de negocio del **GECC**, los incidentes de seguridad y privacidad de la información detectados.

e) Realizar divulgación de los mapas de riesgo y los controles asociados a todas las personas que intervienen en el proceso.

f) Promover la cultura de seguridad y privacidad de la información dentro de los procesos que lidera.

g) Garantizar que los derechos de los titulares de datos personales se cumplan en las actividades de los procesos que lidera, así como el adecuado funcionamiento de las medidas implementadas, mediante el monitoreo periódico y el registro de las evidencias de estas actividades.

h) Ejecutar todas las demás responsabilidades que les sean asignadas para el óptimo desarrollo del **SGSI**.

4.5.11. Propietarios de la Información

Los propietarios de la información deben:

a) Clasificar la información de acuerdo a los lineamientos y procedimientos establecidos para tal fin.

b) Documentar y mantener actualizada la clasificación efectuada.

c) Establecer los permisos de acceso a la información que se otorgarán a los diferentes usuarios según las funciones actuales que desempeñen en la entidad.

d) Ejecutar todas las demás responsabilidades que les sean asignadas para el óptimo desarrollo del **SGSI**.

4.5.12. Áreas de Gestión Humana del GECC

Gestión humana será responsable de:

a) Notificar a todo el personal que ingresa (colaboradores y contratistas), de sus obligaciones respecto del cumplimiento de las políticas de seguridad y privacidad de la información, y de todas las normas, procedimientos y prácticas que de ella se deriven.

b) Apoyar la divulgación de las políticas de seguridad y privacidad de la información a todo el personal y los cambios que en ellas se produzcan, la implementación de los compromisos de confidencialidad y las tareas de capacitación y sensibilización continua que sean necesarias.

c) Cumplir con las responsabilidades asignadas en el marco del **SGR** relacionadas con:

- Incluir responsabilidades de gestión del riesgo en los perfiles de cargo, en los contratos laborales y en el régimen de sanciones laborales para todos los colaboradores.
- Incluir los criterios e indicadores de gestión del riesgo de manera que formen parte de la definición de metas y logros, de las evaluaciones de desempeño y del plan de incentivos.
- Incluir la gestión del riesgo como un tema prioritario en los procesos de capacitación y sensibilización corporativos.

d) Garantizar la implementación de controles relacionados con la gestión del recurso humano que aseguren el cumplimiento de las políticas de seguridad y privacidad de la información definidas por el **GECC**.

e) Definir y revisar periódicamente el Reglamento Interno de Trabajo que se aplica a todos los colaboradores, y actualizar sus implicaciones en cuanto a violaciones a la seguridad y privacidad de la información.

f) Promover en los colaboradores la actualización de sus datos de tal forma que la base de datos de la Gerencia de Gestión Humana Corporativa refleje en forma precisa la información actual de todos los colaboradores.

g) Mantenerse informado sobre los roles y responsabilidades en cuanto a seguridad y privacidad de la información para que los tengan en cuenta durante el proceso de selección de personal o cuando existan cambios de roles de los colaboradores.

h) Evaluar los antecedentes de los colaboradores prospectivos, credenciales académicas, referencias y otros detalles personales.

i) Evaluar en profundidad los antecedentes de colaboradores prospectivos, que aspiren a cargos en los cuales tengan acceso a información Confidencial del **GECC** y/o privilegios elevados en los sistemas de información corporativos (estudios de seguridad).

j) Velar por el cumplimiento del procedimiento definido para el retiro de personal.

k) Ejecutar todas las demás responsabilidades que les sean asignadas para el óptimo desarrollo del **SGSI**.

4.5.13. Áreas de TI del GECC

Las áreas de TI del **GECC** son las encargadas de:

a) Cubrir los requerimientos generados en la operación, comunicación y administración de los sistemas tecnológicos del **GECC**.

b) Realizar las tareas de desarrollo y mantenimiento de los sistemas teniendo en cuenta las exigencias de ley y buenas prácticas en la materia.

c) Garantizar la implementación de controles tecnológicos que aseguren el cumplimiento de las políticas de seguridad y privacidad de la información definidas por el **GECC**.

d) Definir y garantizar el cumplimiento de las pruebas y los cronogramas para la ejecución del análisis, gestión y cierre de las vulnerabilidades a la plataforma tecnológica del **GECC**.

e) Asegurar un nivel aceptable de integridad y disponibilidad de la información almacenada en los sistemas de información que custodian las áreas de TI del **GECC**.

f) Definir y mantener la documentación y pruebas a los procedimientos requeridos y planes alternos de operación para garantizar la continuidad de la infraestructura tecnológica del **GECC**.

g) Apoyar a las áreas para definir los controles tecnológicos necesarios para el tratamiento de riesgos de seguridad y privacidad de la información.

h) Realizar seguimiento a los controles que tiene a cargo para custodiar y proteger los sistemas de información y servicios de TI donde se gestiona la información del **GECC** manteniendo los registros de la ejecución de esta actividad.

i) Revisar los logs generados por la plataforma tecnológica y reportar los eventos relacionados con seguridad y privacidad de la información (semanal) a los canales definidos en el procedimiento de Gestión de incidentes de seguridad y privacidad de la información.

j) Garantizar que los terceros que estén relacionados con el tratamiento de la información, cuenten con acuerdos de confidencialidad que permitan garantizar la gestión adecuada de los riesgos de privacidad de la información, antes, durante y después de terminada su relación contractual con ellos.

k) Ejecutar todas las demás responsabilidades que les sean asignadas para el óptimo desarrollo del **SGSI**.

4.5.14. Áreas Jurídicas del GECC

Las áreas jurídicas del **GECC** son las encargadas de:

a) Verificar el cumplimiento de las políticas de seguridad y privacidad del **GECC** en la gestión de todos los contratos, acuerdos de servicio u otra documentación del **GECC** con sus colaboradores, contratistas y proveedores.
b) Realizar asesorías en materia legal focalizadas a la seguridad y privacidad de la información en caso de ser requeridas.
c) Apoyar a la **GCR** a la identificación de nueva legislación y nuevas regulaciones para definir directrices a considerar en cuanto a la seguridad y privacidad de información.

4.5.15. Áreas de Seguridad Física del GECC

Las áreas de seguridad física del **GECC** son las encargadas de:

a) Elaborar, desarrollar, controlar y evaluar un plan de mantenimiento preventivo y reparativo de la infraestructura física.
b) Apoyar los proyectos de construcción de infraestructura física para la implementación de controles de seguridad física.
c) Brindar información y soporte oportuno a los requerimientos de los diferentes entes del estado, respecto a la infraestructura de la organización y controles de seguridad física.
d) Gestionar de manera oportuna los requerimientos relacionados con la infraestructura que afecten la seguridad y privacidad de la información, generados por el **GECC**.
e) Apoyar en la definición de controles de seguridad física para la infraestructura física teniendo en cuenta los requisitos de seguridad y privacidad de la información.
f) Apoyar el cumplimiento de la política de seguridad y privacidad de la información del **GECC** y las directrices dentro del área que lidera.
g) Aplicar controles de seguridad y privacidad de la información para proteger los registros físicos del **GECC**.
h) Realizar seguimiento y monitoreo a los controles de seguridad física implementados para proteger la seguridad y privacidad de la información del **GECC**.
i) Reportar al Jefe Corporativo de Seguridad de la Información o quien haga sus veces en las empresas del **GECC** eventos o incidentes relacionados con la

seguridad física que afecten la seguridad y privacidad de la información y mantener comunicación para implementar con prioridad las medidas de seguridad física que se definan poner en operación.

j) Participar en las pruebas de los planes de continuidad, de emergencia, contingencia, de respaldo y recuperación para los procesos y plataformas tecnológicas del **GECC**.

k) Apoyar cuando se requiera, la evaluación de las amenazas físicas que pueden afectar la seguridad y privacidad de la información del **GECC**.

4.5.16. Áreas de Compras y Gestión de Proveedores del GECC

Las áreas de Compras y Gestión de Proveedores del **GECC** son las encargadas de:

a) Incluir en los acuerdos con terceros requisitos de seguridad y privacidad de la información para tratar los riesgos asociados con el acceso de proveedores a los activos de la organización durante el suministro de productos y servicios.

b) Notificar a todos los proveedores de sus obligaciones respecto del cumplimiento de las políticas generales de seguridad y privacidad de la información del **GECC** aplicables a ellos, y de todas las normas, procedimientos y prácticas que de ellas se deriven.

c) Realizar seguimiento y monitoreo a la prestación del servicio de proveedores.

d) Reportar eventos e incidentes de seguridad y privacidad de la información relacionado con proveedores.

