MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA

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, por la Superintendencia Financiera de Colombia, por la Superintendencia Nacional de Salud, por 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 DE LA INFORMACION 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**.**

1.OBJETIVO

Definir el marco de referencia, instrumentos y metodologías generales para la implementación y funcionamiento del **SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI)** para Coomeva, sus unidades de negocio y las empresas que conforman el Grupo Empresarial Cooperativo Coomeva **(GECC)** y el Conglomerado en su conjunto, con el fin de identificar, analizar, monitorear, medir y controlar 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.

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**:

3.1. **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.

3.2. **Activo Primario:** Es todo activo que corresponde a actividades, procesos del negocio e información (e.j: datos e información impresa).

3.3. **Activo Secundario:** Es todo activo de los cuales dependen los activos primarios (e.j: software, instalaciones, etc.).

3.4. **Amenaza**: Causa potencial de un incidente no deseado que implica un daño.

3.5. **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.

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

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

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

3.9. **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.

3.10. **Dato Personal:** Se refiere a toda aquella información asociada a una persona y que permite su identificación. 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.

3.11. **Directriz**: Especificación que aclara lo que debe hacerse y el cómo hacerlo, para alcanzar los objetivos definidos en las normas y políticas.

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

3.13. **Equipo de respuesta a incidentes de seguridad de la información (ISIRT – Information Security Incident Response Team):** Equipo conformado por miembros confiables de la organización, que cuentan con las habilidades y competencias para tratar los incidentes de seguridad de la información, durante el ciclo de vida de éstos.

3.14. **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.

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

3.16. **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.

3.17. **GECC**: Grupo Empresarial Cooperativo Coomeva.

3.18. **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**.

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

3.20. **Incidente de Seguridad:** 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 el Incidente de seguridad de la información: 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.

3.21. 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.

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

3.23. Investigación forense de seguridad de la información (Information Security Forensics): Aplicación de técnicas de investigación y análisis para recolectar, registrar y analizar información de incidentes de seguridad de la información.

3.24. 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.

3.25. ISO/IEC 27005:2011: 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.

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

3.27. 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.

3.28. Manual Corporativo del Sistema de Gestión de la Seguridad 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.

3.29. 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.

3.30. **Terceros**: Personas que no tienen un vínculo laboral directo con las empresas que componen el Grupo Empresarial Cooperativo Coomeva **GECC** (Ejemplo: asociados, proveedores, visitantes, clientes, usuarios, etc.).

3.31. **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 DE LA INFORMACIÓN

4.1. DEFINICIÓN DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Unidad Corporativa de Gestión del Riesgo (**en adelante UCGR**) adopta las buenas prácticas de la Norma **NTC-ISO-IEC 27001:2013** para soportar los procesos de establecimiento, implementación, mantenimiento y mejora continua del **SGSI** del **GECC**; tomando como referencia las necesidades y objetivos de la organización, los requisitos de seguridad 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 Riesgo del **GECC** con el fin de aprovechar la madurez de este último y así facilitar el proceso de implementación al interior del negocio.

4.2. POLÍTICAS PARA LA GESTIÓN DE SEGURIDAD 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 General de Seguridad de la Información Corporativa

La política de seguridad de la información tiene como objetivo principal que *"Todos los colaboradores del **GECC** velen porque la información de los asociados, colaboradores, clientes y/o afiliados durante su almacenamiento, tránsito y procesamiento, mantengan siempre los criterios de confidencialidad, integridad y disponibilidad"*.

De manera detallada las políticas de seguridad de la información corporativa se definen y establecen en el documento **XX-XX-XXX Políticas y Responsabilidades de Seguridad de la Información del Grupo Empresarial Cooperativo Coomeva (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,** 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 5.5 COMUNICACIÓN Y CONSULTA DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN.

4.4. MECANISMOS DE CAPACITACIÓN

Son los establecidos en el **MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DEL RIESGO DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA**, Capítulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO. Mecanismos de capacitación.

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

La Estructura de Gobierno del **SGSI** en el **GECC** es la misma que se establece en el **MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DEL RIESGO**, 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 mencionado en el párrafo anterior, realizando los ajustes necesarios según las normas empresariales o sectoriales y de organismos de vigilancia y control que les sean aplicables y cumplirán como mínimo las siguientes funciones:

4.5.1. Consejo de Administración - Juntas Directivas

a) Aprobar las políticas de seguridad de la información y aquellas para la protección de datos personales corporativas y de las empresas del GECC, respectivamente.
b) Garantizar la alineación entre la planeación estratégica del negocio (objetivos estratégicos) y el programa de seguridad de la información.
c) Aprobar el nivel de riesgo aceptable para el negocio, el apetito de riesgo.
d) Supervisar el cumplimiento de las políticas y el cumplimiento de las exigencias regulatorias.
e) Supervisar la utilización adecuada de los recursos de seguridad y las políticas definidas para garantizar la integración de la seguridad 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 para garantizar que los procesos operen de la forma planeada.

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

j) Apoyar el cumplimiento de los requerimientos legales y regulatorios relacionados con la seguridad de la información, la protección de datos personales y el control interno.

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

l) Definir el régimen de sanciones por incumplimiento de las políticas de seguridad corporativas.

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 SISTEMA DE GESTIÓN DEL RIESGO,** 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 de la información y protección de datos personales.

b) Difundir las políticas generales y supervisar su aplicación.

c) Aprobar los procedimientos corporativos para la protección de datos personales en el **GECC**.

d) Aprobar las políticas específicas (detalladas) y las estrategias de seguridad de la información y protección de datos personales.

e) Formalizar procesos para integrar la seguridad de la información y la protección de datos personales en los objetivos del negocio.

f) Verificar que los roles y responsabilidades de los cargos incluyan la gestión de riesgos en todas sus actividades, al igual que la protección de datos personales.

g) Apoyar las iniciativas de sensibilización, capacitación y generación de cultura en seguridad de la información y protección de datos personales para todos los colaboradores del **GECC**.

h) Supervisar y garantizar el cumplimiento de las normas legales y regulaciones vigentes asociadas a la seguridad de la información y la protección de datos personales.

i) Exigir el desarrollo de casos de negocio que justifiquen las iniciativas e inversiones en seguridad de la información y protección de datos personales.

j) Seguimiento de indicadores que midan la eficiencia de la estrategia de seguridad de la información y protección de datos personales.

k) Asignar recursos adecuados y delegar autoridad para implementar y mantener el plan de seguridad de la información y el programa integral de gestión de datos personales definido.

l) Apoyar el mejoramiento continuo de la seguridad de la información y la protección de datos personales.

4.5.4. Comité Corporativo de Gestión del Riesgo

La composición, funciones y demás aspectos relacionados con este Comité, son los establecidos en el **MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DEL RIESGO,** Capitulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO.

4.5.5. Unidad Corporativa de Gestión del Riesgo (UCGR)

La composición, funciones y demás aspectos relacionados con la UCGR, son los establecidos en el **MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DEL RIESGO,** Capitulo 5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO.

4.5.6. Jefatura Corporativa de Seguridad de la Información

Tendrá a su cargo las siguientes responsabilidades:

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

b) Definir, socializar y ejecutar el Plan Estratégico de Seguridad 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 de la información y protección de datos personales aplicables al **GECC**.

d) Liderar el desarrollo de los proyectos de seguridad de la información en las empresas del **GECC** que están bajo la supervisión de la Unidad Corporativa de Gestión del Riesgo (UCGR).

e) Proponer a la Unidad Corporativa de Gestión del Riesgo, la política y las funciones generales en materia de seguridad de la información y protección de datos personales para que sean sometidas a aprobación por parte de las instancias correspondientes.

f) Monitorear el cumplimiento de los indicadores establecidos dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

g) Diseñar, definir, implementar y monitorear el plan y actividades de seguridad de la información y protección de datos personales, y supervisar su eficacia.

h) Garantizar la alineación constante de las iniciativas de seguridad de la información y protección de datos personales con los procesos del negocio.

i) Monitorear los procesos de seguridad de la información y protección de datos personales para garantizar que se alcancen los objetivos definidos (evaluación anual).