4.5.17. Todos los Colaboradores

Sus funciones corresponden a las establecidas en el Manual Corporativo del **SISTEMA DE GESTIÓN DEL RIESGO DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA**, Capitulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO.

Las responsabilidades de los colaboradores y contratistas del **GECC** incluyen (pero no se limitan a):

a) Acceder solo a los datos a los que tiene autorización y requiere utilizar para sus labores.

b) Propender por el uso adecuado y custodia de la información asociada a las funciones del cargo de acuerdo a su nivel de clasificación y a los niveles de tratamiento definidos por la empresa.

c) Acatar todas las leyes, regulaciones, normas y políticas (internacionales, nacionales, organizacionales, etc.) aplicables al buen uso de los recursos informáticos y la información.

d) Reportar toda violación detectada frente a la seguridad y privacidad de la información, y colaborar en las investigaciones relacionadas.

e) Proteger las claves y dispositivos de acceso asignados bajo su responsabilidad.

f) Proteger de manera adecuada la información que se genere hacia dispositivos de almacenamiento externo o hacia listados impresos.

g) Cerrar las aplicaciones y bloquear los equipos informáticos cuando los deje desatendidos.

h) Usar sólo software debidamente licenciado y/o autorizado por la organización.

i) Seguir y cumplir todos los procedimientos y políticas definidas para la seguridad y privacidad de la información aplicables a las labores realizadas.

j) Verificar la correcta actualización de los mecanismos de protección dispuestos por la organización para el aseguramiento de la información almacenada en las estaciones de trabajo.

k) Reportar cualquier evento o incidente de seguridad y privacidad de la información identificado.

l) Asistir a las capacitaciones y sensibilizaciones de seguridad y privacidad de la información para apoyar la estrategia de seguridad y privacidad del **GECC**.

Los conocimientos y habilidades requeridas para el gobierno y roles para la gestión de la seguridad y privacidad de la información del **GECC** están definidas en el **Anexo A - Conocimientos y habilidades para el gobierno del SGSI del GECC**.

5. PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

5.1 NORMAS

El proceso de Gestion del Riesgo de Seguridad y Privacidad de la Informacion definido por la **GCR** se soporta bajo las prácticas de la norma **ISO/IEC 31000:2011**; sin embargo, para realizar el análisis más detallado de los riesgos sobre los activos de información se complementa con las directricez de la norma **ISO/IEC 27005:2018 Information Security Risk Management**, la cual consta de las siguientes actividades: Establecimiento del contexto, Valoración del riesgo, Tratamiento del riesgo, Aceptación del riesgo, Comunicación del riesgo, Monitoreo y revisión del riesgo.

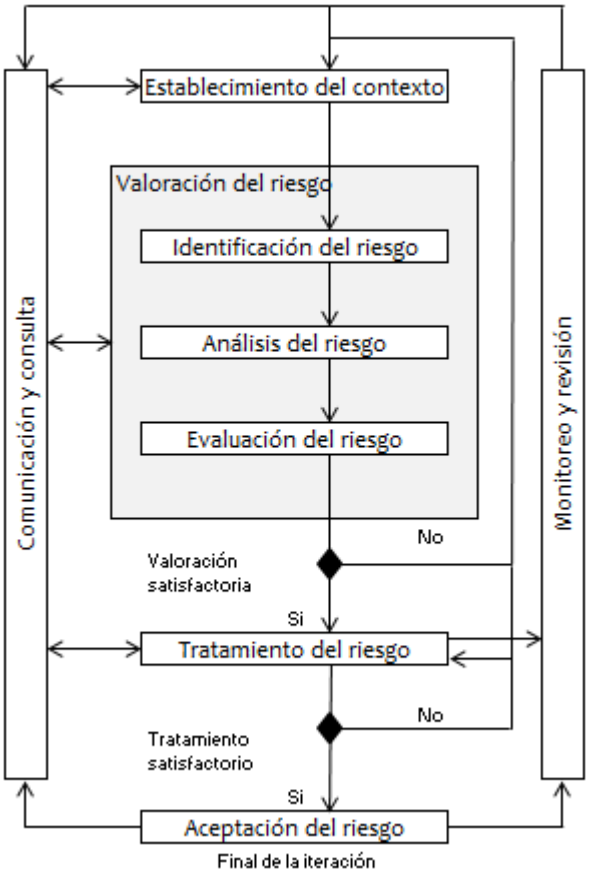

Figura 1. Proceso de Gestión del Riesgo de Seguridad de la Información ISO/IEC 27005:2011

Los análisis de riesgos se realizarán con periodicidad anual o cada vez que:

- Ocurran cambios significativos en los procesos, instalaciones de procesamiento de información o sistemas de información.
- Ocurran cambios sobre los criterios de aceptación de riesgos, y los criterios para realizar valoraciones de riesgos de la seguridad y privacidad de la información.
- Se materialice un riesgo (identificado o no).

A continuación, se presenta de forma general las actividades del proceso de gestión de riesgos de seguridad y privacidad de la información, para mayor detalle consultar el documento **GC-IN-585 Gestión de Riesgos de Seguridad y Privacidad de la Información.**

5.2 ESTABLECIMIENTO DEL CONTEXTO

En esta etapa se obtiene información para el entendimiento de los procesos o actividades del negocio con el fin de establecer los criterios básicos, definir el alcance y límites y la organización para una adecuada gestión del riesgo de la seguridad y privacidad de la información.

Para establecer el contexto de la organización se definen las siguientes actividades:

5.2.1 Levantamiento de Información

Se debe obtener información de los procesos a ser objeto del análisis de riesgos.

5.2.2 Definición de Criterios

Se definen los criterios de la organización acerca de cómo serán sus riesgos evaluados y tratados.

5.2.3 Definición del Alcance y Límites

Se seleccionan los procesos o actividades que se incluirán en el proceso de análisis de riesgos con el fin de garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo.

5.2.4 Organización para una adecuada gestión del riesgo de la seguridad y privacidad de la información

Se identifican y establecen los roles y responsabilidades para la gestión de riesgos de seguridad y privacidad de la información.

5.3 VALORACIÓN DEL RIESGO

En esta etapa se desarrollan las siguientes actividades:

- Identificación del riesgo.
- Análisis del riesgo.
- Evaluación del riesgo.

5.3.1. Identificación del riesgo

Para identificar los riesgos de seguridad y privacidad de la información se definen las siguientes actividades:

5.3.1.1. Conocimiento del proceso

Se definen las actividades a realizar para lograr un conocimiento del proceso a evaluar y poder identificar de manera general y previa al análisis de riesgos, los posibles activos de información, amenazas, vulnerabilidades y controles existentes.

5.3.1.2. Identificación, Valoración y Clasificación de Activos de Información

a) Definición del inventario:

En esta actividad, se listan los posibles activos de información identificados en la etapa anterior, posteriormente se socializan con el líder de proceso con el fin de generar el listado de activos de información definitivo.

Luego se debe llevar a cabo la valoración y clasificación de activos de información según lo establecido en el documento **GC-DC-537 Estándar para Valoración, Clasificación, Etiquetado y Manejo de la Información** y registrar la información en el formato **GC-FT-736 Inventario de Activos de Información**.

b) Revisión del inventario:

El inventario de activos de información se debe revisar periódicamente por el líder del proceso, esta actividad se refiere a la verificación que se puede llevar a cabo para determinar si la información continua o no siendo parte del inventario, o si los valores asignados a la información en cada campo deben ser actualizados, en esta parte se especifican los casos o eventos por los cuales se realizará la revisión del inventario de activos de información.

c) Actualización del inventario:

Una vez se ha definido qué cambios se realizarán en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información con los valores sugeridos para ello.

d) Publicación o formalización del inventario:

El inventario de activos información del proceso es un documento CONFIDENCIAL, y de acceso de sólo lectura para los usuarios autorizados por el líder del proceso.

El líder del proceso será el encargado custodiar y mantener actualizada la última versión del inventario de activos de información de su proceso.

5.3.1.3. Identificación de Amenazas y Vulnerabilidades en los Activos de Información

Con el objetivo de poder determinar el nivel de riesgo al cual está expuesto cada activo de información se requiere identificar las amenazas y vulnerabilidades, las cuales conforman las causas del riesgo, que podrían impactarles frente a su confidencialidad, integridad y disponibilidad y con base en ello asociarlos.

5.3.1.4. Redacción de los riesgos

Una vez se determina la causa del riesgo (amenaza y vulnerabilidad) del activo de información primario se continua con la redacción del riesgo con su respectivo identificador, el cual será incluido en el mapa de riesgos.

5.3.1.5. Redacción de las causas

Una vez se redacta el riesgo del activo de información primario se continua con la redacción de las causas, las cuales están conformadas por las vulnerabilidades.

5.3.2. Análisis del Riesgo

5.3.2.1. Estimación del Riesgo Inherente

En esta actividad se califican la probabilidad de ocurrencia y el impacto (analizándolos sin tener en cuenta ninguna medida de control que se encuentre establecida) con el fin de poder determinar el nivel de riesgo inherente, el cual se hará para cada escenario de riesgo identificado (conjunto de riesgo y causas <<amenaza y vulnerabilidades>>). Esta actividad se debe realizar con los responsables de la gestión de riesgos definidos. Para mayor detalle ver ejemplos en el documento **GC-IN-585 Gestión de Riesgos de Seguridad y Privacidad de la Información.**

Probabilidad: Es la posibilidad que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza sobre un activo de información.

Los criterios definidos para valorar la probabilidad son:

Probabilidad			
Escala	**Categoría**	**Descripción de Probabilidad**	**Descripción de Frecuencia**
5	Muy Alta	Se espera que ocurra la mayoría de las veces	Podría presentarse o ha ocurrido por lo menos una vez en el mes.
4	Alta	Probablemente ocurre muchas veces	Podría presentarse o ha ocurrido por lo menos una vez en el trimestre.
3	Media	Podría ocurrir algunas veces	Podría presentarse o ha ocurrido por lo menos 1 vez en el semestre.
2	Baja	Ocasionalmente puede ocurrir	Podría presentarse o ha ocurrido 1 vez en el año.
1	Muy Baja	Podría ocurrir excepcionalmente	No se ha presentado durante 1 año.

Tabla 4. Criterios Probabilidad de Ocurrencia

Impacto: Es la magnitud del daño que podría ser causado cuando una amenaza explota una vulnerabilidad del activo o control.

El impacto será el calculado en la etapa de valoración del activo. Si la amenaza identificada afecta una de las propiedades de la información (Confidencialidad, Integridad y Disponibilidad), se tomará el impacto de la propiedad afectada, si son dos o más, se tomará la calificación más alta de cada una de las áreas de impacto (Financiero, Operativo, Reputacional y Legal).

El impacto se mide cualitativamente a través de las cuatro categorías que se indican en la siguiente tabla:

IMPACTO					
ESCALA	**Consecuencias si el riesgo se materializa**	**Financiero (FI)**	**Operación/Servicio (OP)**	**Reputación/Imagen (IM)**	**Legal (LE)**
5. Catastrófico	A la organización le sería casi imposible recuperarse o los daños serian severos.	Pérdida mayor o igual al 100% del margen del patrimonio mínimo.	Falla de las operaciones y estándares de calidad, caída del servicio siendo muy difícil su recuperación. Perdida permanente o masiva de clientes, fallas de los principales proveedores.	Seria afectación de la reputación a nivel Nacional. Grave protesta pública o de los medios. Perdida de licencia social para operar.	Liquidación o Intervención de la organización por fraude, corrupción o graves incumplimientos. Máximas penalidades financieras.

IMPACTO					
ESCALA	**Consecuencias si el riesgo se materializa**	**Financiero (FI)**	**Operación/Servicio (OP)**	**Reputación/Imagen (IM)**	**Legal (LE)**
					Suspensión de actividades o cancelación de productos. Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.
4. Mayor	Las consecuencias a pesar de ser severas, podrían ser gestionadas hasta cierto punto.	Pérdida entre el 70% y 99% del margen del patrimonio mínimo.	Interrupción/falla significativa de las operaciones y el servicio entre 24 y 72 horas. Falla en logro de metas de proyectos clave, no cumplimiento de especificaciones de productos, graves fallas de calidad, alto retiro de clientes.	Afectación de la reputación a nivel Regional. Cobertura adversa significativa en públicos y medios. Requiere declaraciones públicas de la organización.	Sanciones económicas significativas por incumplimiento de normas establecidas/operaciones / obligaciones contractuales por parte de los Entes de control y vigilancia. Cierre temporal de las operaciones relacionadas con el tratamiento de datos sensibles.
3. Moderado	Las consecuencias no serían severas y, podrían ser gestionadas.	Pérdida entre el 50% al 69% del margen del patrimonio mínimo.	Interrupción/falla moderada de las operaciones y el servicio entre 12 y 24 horas, tensas relaciones con clientes y proveedores. Problemas de calidad. Demora en proyectos.	Afectación de la reputación en niveles Locales. Afectación y riesgo en las relaciones con la comunidad.	Glosa con sanciones económicas menores por incumplimiento de las normas u obligaciones. Incumplimiento de un contrato. Suspensión hasta por 6 meses del tratamiento de datos sensibles.
2. Menor	Las consecuencias serían consideradas relativamente poco importantes.	Pérdida entre el 10% y 49% del margen del patrimonio mínimo.	Interrupción de las operaciones de la organización por algunas horas. (menos de 12 horas). Reducción menor en estándares de calidad.	Afectación moderada de la reputación a nivel Interno o quejas o reacción adversa menor en públicos y medios que no requiere medidas especiales.	Glosa por parte de Entes de control sin sanciones económicas por incumplimiento de normas u obligaciones. Multas institucionales hasta por el equivalente de 2.000 smmlv por incumplimiento de la Ley 1581 de 2012.
1. Insignificante	No hay consecuencias detectables.	Pérdida entre el 5% y 9% del margen del patrimonio mínimo.	No hay interrupción de las operaciones de la organización.	Afectación leve de reputación a nivel Interno o preocupación pública sin efecto duradero. No es de interés público.	Se imponen glosas u observaciones por parte de Control Interno.

Tabla 5. Categorías de Clasificación de Impacto del Riesgo

El nivel de riesgo inherente se calcula tomando el valor más alto de las probabilidades de las causas del riesgo y del impacto del escenario de riesgo como se puede observar en la siguiente tabla:

RIESGO INHERENTE						
PROBABILIDAD	IMPACTO				VALORACION IMPACTO	NIVEL DEL RIESGO INHERENTE
	Financiero	Operación / Servicio	Imagen / Reputación	Legal		
(5) Muy Alta	(2) Menor	(4) Mayor	(5) Catastrófico	(1) Insignificante	(5) Catastrófico	(4) Critico

Tabla 6. Calculo Nivel de Riesgo Inherente

5.3.2.2. Identificación y Evaluación de los Controles Existentes

Una vez calculado el nivel del riesgo inherente, los responsables de la gestión de riesgos deben realizar la identificación y evaluación de los controles existentes para cada una de las vulnerabilidades identificadas y de esta forma reducir el nivel de riesgo.

Los controles identificados serán evaluados de acuerdo a lo definido en el documento **GC-DC-487 Manual Corporativo del Sistema de Gestión de Riesgo – Numeral 6.2.2.3** y documentos específicos de los negocios para este tema si aplica.

5.3.2.3. Estimación Riesgo Residual

De acuerdo a la evaluación de cada uno de los controles, el valor de la probabilidad e impacto inherente son recalculados, dando como resultado la probabilidad y el impacto residual para cada escenario de riesgo.

5.3.3. Evaluación del Riesgo

5.3.3.1. Redacción de las consecuencias

Una vez se obtiene los niveles de riesgo inherente y residual se continua con la redacción de las consecuencias del riesgo.

5.3.3.2. Priorización de los riesgos

En esta etapa se organizan los riesgos, primero de acuerdo al nivel de riesgo, posteriormente por el impacto (de mayor a menor) y por último por la probabilidad (de

mayor a menor). De esta manera se organizan los riesgos en el orden de prioridad en el cual deben ser presentados al líder del proceso para su revisión y ajustes de ser necesario. Finalmente se firma el acta de aceptación de los mismos por parte del líder del proceso.