j) Definir estrategias de capacitación y concientización en seguridad de la información y protección de datos personales, al igual que la medición de la eficiencia y efectividad de las mismas.

k) Monitorear y evaluar de manera periódica los controles de seguridad de la información para mitigar el riesgo a niveles aceptables en las empresas del **GECC** que están bajo la supervisión de la Unidad Corporativa de Gestión del Riesgo (UCGR).

l) Conocer y consolidar las exposiciones, incidencias y el comportamiento de indicadores relativos a la seguridad de la información y protección de datos personales dentro del **GECC**.

m) Definir procesos para la adecuada gestión de riesgos de seguridad de la información y protección de datos personales.

n) Definir procesos para la adecuada gestión de incidentes de seguridad de la información y protección de datos personales.

4.5.7. Comité Técnico Corporativo de Seguridad de la Información

El Comité 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 **UCGR**. Es liderado por el Jefe Corporativo

Seguridad de la Información, con el apoyo de los representantes designados por cada una de las empresas y unidades 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) Examinar y proponer actualizaciones al **Manual Corporativo del Sistema de Gestión de Seguridad 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 de la información y protección de datos personales.

c) Validar y certificar el cumplimiento del Gobierno de Seguridad de la Información en cada una de las empresas del **GECC**.

d) Revisar y apoyar las estrategias de seguridad de la información y protección de datos personales, al igual que su integración con los procesos de negocio.

e) Analizar el riesgo residual y promover prácticas de seguridad de la información y protección de datos personales en cada una de las empresas.

f) Retroalimentar sobre la eficacia de los controles de seguridad de la información y protección de datos personales que apoyan las funciones del negocio.

g) Revisar el avance de los procesos de capacitación y sensibilización en seguridad de la información y protección de datos personales diseñados para el **GECC**.

h) Discutir las problemáticas de seguridad de la información y protección de datos personales que atañen al **GECC** y propender por la solución de las mismas.

i) Socializar el seguimiento, supervisión y monitoreo de los incidentes de seguridad de la información.

j) Realizar seguimiento a los proyectos de seguridad de la información y aquellos que puedan afectar la seguridad de la información que sean ejecutados por el **GECC**, analizar la viabilidad de nuevos proyectos y su alineación con el plan de seguridad de la información definido.

k) Compartir experiencias obtenidas desde cada uno de los sectores en materia de seguridad de la información y protección de datos personales, así como también analizar nuevas disposiciones regulatorias y mejores prácticas.

l) Revisar la exposición al riesgo de manera global del **GECC**, así como la específica de cada sector del **GECC**.

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

4.5.8. Áreas de Gestión del Riesgo de Seguridad de la Información y de Protección de Datos Personales en el GECC.

Empresa	Área	Responsables Directos	Apoyo
Coomeva: • **Servicio al Asociado** • **Educación y Democracia** • **Corporativo** • **Solidaridad y Seguros** • **Recreación**	• Gerencias Unidades GECC • Unidad Corporativa de Gestión del Riesgo	• Gerentes Unidades del GECC • Líderes de los procesos en las unidades del GECC	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Servicios Administrativos	• Gerencia • Dirección TI • Área de riesgo, seguridad de la información o quienes hagan sus veces • Unidad Corporativa de Gestión del Riesgo	• Gerente General • Director Servicios TI • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Financiero: • **Bancoomeva**	• Presidencia Bancoomeva • Vicepresidencia de Riesgo y Gestión • Seguridad de la Información	• Presidente Bancoomeva • Vicepresidente de Riesgo y Gestión • Coordinador nacional de seguridad de la información • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Protección: • **Corredor de Seguros**	• Gerencia Sector Protección • Gerencia General • Área de riesgo, seguridad de la información o quienes hagan sus veces	• Gerente Sector Protección • Gerente General • Líderes de los procesos • Coordinador de riesgo	• Jefe, coordinador y analista corporativo seguridad de la información
Conecta Financiera-Salud	• Gerencia • Área de riesgo, seguridad de la información o quienes hagan sus veces	• Gerente • Líderes de los procesos • Coordinador de riesgos	• Jefe, coordinador y analista corporativo seguridad de la información