5.3.3.3. Generación Mapa de Calor

La combinación de probabilidad e impacto determinan el nivel de los riesgos, los cuales son clasificados en cuatro zonas denominadas zonas de severidad del riesgo.

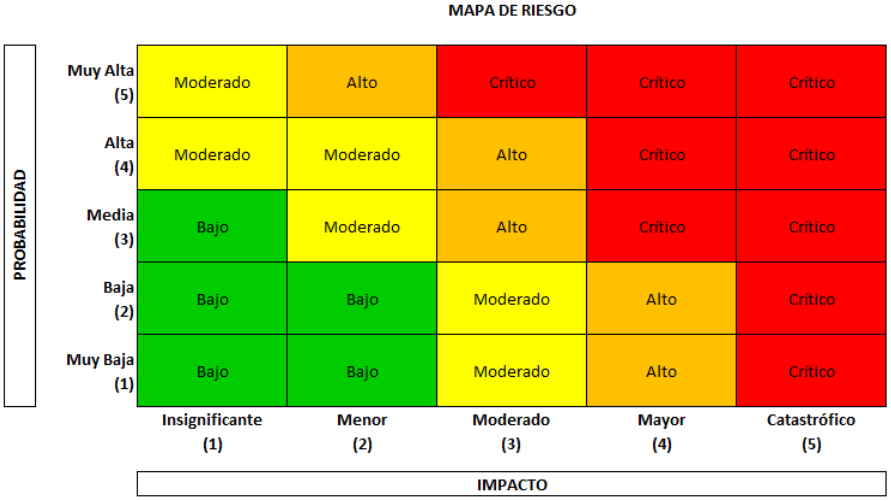

Figura 2. Mapa de Riesgos

Las definiciones de las zonas en el mapa de riesgos son las siguientes:

Bajo (Zona Verde): Un riesgo situado en esta región del mapa significa que la combinación probabilidad - impacto no implica una gravedad significativa, por lo que no amerita la inversión de recursos y no requiere acciones adicionales para su gestión diferentes a las ya aplicadas.

Moderado (Zona Amarilla): Un riesgo situado en esta región del mapa significa que, aunque deben desarrollarse actividades para la gestión sobre el riesgo, estas tienen una prioridad de segundo nivel, pudiendo ser desarrolladas a mediano plazo (6 a 12 meses); estas actividades son de responsabilidad del Líder del Proceso según corresponda y de la Presidencia Ejecutiva, Presidentes o Gerentes Generales.

Alto (Zona Naranja): Un riesgo situado en esta región del mapa significa que se requiere siempre desarrollar acciones prioritarias a corto plazo (3 a 6 meses) para su gestión,

debido al alto impacto que tendrían sobre el sistema y la organización. Estas actividades son de responsabilidad del Líder del Proceso según corresponda, de la Presidencia Ejecutiva, Presidentes o Gerentes Generales y del Consejo de Administración o Juntas Directivas. A partir de este nivel, el riesgo no es aceptable por la organización.

Crítico (Zona Roja): Un riesgo situado en esta región del mapa significa que bajo ninguna circunstancia se deberá mantener un escenario con esa capacidad potencial de afectar la estabilidad del sistema y la organización. Por ello, estos riesgos requieren una atención de alta prioridad (1 a 3 meses) para buscar disminuir en forma inmediata su medida. Las acciones que se definan son de responsabilidad del Líder del Proceso según corresponda, de la Presidencia Ejecutiva, Presidentes o Gerentes Generales y del Consejo de Administración o Juntas Directivas

Las zonas de riesgo no toleradas (alto, critico) son aquellas donde se ubican los riesgos no aceptables para la organización y para los cuales deben diseñarse y llevarse a cabo planes de tratamiento para lograr disminuir el nivel de riesgo y llevarlos a zonas toleradas para el **GECC**.

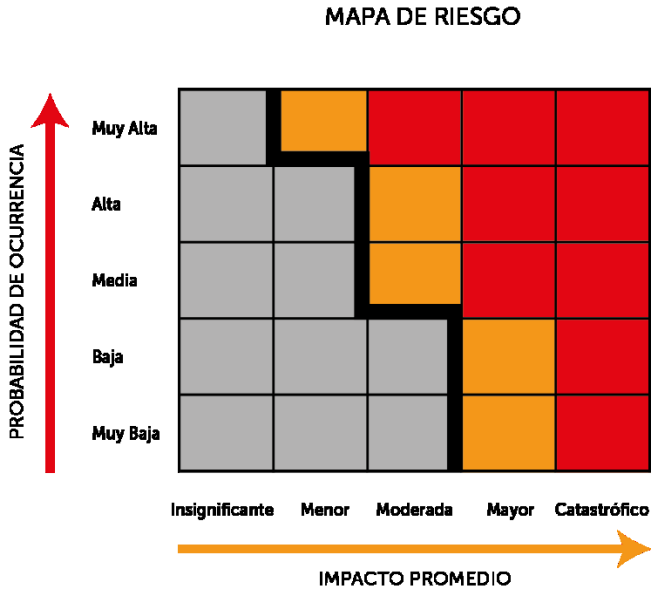

Figura 3. Zonas de Riesgo No Toleradas

5.4. TRATAMIENTO DEL RIESGO

En esta etapa se diseñan las acciones que deberán ser implementadas para que los riesgos ubicados en zonas no toleradas de riesgo, se conviertan en riesgos aceptables

para la organización. Las cuatro opciones disponibles para el tratamiento del riesgo son: Reducir, Asumir, Evitar y Transferir:

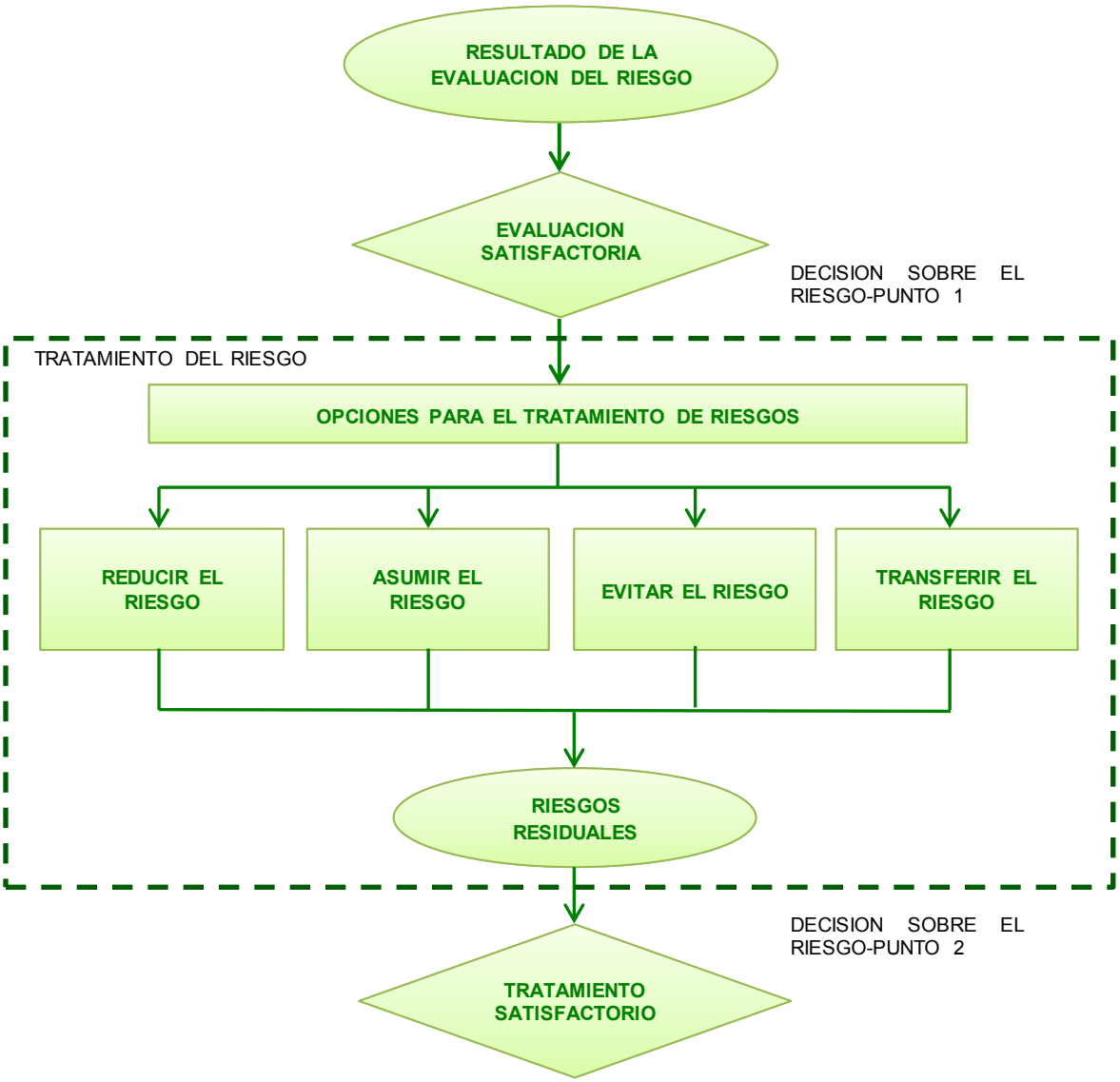

Figura 4. Actividad para el Tratamiento del Riesgo

Las opciones para la evaluación del riesgo deberán ser seleccionadas teniendo en cuenta la relación costo-beneficio, es decir, los tratamientos a implementar no deberán representar un costo mayor a la materialización del riesgo. Es recomendable considerar las opciones asociadas al desarrollo de controles que permitan una reducción alta de los riesgos a un costo relativamente bajo.

5.4.1. Opciones para el Tratamiento de los Riesgos

5.4.1.1. Reducir el riesgo

Se toma la decisión de mitigar el riesgo a través de la implementación de controles, a fin de que los riesgos sean reevaluados como riesgos aceptables para el **GECC**. Para lograrlo se deberán tener en cuenta los criterios de aceptación de riesgos, así como políticas, escenarios legales, reglamentarios y contractuales.

5.4.1.2. Asumir el riesgo

Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de los riesgos, en este caso, si los riesgos satisfacen los criterios de aceptación, no resultará necesaria la implementación de nuevos controles.

5.4.1.3. Evitar el riesgo

Si es evidente que el costo de implementar un tratamiento sobre riesgos específicos es considerablemente alto, se puede decidir dar de baja la actividad o la acción que origina el riesgo particular.

5.4.1.4. Transferir el riesgo

Asociado a la decisión de compartir riesgos con partes externas, en este sentido, transferir la responsabilidad para gestionar riesgos específicos. Este tratamiento puede involucrar la compra de seguros que permitirán soportar las consecuencias de la materialización de una amenaza, así como también solicitar servicios de monitoreo en procesos o sistemas de información. Cabe anotar que es posible la fusión de las opciones de tratamiento anteriormente expuestas, esto quiere decir que no son excluyentes entre ellas.

Teniendo en cuenta la anterior información se elabora el plan de tratamiento con los controles propuestos para los riesgos ubicados en la zona no tolerable, posteriormente junto con el líder del proceso se revisan, se ajustan de ser necesario y finalmente debe ser firmado como constancia de su aceptación.

El tratamiento de los riesgos de seguridad y privacidad de la información se definirán en el formato **GC-FT-737 Matriz de Riesgo Seguridad y Privacidad de la Información**.

5.5. ACEPTACIÓN DE RIESGOS

En esta etapa es necesario asegurar que los riesgos resultantes posteriores a la implementación del plan de tratamiento son aceptados por la alta dirección del **GECC**. Para ello deberá ser documentada formalmente la responsabilidad, condiciones y justificación de la decisión en caso de que dichos riesgos no cumplan con los criterios normales de aceptación del riesgo en el **GECC**.

Para la aceptación de riesgos de seguridad y privacidad de la información se utilizará el formato **GC-FT-726 Aceptación de Riesgos de Seguridad y Privacidad de la Información**.

5.6. COMUNICACIÓN Y CONSULTA DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La fase de comunicación de riesgos involucrará la información resultante en las etapas anteriormente descritas para la Gestión de Riesgos de Seguridad y Privacidad de la Información, y deberá ser compartida entre los altos directivos y partes involucradas a nivel interno (áreas de las empresas que componen el **GECC**, colaboradores y directivos) y externo (clientes, proveedores y entes reguladores) para la toma de decisiones. En esta fase de comunicación se establecen los aspectos mínimos del plan de comunicación y los medios para comunicar la gestión de riesgos.

5.7. MONITOREO Y REVISIÓN DEL RIESGO EN LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se deberán revisar y monitorear todos los riesgos y sus factores (impactos de los activos de información, amenazas, vulnerabilidades, probabilidades, etc.) con el objetivo de evidenciar de manera temprana cualquier tipo de cambio en el contexto de las empresas que componen el grupo y de esta forma mantener una visión amplia de la perspectiva en riesgos de seguridad y privacidad de la información **GECC**.

El monitoreo permanente de los riesgos posibilitará la continua gestión manteniendo alineada de esta forma los objetivos estratégicos del **GECC** con los criterios de aceptación de los riesgos.

6. GESTIÓN DE CUMPLIMIENTO

6.1. NORMAS

6.1.1. La **GCR** a través del equipo de Seguridad y Privacidad de la Información ejecutará una vez al año (o cuando sea necesario) una validación de la normatividad emitida en materia de seguridad y privacidad de la información aplicable al **GECC**, con el fin definir las acciones necesarias que garanticen su acogimiento. Algunos de los entes que regulan la operación del **GECC** son:

- Superintendencia Financiera de Colombia.
- Superintendencia de la Economía Solidaria.
- Superintendencia Nacional de Salud.
- Superintendencia de Industria y Comercio.
- Superintendencia de Sociedades.
- Otros entes de control.

6.1.2. La **GCR** a través del equipo de Seguridad y Privacidad de la Información ejecutará una vez al año (o cuando sea necesario) una validación del acogimiento de las políticas y procedimientos de seguridad y privacidad de la información por parte de los colaboradores, contratistas y proveedores del **GECC**.

6.1.3. Los responsables de seguridad y privacidad de la Información o quien haga sus veces en las empresas que no están bajo la supervisión directa de la **GCR** deben ajustarse a los lineamientos descritos en el presente documento.

6.1.4. Los Oficiales de Protección de Datos Personales o quien haga sus veces en las empresas del **GECC**, deben velar porque toda información de tipo personal que se registre en las bases de datos, cuente con la autorización del Titular para su tratamiento.

6.1.5. Los Oficiales de Protección de Datos Personales o quien haga sus veces en las empresas del **GECC**, deben garantizar el marcado de las bases de datos de acuerdo a los requerimientos legales.

6.1.6. El equipo de Seguridad y Privacidad de la Información de la **GCR** o quien haga sus veces en las empresas del **GECC**, son responsables de definir los mecanismos internos para reportar a la organización (dirigentes, administradores, accionistas, socios, etc.) el seguimiento y ejecución del **SGSI**.

6.2. OBJETIVO

El cumplimiento de políticas y estándares es una preocupación permanente y prioritaria dentro del **SGSI**. Es por esto que la **GCR** y los responsables de seguridad y privacidad de la información en las empresas del **GECC** buscan garantizar los siguientes objetivos:

1. Cumplimiento de requisitos legales y contractuales que aplican al **GECC** en materia de seguridad y privacidad de la información.
2. Revisiones de seguridad y privacidad de la información, con el fin de asegurar la adopción de políticas y procedimientos definidos por el **GECC**.

A continuación, se presenta de forma detallada el alcance de los objetivos del proceso de cumplimiento de seguridad y privacidad de la información:

6.2.1. Cumplimiento de requisitos legales y contractuales

El objetivo del equipo de Seguridad y Privacidad de la Información de la **GCR** y los responsables de seguridad y privacidad de la información en las empresas del **GECC** es evitar el incumplimiento de las exigencias legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad y privacidad de la información dentro del **GECC**; y en especial, aquellas que se encuentren relacionadas con:

- Identificación de la legislación aplicable y requisitos contractuales (internos y externos).
- Derechos de la propiedad intelectual.
- Protección de registros.
- Privacidad y protección de datos personales.
- Reglamentación de controles criptográficos.