	• Unidad Corporativa de Gestión del Riesgo		
Coomeva Sector Salud: • **EPS** • **Medicina Prepagada** • **Sinergia Global en Salud**	• Gerencia General Sector Salud • Gerencia General EPS • Gerencia General MP • Gerencia General Sinergia • Área de riesgo, seguridad de la información o quienes hagan sus veces	• Gerente General Sector Salud • Gerente General EPS • Gerente General MP • Gerente General Sinergia • Líderes de los procesos • Gerente Nacional de Riesgo	• Jefe, coordinador y analista corporativo seguridad de la información
Hospital en Casa	• Gerencia General • Área de riesgo, seguridad de la información o quienes hagan sus veces	• Gerente General • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Clínica Farallones	• Gerencia General • Área de riesgo, seguridad de la información o quienes hagan sus veces	• Gerente General • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Clínica Palma Real	• Gerencia General • Área de riesgo, seguridad de la información o quienes hagan sus veces	• Gerente General • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Fundación	• Gerencia Nacional • Área de riesgo, seguridad de la información o quienes hagan sus veces • Unidad Corporativa de Gestión del Riesgo	• Gerente Nacional • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información
Coomeva Sector Recreación y Turismo: • **Turismo Coomeva** • **Club Los Andes**	• Gerencia Sector • Gerencia Turismo • Gerencia Club Andes • Área de riesgo, seguridad de la	• Gerente Sector • Gerente Turismo • Gerente Club Andes • Líderes de los procesos	• Jefe, coordinador y analista corporativo seguridad de la información

	• información o quienes hagan sus veces • Unidad Corporativa de Gestión del Riesgo		
Fondo de Empleados Fecoomeva	• Gerencia General • Área de riesgo, seguridad de la información o quienes hagan sus veces • Unidad Corporativa de Gestión del Riesgo	• Gerente General • Líderes de los procesos • Asistente de gestión de riesgo	• Jefe, coordinador y analista corporativo seguridad de la información

Tabla 1. Áreas Responsables de Seguridad de la Información y Protección de Datos Personales

4.5.9. Áreas Responsables de la Gestión y Control del Riesgo en el GECC

Los dominios de seguridad de la información que se detallan a continuación son los definidos en la norma **ISO/IEC 27002:2013**:

Dominio	Objetivo	Áreas Responsables
Seguridad de los Recursos Humanos	La necesidad de educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.	• Gerencia Corporativa de Gestión Humana • Jefatura y/o Coordinación de Gestión Humana en cada unidad o empresa del GECC
Gestión de Activos de Información	Que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la gestión de riesgos.	• Propietarios de la Información en cada unidad o empresa del GECC
Control de Acceso	Controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.	• Dirección de Servicios de TI CSA
Criptografía	Uso de sistemas y técnicas criptográficas para la protección de la información con base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.	• Dirección de Servicios de TI CSA • Responsable de Tecnología en cada unidad o empresa del GECC
Seguridad Física y del Entorno	Minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.	• Dirección de Servicios de TI CSA • Jefatura Nacional de Seguridad CSA
Seguridad en las Operaciones	Establecer controles que aseguren la operación de los procesos apoyados en la infraestructura	• Dirección de Servicios de TI CSA

	tecnológica.	
Seguridad de las Comunicaciones	Asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.	• Dirección de Servicios de TI CSA
Seguridad en la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.	• Dirección de Servicios de TI CSA • Responsable de Tecnología en cada unidad o empresa del GECC
Relación con los proveedores	Implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados a terceros.	• Dirección de negociación y compras CSA
Gestión de los Incidentes de Seguridad de la Información	Garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.	• Dirección de Servicios de TI CSA • Jefatura y/o Coordinación Seguridad de la información de las empresas. • Responsable de Tecnología en cada unidad o empresa del GECC
Planificación de la Continuidad del Negocio	Preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad	• Dirección de Servicios de TI CSA • Gestor de Continuidad de Negocio UCGR • Responsable de continuidad de negocio en cada unidad o empresa del GECC
Cumplimiento	Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.	• Áreas legales de las unidades o empresas del GECC • Unidad Corporativa de Gestión del Riesgo (UCGR)

Tabla 2. Dominios de Seguridad de la Información y Responsables

La UCGR ejerce las funciones de dirección y coordinación técnica del Gobierno del Riesgo de Seguridad de la Información y de Protección de Datos Personales en el GECC y por lo tanto es la responsable de impartir directrices y de impulsar, supervisar, monitorear y asesorar la adopción y aplicación de políticas, de metodologías, el desarrollo de los planes, la ejecución de controles y actividades y de evaluar la gestión y nivel de madurez de la seguridad de la información en el GECC.