6.2.2. Revisiones de seguridad y privacidad de la información

El objetivo del equipo de Seguridad y Privacidad de la Información de la **GCR** y los responsables de seguridad y privacidad de la información en las empresas del **GECC** será garantizar que las políticas y procedimientos definidos para el **GECC** se implementen y operen de forma adecuada.

- Revisión independiente de la seguridad de la información.
- Cumplimiento con las políticas y normas de seguridad.

- Revisión del cumplimiento técnico.

La metodología definida por la **GCR** para cumplir los objetivos propuestos frente al cumplimiento en Seguridad y Privacidad de la Información, se encuentra detallada en el documento **GC-IN-581 Identificación y Cumplimiento Normativo en Seguridad y Privacidad de la Información**. En materia de protección de datos personales se deberá consultar el documento **GC-IN-540 Lineamientos para el Tratamiento de Datos Personales en el GECC**.

7. GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.1. OBJETIVO

Con el fin de dar respuesta adecuada y eficaz a las amenazas y vulnerabilidades que se puedan presentar o materializar sobre los activos de información de las empresas y unidades del **GECC**, la **Gerencia Corporativa de Riesgo** (en adelante **GCR**) es responsable de definir un procedimiento estándar de Gestión de Incidentes de Seguridad y Privacidad de la Información soportado en las buenas prácticas de la guía técnica colombiana **GTC-ISO-27035:2013**.

El proceso de Gestión de Incidentes de Seguridad y Privacidad de la Información definido por el **GECC** tiene como objetivos principales:

a. Definir roles y responsabilidades dentro de la organización como eje puntual para evaluar los riesgos y que permita mantener la operación, la continuidad y la disponibilidad del servicio.
b. Gestionar los eventos de seguridad y privacidad de la información para detectar, reportar y evaluarlos como incidentes de seguridad y privacidad de la información de forma eficaz y oportuna.
c. Responder a incidentes de seguridad y privacidad de la información, y hacer su gestión.
d. Detectar, evaluar y gestionar las vulnerabilidades de seguridad y privacidad de la información.
e. Minimizar los impactos adversos de los incidentes en la organización y sus operaciones de negocios mediante los controles adecuados como parte de la respuesta a los incidentes.
f. Mejorar continuamente la seguridad y privacidad de la información, y la gestión de incidentes en general con el apoyo de los diferentes actores del proceso, consolidando las lecciones aprendidas que dejan su gestión.

7.2. ROLES Y RESPONSABILIDADES PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL GECC

Los roles y responsabilidades para la gestión de incidentes de seguridad y privacidad de la información en el **GECC** se encuentran detallados en el documento **GC-DC-504 Políticas y Responsabilidades de Seguridad de la Información del GECC**.

7.3. FASES DE LA GESTIÓN DE INCIDENTES

Con el fin de alcanzar los objetivos planteados, el equipo de Seguridad y Privacidad de la Información de la **GCR** sigue las cinco (5) fases definidas por la **GTC-ISO-27035:2013** para garantizar la gestión adecuada de los incidentes de seguridad y privacidad de la información identificados por el negocio. Las fases mencionadas y el alcance de las mismas se presentan a continuación:

Figura 5. Fases de la gestión de incidentes de seguridad y privacidad de la información

Para mayor detalle de la gestión de incidentes de seguridad y privacidad de la información se referencia el documento **GC-IN-584 Gestión de Incidentes de Seguridad y Privacidad de la Información**.

Nota: Los responsables de seguridad y privacidad de la información o quien haga sus veces en las empresas que no están bajo la supervisión directa de la **GCR**, deben ajustarse a los lineamientos definidos a continuación y seguir las particularidades definidas en la documentación con la que cuentan para este tema.

7.3.1. PLANIFICACIÓN Y PREPARACIÓN

7.3.1.1. Política de gestión de incidentes de seguridad y privacidad de la información.

Todos los dirigentes, administradores, directivos, colaboradores, contratistas, proveedores, asociados, clientes, afiliados y usuarios de las empresas y unidades del **GECC** tienen la responsabilidad de detectar y reportar los eventos de seguridad y privacidad de la información que son ocasionados por accidentes, errores o actos maliciosos intencionados, robo, apropiación indebida, extorsión, fraude, espionaje o eventos ambientales; de tal forma que la **GCR** o quien hagan sus veces en las empresas del **GECC** acompañe y verifique que las áreas responsables brinden solución oportuna y eficaz y establezcan los controles correspondientes.

El despliegue de la Política de Gestión de Incidentes de Seguridad y Privacidad de la Información es aprobado por la Presidencia Ejecutiva.

7.3.1.2. Políticas de gestión de riesgos, seguridad y privacidad de la información.

Las Políticas para la Gestión de Riesgo se encuentran contenidas en el documento **GC-DC-487 Manual Corporativo del Sistema de Gestión del Riesgo del GECC** y las de seguridad y privacidad de la información se encuentran en el documento **GC-DC-504 Políticas y Responsabilidades de Seguridad y Privacidad de la Información del Grupo Empresarial Cooperativo Coomeva (GECC)**. Estas políticas deben revisarse y actualizarse en conjunto con otras políticas corporativas como la de Continuidad de Negocio.

El **GECC** cuenta con los mecanismos de respuesta a las solicitudes y reclamos de los titulares de acuerdo a lo exigido por la Ley de protección de datos personales; por lo que se define la Política de Protección de Datos Personales y el Aviso de Privacidad publicado en su página web www.coomeva.com.co.

7.3.1.3. Equipo de respuesta a incidentes de seguridad y privacidad de la información

El Equipo de Respuesta a Incidentes de Seguridad y Privacidad de la Información de las empresas que están bajo la supervisión de la **GCR** está conformado por el personal de Seguridad y Privacidad de la Información de la **GCR**, los líderes técnicos de la Unidad de Tecnología Informática (UTI/CSA) que sean requeridos y los líderes de los procesos o servicios afectados; y estará liderado por el Jefe Corporativo de Seguridad de la

Información o quien este designe. Las empresas que no están bajo la supervisión de la **GCR** deberán adoptar esta práctica, liderada por el responsable de seguridad y privacidad de la información designado.

7.3.1.4. Esquema de gestión de eventos de riesgo

Para definir la **Gestión de incidentes de seguridad y privacidad de la información** se parte de la **Gestión de eventos de riesgo**, el cual es el punto de partida para todos los sistemas de riesgos que hacen parte del Sistema de Gestión del Riesgo del **GECC** y contempla de manera general las etapas 2, 3 y 4 de la **FASE DE GESTIÓN DE INCIDENTES** mostradas en la **Figura 5** de este documento.

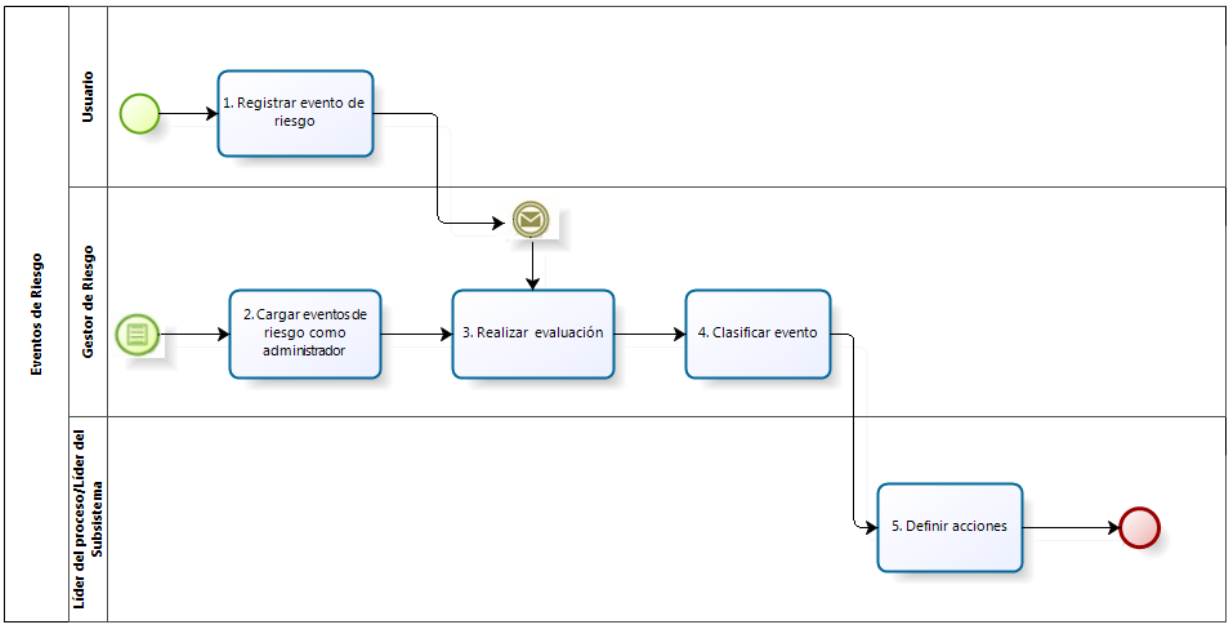

Figura 6. Flujo de Gestión de Evento de Riesgo (Alto Nivel)

7.3.1.5. Esquema de gestión de incidentes de seguridad y privacidad de la información

Los dirigentes, administradores, directivos, colaboradores, contratistas, proveedores, asociados, clientes, afiliados y usuarios del **GECC** tienen la responsabilidad de identificar y reportar los eventos de seguridad y privacidad de la información a través de los medios definidos por la organización descritos en el documento **GC-IN-584 Gestión de Incidentes de Seguridad y Privacidad de la Información**, y donde se puede encontrar una descripción más detallada del proceso de identificación, reporte y gestión de eventos e incidentes de seguridad y privacidad de la información.

7.3.1.6. Toma de conciencia de gestión de incidentes de seguridad y privacidad de la información

Se deben establecer planes de sensibilización para los usuarios (internos y externos) relacionados con la identificación y reporte de eventos de seguridad y privacidad de la información.

7.3.1.7. Pruebas del esquema de gestión de incidentes de seguridad y privacidad de la información

Se deben documentar las pruebas que se programen sobre el esquema de gestión de incidentes de seguridad y privacidad de la información definido por el **GECC**.

7.3.2. DETECCIÓN Y REPORTE

Se deben establecer los mecanismos para que los usuarios internos y externos del **GECC** detecten y reporten los eventos de seguridad y privacidad de la información a través de los medios establecidos por la organización. Para un mayor detalle, referirse al documento **GC-IN-584 Gestión de Incidentes de Seguridad y Privacidad de la Información**. La información mínima requerida para el registro del evento se presenta en el formulario **GC-FT-692 Reporte de eventos e incidentes de seguridad y privacidad de la información**.

7.3.3. EVALUACIÓN Y DECISIONES

7.3.3.1. Evaluación y categorización de los eventos

Se deben analizar los eventos reportados por los usuarios internos y externos del **GECC**, y definir si estos efectivamente representan un incidente de seguridad y privacidad de la información, así mismo su impacto, las pérdidas y recuperaciones que puedan ser asociadas a este, para la categorización y el trámite correspondiente de los mismos.

7.3.3.2. Documentación del incidente

Se debe documentar en forma detallada el incidente, con el fin dar respuesta al mismo. La información detallada para dar respuesta al incidente de seguridad y privacidad de la información se presenta en el formulario **GC-FT-692 Reporte de Eventos e Incidentes de Seguridad y Privacidad de la Información**.

7.3.3.3. Categorización del incidente

Se debe categorizar el incidente documentado para el manejo estadístico correspondiente. Para esto se tiene en cuenta la lista de categorías de la guía técnica colombiana **GTC-ISO-27035:2013**:

Categorías de incidentes

- Desastre natural
- Disturbios sociales
- Daño físico a equipos e instalaciones
- Fallas de infraestructura física y de TI
- Perturbación por radiación
- Falla técnica de sistemas de información
- Software malicioso (malware)
- Ataque técnico
- Violación o incumplimiento de requisitos legales, contractuales o uso inadecuado de recursos
- Compromiso de las funciones
- Poner en riesgo de la información del Negocio
- Poner en riesgo de la información de Datos Personales
- Contenidos peligrosos en las redes de información
- Otros incidentes

Nota: Para una descripción más detallada de las categorías de incidentes, referirse al documento **GC-IN-584 Gestión de Incidentes de Seguridad y Privacidad de la Información**.

7.3.4. RESPUESTAS

7.3.4.1. Priorización y respuestas al incidente

Se debe dar respuesta a los incidentes de seguridad y privacidad de la información dentro de los tiempos acordados según su prioridad.
Se debe acordar con el usuario o área afectada el tiempo requerido para gestionar el incidente de seguridad y privacidad de la información; siempre y cuando éste no afecte la disponibilidad de los servicios tecnológicos corporativos.

7.3.4.2. Análisis forense

Se deben definir los requisitos para la ejecución o contratación de una Investigación Forense (en caso que se requiera) que permita identificar a detalle el origen, responsable y comportamiento del incidente. Así mismo, garantizar la cadena de custodia correspondiente en caso que el incidente tenga un tratamiento judicial.

7.3.4.3. Recuperación del incidente

Se debe garantizar la recuperación del negocio ante el incidente presentado.

7.3.4.4. Reportes relacionados con la privacidad de la información

Se debe reportar de forma inmediata (o una vez se analicen) a los titulares de la información (clientes, colaboradores, contratistas y proveedores) los incidentes presentados sobre sus datos personales, las consecuencias asociadas a los mismos y los mecanismos que podría adoptar para disminuir el daño potencial.

Se debe reportar de forma oportuna a la Superintendencia de Industria y Comercio (SIC) los incidentes presentados sobre los datos personales de los titulares de la información. El reporte debe ser realizado a través del aplicativo RNBD dispuesto por la SIC https://rnbd.sic.gov.co/sisi/login.

Se debe recolectar información de los incidentes para soportar el reporte correspondiente ante la SIC.

7.3.5. LECCIONES APRENDIDAS

7.3.5.1. Documentación

Se deben documentar las lecciones aprendidas resultantes del proceso de gestión de incidentes, con el objetivo de garantizar la base de conocimiento.

7.3.5.2. Mejora

Se debe realizar como mínimo una (1) vez al año la revisión y mejora de los procesos de gestión de riesgos y gestión de incidentes de seguridad y privacidad de la información apoyados en las lecciones aprendidas que han sido documentadas.

8. MONITOREO Y REVISIÓN DEL MARCO DE REFERENCIA

Cada empresa del **GECC** debe definir los mecanismos para monitoreo y revisión del marco de referencia que considere pertinente, cumpliendo con los requisitos mínimos establecidos en el **MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DEL RIESGO DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA.** Capítulo 7.

9. MEJORA CONTINUA DEL MARCO DE REFERENCIA

Acorde con las falencias detectadas, cada empresa del **GECC** debe definir los planes de acción encaminados a la actualización y mejora del Sistema de Gestión de la Seguridad y Privacidad de la Información (**SGSI**), cumpliendo con los requisitos mínimos establecidos en el **MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DEL RIESGO DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA.** Capítulo 8.

10. IMPLEMENTACIÓN

El marco, las políticas y metodologías establecidas en el presente Manual serán desarrolladas e implementadas acogiendo el principio de gradualidad, ello teniendo en cuenta la naturaleza, normatividad, tipo de negocio y características de cada entidad integrante del **GECC** y basados en el entendimiento de la gestión del riesgo como un proceso, el cual implica sucesivos avances de madurez a lo largo del tiempo.

Cada entidad integrante del **GECC**, según el grado de desarrollo y madurez alcanzado, puede adelantar la implementación de su **SGSI,** estructurando un proyecto dentro de los 4 meses siguientes a la aprobación del presente Manual, el cual deberá presentar a la **GCR** y con su previo visto bueno, será presentado para aprobación de la respectiva Junta Directiva dentro de los 6 meses siguientes a la aprobación del presente Manual, basándose para ello en la metodología de Gestión de Proyectos vigente en el **GECC**, con el fin de permitir la visualización del alcance, tiempo y costos que ello implica.

Dado el grado de madurez alcanzado por Bancoomeva en cuanto al desarrollo de su propio Sistema de Administración de Riesgos, y sin perjuicio de las normas especiales que le son aplicables, además de su obligación de acoger lo pertinente a la gestión de riesgos de conglomerado, el Banco revisará cuales elementos del Sistema Corporativo de Gestión del Riesgo son susceptibles de ser adoptados, por cuanto alinean, complementan o fortalecen su propio Sistema, de lo cual informará a su Junta Directiva, a la Presidencia Ejecutiva del **GECC** y a la Gerencia Corporativa de Riesgo, presentando el respectivo Proyecto de implementación dentro de los 4 meses siguientes a la aprobación de este Manual. De igual manera procederá Coomeva Corredores de Seguros y Coomeva EPS.