4.5.10. 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 de aseguramiento objetivo y asesoría a la estrategia de seguridad de la Información y protección de datos personales a nivel Corporativo.

a) Evaluar y reportar el grado de alineación de la estrategia de seguridad de la información y protección de datos personales con los objetivos del **GECC**.
b) Evaluar y reportar acerca de los riesgos corporativos de seguridad de la información y protección de datos personales 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 corporativo de seguridad de la información y protección de datos personales, y el uso adecuado de los recursos.
d) Evaluar y reportar sobre la eficiencia de los procesos de aseguramiento 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 de la información y protección de datos personales 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.

4.5.11. 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.

4.5.12. 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 de SGSI deben:

a) Comunicar mensualmente (o antes según sea requerido) 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 de la información y la protección de datos personales.

b) Asesorar en materia de riesgos de seguridad de la información y protección de datos personales a los líderes de procesos para alcanzar una adecuada implementación de la presente metodología.

c) Monitorear frecuentemente el debido cumplimiento de la metodología al interior de las unidades y empresas que componen el **GECC**.

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

4.5.13. Líderes de Proceso

Los Líderes del proceso deben:

a) Realizar los procesos de identificación, medición y control de riesgos de seguridad de la información y protección de datos personales cada vez que se cree o se realice un cambio en procedimientos, instructivos, productos o servicios.

b) 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.

c) Reportar mensualmente a la Unidad Corporativa de Gestión del Riesgo o a quienes hagan sus veces en las empresas y unidades de negocio del **GECC**, los incidentes de seguridad de la información y protección de datos personales detectados.

d) Realizar divulgación de los mapas de riesgo y los controles asociados a su proceso, a todos los colaboradores que participan del proceso.

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

4.5.14. Propietarios de la Información

Los propietarios de la información deben:

a) Clasificar la información de acuerdo al grado de criticidad y sensibilidad de la misma, y definir el responsable de tratamiento.

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.

4.5.15. Gestión Humana

Gestión humana será responsable de:

a) Notificar a todo el personal que ingresa, de sus obligaciones respecto del cumplimiento de la política de seguridad de la información y protección de datos personales, y de todas las normas, procedimientos y prácticas que de ella se deriven.

b) Divulgar la presente política a todo el personal, de los cambios que en ella se produzcan, de la implementación de los compromisos de confidencialidad y de las tareas de capacitación continua que sean necesarias.

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

- La inclusión de las responsabilidades de gestión del riesgo en los manuales de funciones y responsabilidades, 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 fortalecimiento del talento y la cultura y definir y realizar seguimiento al Plan de Capacitación Corporativo sobre el Sistema Corporativo de Gestión del Riesgo.

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

4.5.16. Unidad de Tecnología Informática (CSA/UTI)

La Unidad de Tecnología Informática será la responsable 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.

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

4.5.17. Áreas Jurídicas del GECC

Las áreas jurídicas son las encargadas de:

a) Verificar el cumplimiento de la presente política en la gestión de todos los contratos, acuerdos de servicio u otra documentación del **GECC** con sus empleados y con terceros.

b) Realizar asesorías en materia legal focalizadas a la seguridad de la información y protección de datos personales, de ser requeridas.

4.5.18. 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 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.

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 de la información y protección de datos personales, 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 confidencial que se genere hacia dispositivos de almacenamiento externo o hacia listados impresos.

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

h) Usar solo software debidamente licenciado y autorizado por la organización.

i) Seguir todos los procedimientos y políticas definidas y 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 incidente de seguridad de la información y protección de datos personales identificado.

5. PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACION Y PROTECCIÓN DE DATOS PERSONALES

El proceso de Gestion del Riesgo de Seguridad de la Informacion y Protección de Datos Personales definido por la **UCGR** se soporta bajo las prácticas de la norma **NTC-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 27005:2011 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.

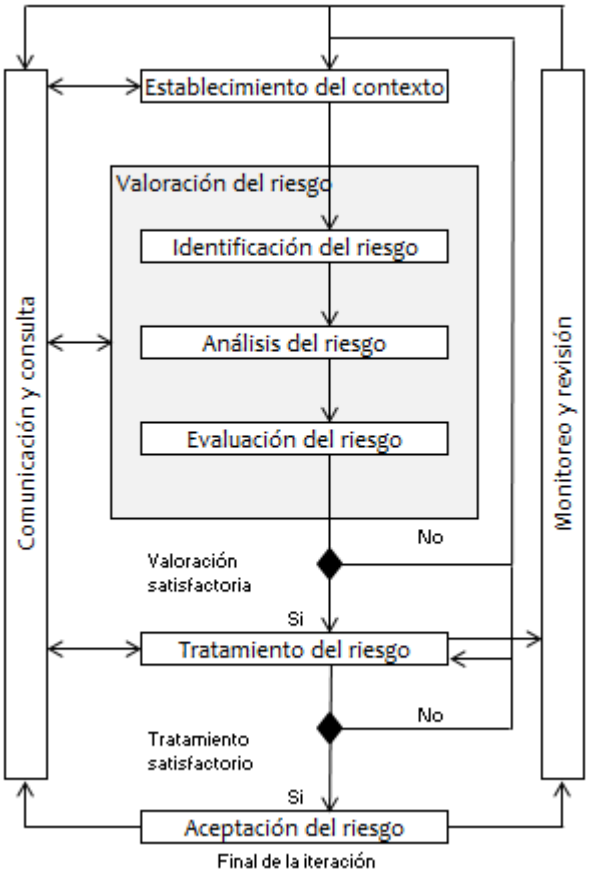


Figura 1. Proceso de Gestión del Riesgo de Seguridad de la Información ISO/IEC 27005:2011

5.1 ESTABLECIMIENTO DEL CONTEXTO

En esta etapa se desarrolla un entendimiento de los procesos del negocio “Cadena de Valor” con el fin de identificar los activos de información que harán parte de la Gestión de Riesgos de la Seguridad de la Información y Protección de Datos Personales.

Se debe tener presente una etapa inicial de recolección de información, para ello se debe contemplar:

- Preparación de entrevistas:
  - Cuestionarios
  - Ubicación de los entrevistados
  - Los objetivos del ejercicio a realizar

- Realización de entrevistas
  - Definición de las funciones
  - Identificación de herramientas que dispone el entrevistado para sus funciones
  - Identificación de los subprocesos pertenecientes al área o proceso analizado

5.1.2 Definición del Alcance

En esta etapa se seleccionan los procesos que a criterio del cliente son considerados como críticos dentro de su cadena de valor; y sobre los cuales se desarrollará la metodología de análisis de riesgo.

5.1.3 Equipo de Implementación

Se deben definir los recursos requeridos para la implementación de la presente metodología:

- Grupos de líderes de procesos con quienes se obtendrá la información para llevar a cabo la gestión.
- Participantes de la implementación: Usuarios y personas que realizarán la implementación.
- Comité de seguimiento, encargado de hacer seguimiento al plan de trabajo de la Gestión del Riesgo de la Seguridad de la Información y Protección de Datos Personales establecido con cada una de las empresas o unidades del **GECC**.

5.1.4 Definición de Criterios

Los criterios básicos establecidos para la gestión del riesgo en la seguridad de la información y protección de datos personales son:

- Valoración Activo de Información
- Probabilidad de Ocurrencia
- Impacto
- Zonas de Severidad

Estos criterios son de tipo cualitativo con una escala de valor del Uno (1) al Cinco (5) y serán detallados en las actividades de valoración del riesgo.