11. APROBACION

El presente Manual fue aprobado por el Consejo de Administración, mediante Acuerdo No. 553 del 29 de junio de 2018 según consta en el Acta No. 1132.

Anexo A – Conocimiento y Habilidades para los Roles del SGSI del GECC

CONOCIMIENTOS Y HABILIDADES REQUERIDAS PARA EL GOBIERNO DEL SGSI DEL GECC

No.	ROL	CONOCIMIENTOS Y/O HABILIDADES
1	**Consejo de Administración - Juntas Directivas, Comité Corporativo de Auditoría y Riesgos de COOMEVA, Presidente Ejecutivo del GECC, Presidentes, Gerentes Generales o quienes hagan sus veces, Comité Corporativo de Gestión del Riesgo, Comité Técnico Corporativo de Seguridad y Privacidad de la Información y la Gerencia Corporativa de Riesgo (GCR).**	• Sistemas de Gestión de Seguridad de la Información. • Gestión de incidentes de seguridad de la información. • Gestión de la continuidad de negocio. • Legislación Colombiana en temas de seguridad y privacidad de la información. • Haber asistido a charlas relacionadas con seguridad y privacidad de la Información. • Políticas, procedimientos y organización de la seguridad y privacidad de la información (SGSI). • Medición de indicadores del SGSI.
2	**Jefatura Corporativa de Seguridad de la Información**	• Formación en Sistemas de Gestión de Seguridad de la Información. • Gestión de Riesgos. • Análisis de Vulnerabilidades y Ethical Hacking. • Seguridad en Redes, Bases de datos, Aplicaciones y Sistemas Operativos. • Formación Sistemas de Gestión de Continuidad de Negocio. • Criptografía. • Programación Segura. • Seguridad de Base de Datos. • Norma ICONTEC 31000 y 31010. • Norma ICONTEC 27001, 27002, 27004, 27005 y 27035. • Norma ICONTEC 22301. • Tecnologías de seguridad: firewalls, IDS/IPS, cifrado, antivirus, sistemas biométricos. • Legislación Colombiana relacionada con seguridad y privacidad de la información. • Estrategias de seguridad de la información. • Planeación y/o desarrollo de auditorías de seguridad de la información.

CONOCIMIENTOS Y HABILIDADES REQUERIDAS PARA EL GOBIERNO DEL SGSI DEL GECC

No.	ROL	CONOCIMIENTOS Y/O HABILIDADES
3	**Auditoria Corporativa**	• Conocimiento básico en Sistemas de Gestión de la Seguridad de la Información. • Experiencia en la planeación y/o desarrollo de auditorías de sistemas y/o seguridad de la información. • Conocimientos en seguridad informática. • Conocimiento básico de la Legislación Colombiana en temas de seguridad y privacidad de la información. • Haber asistido a charlas relacionadas con seguridad y privacidad de la información. • Conocimientos de las políticas, procedimientos y organización de la seguridad y privacidad de la información (SGSI). • Conocimiento en gestión de incidentes de seguridad de información. • Gestión de vulnerabilidades a la plataforma tecnológica. • Auditoría a Sistemas de Gestión de la Seguridad de la Información.
4	**Áreas de Responsabilidad de Dirección, Administración, Operación y Control y Áreas o Líderes Responsables de la Implementación del SGSI.**	• Conocimientos de Sistemas de Gestión de Seguridad de la Información. • Conocimiento básico de la Legislación Colombiana en temas de seguridad y privacidad de la información. • Haber asistido a charlas relacionadas con seguridad y privacidad de la Información. • Conocimientos de las políticas, procedimientos y organización de la seguridad y privacidad de la información (SGSI). • Medición de indicadores del SGSI. • Norma ICONTEC 31000 y 31010. • Norma ICONTEC 27001, 27002, 27004, 27005 y 27035. • Norma ICONTEC 22301.
5	**Líderes de Proceso**	• Conocimientos básicos de Sistemas de Gestión de Seguridad de la Información. • Conocimiento básico de la Legislación Colombiana en temas de seguridad y privacidad de la información. • Haber asistido a charlas relacionadas con seguridad y privacidad de la Información. • Conocimientos de las políticas, procedimientos y organización de la seguridad y privacidad de la información (SGSI).

CONOCIMIENTOS Y HABILIDADES REQUERIDAS PARA EL GOBIERNO DEL SGSI DEL GECC

No.	ROL	CONOCIMIENTOS Y/O HABILIDADES
6	**Propietarios de la Información**	• Conocimientos básicos de Sistemas de Gestión de Seguridad de la Información. • Conocimientos del dominio “Gestión de activos” (Anexo A de la norma ISO 27001) relacionado con la clasificación de información y sus responsabilidades. • Conocimiento básico de la Legislación Colombiana en cuanto a seguridad y privacidad de la información. • Haber asistido a charlas relacionadas con seguridad y privacidad de la Información. • Conocimientos de las políticas, procedimientos y organización de la seguridad y privacidad de la información (SGSI).
7	**Áreas de Gestión Humana del GECC**	• Conocimientos básicos de Sistemas de Gestión de Seguridad de la Información. • Conocimientos del dominio “Seguridad de los Recursos Humanos” (Anexo A de la norma ISO 27001). • Conocimiento básico de la Legislación Colombiana en cuanto a seguridad y privacidad de la información. • Haber asistido a charlas relacionadas con seguridad y privacidad de la Información. • Conocimientos de las políticas, procedimientos y organización de la seguridad y privacidad de la información (SGSI).
8	**Áreas Jurídicas del GECC**	• Conocimientos básicos en Sistemas de Gestión de la Seguridad de la Información. • Conocimiento básico de la Legislación Colombiana en cuanto a seguridad y privacidad de la información. • Conocimientos en derecho informático. • Haber asistido a charlas relacionadas con seguridad y privacidad de la Información. • Conocimientos de las políticas, procedimientos y organización de la seguridad y privacidad de la información (SGSI) en la empresa. • Conocimientos de los controles del dominio “Cumplimiento” del Anexo A de la norma ISO 27001 relacionado con el cumplimiento de los requisitos legales y contractuales.
9	**Áreas de Seguridad Física del GECC**	• Conocimientos básicos en Sistemas de Gestión de la Seguridad de la Información. • Conocimientos de Continuidad de Negocio. • Conocimientos en Seguridad y Privacidad de la Información. • Conocimientos de los controles del dominio “Seguridad Física y del Entorno” del Anexo A de la norma ISO 27001 relacionado con seguridad física. • Conocimiento básico de la Legislación Colombiana en cuanto a seguridad y privacidad de la información. • Haber asistido a charlas relacionadas con seguridad y privacidad de la Información. • Conocimientos de las políticas, procedimientos y organización

CONOCIMIENTOS Y HABILIDADES REQUERIDAS PARA EL GOBIERNO DEL SGSI DEL GECC

No.	ROL	CONOCIMIENTOS Y/O HABILIDADES
10	**Áreas de Compras y Gestión de Proveedores del GECC**	de la seguridad y privacidad de la información (SGSI). • Conocimientos básicos en Sistemas de Gestión de la Seguridad de la Información. • Conocimientos de Continuidad de Negocio. • Conocimientos en Seguridad y Privacidad de la Información. • Conocimientos de los controles del dominio "Gestión de proveedores" del Anexo A de la norma ISO 27001. • Conocimiento básico de la Legislación Colombiana en cuanto a seguridad y privacidad de la información. • Haber asistido a charlas relacionadas con seguridad y privacidad de la Información. • Conocimientos de las políticas, procedimientos y organización de la seguridad y privacidad de la información (SGSI).
11	**Todos los colaboradores**	• Conocimientos básicos en Sistemas de Gestión de la Seguridad de la Información. • Conocimiento básico de la Legislación Colombiana en cuanto a seguridad y privacidad de la información. • Haber asistido a charlas relacionadas con seguridad y privacidad de la Información. • Conocimientos de las políticas, procedimientos y organización de la seguridad y privacidad de la información (SGSI) en la empresa.