5.1.5 Comunicación de la Implementación de la Gestión

Es importante informar y sensibilizar a las personas impactadas en el proceso de implementación acerca de la finalidad y necesidad de su participación, de esta manera lograr así una disponibilidad del personal involucrado y disponibilidad de los medios necesarios para lograr el éxito de los objetivos propuestos.

5.2 VALORACIÓN DEL RIESGO

En esta etapa se desarrollan las siguientes actividades:

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

5.2.2 Identificación del riesgo

5.2.2.1 Identificación de Activos de Información

Para esta actividad se debe llevar a cabo la clasificación de activos de información según su importancia en la organización y su nivel de exposición al riesgo, y registrar la información en el formato **GC-FT-XXX Matriz de Riesgos SI**. Previo a esta actividad, se debe establecer que es y que no es un activo de información, para ello es importante tener presente la siguiente definición: "*Algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger*".

La clasificación de activos de información deberá tener estructurados los siguientes bloques de datos:

- **Id Activo**: Consecutivo de identificación del activo dentro del inventario.
- **Tipo de Activo:** Se tipifica el activo como primario o secundario.
- **Nombre Activo**: Nombre del activo que se desea proteger.
- **Descripción**: Entender el valor y el rol del activo de información para la organización y para el proceso.
- **Dependencia Activo Primario:** En este campo se relacionan los activos primarios que se apoyan en el activo secundario.
- **Categoría del Activo**: Se categoriza el activo con base a la metodología de Magerit V3.0, la cual sirve de criterio para la identificación de amenazas potenciales y vulnerabilidades apropiadas a la naturaleza del activo.
    - Datos
    - Información Impresa
    - Aplicaciones / Software
    - Equipos Informáticos / Hardware
    - Redes de Comunicaciones
    - Medios de Almacenamiento
    - Servicios
    - Recurso Humano
    - Instalaciones
    - Equipamiento Auxiliar
- **Propietario**: Cargo o equipo de trabajo que tiene la responsabilidad de controlar, desarrollar, mantener, usar y asegurar el activo.
- **Custodio**: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar los componentes tecnológicos donde se encuentra la información.
- **Usuarios**: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.
- **Ubicación Física**: Sitio físico donde se encuentra almacenado el activo.

- **Ubicación Digital**: Servidor o sitio lógico donde se encuentra almacenado el activo. Identificar la ruta específica de ubicación.

- **Clasificación de la Información**: (De acuerdo a las características de confidencialidad establecidas en el documento **GC-DC-489_Política de Seguridad de la Información GECC**: Confidencial, Uso Interno, Pública).

- **Proceso/procedimientos**: Se listan los procesos/procedimientos del negocio, posteriormente se relacionan los activos que impactan dichos procesos.

- **Criticidad Activo**: Se calcula validando el impacto que se puede generar al verse afectado el activo en cualquiera de las tres dimensiones de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

5.2.2.2 Valoración de la Criticidad de los Activos de Información

Para lograr identificar una protección apropiada en los activos de información, es necesario medir su valor potencial en términos de la importancia sobre las diversas gestiones y procesos ejecutados por las empresas del **GECC**.

Para ello se deben considerar los criterios de valoración del activo, de esta manera se define una escala de valoración de impacto la cual estaría relacionada con el daño que causaría a la organización el que un activo de información resulte afectado negativamente en cuanto a su confidencialidad, integridad y disponibilidad. El valor final del impacto en el activo de información, corresponde al mayor valor de las tres dimensiones evaluadas.

Confidencialidad		
Propiedad que determina la condición de que la información no sea revelada a individuos, entidades o procesos no autorizados.		
Criterio	**Descripción**	**Explicación**
I	**Insignificante**	La información es PUBLICA y no se tiene ningún impacto sobre el resultado del proceso en caso de ser accedido por personas no autorizadas
ME	**Menor**	La información a pesar de ser PUBLICA ya ha sido clasificada y nutrida por la organización y de ser accedida por personas no autorizadas podría afectar el resultado o poner en riesgo la empresa.
MO	**Moderado**	La información es de USO INTERNO pero de ser accedida por personas no autorizadas no afectaría en mayor grado el resultado o pondría en riesgo la empresa.
MA	**Mayor**	La información es de USO INTERNO y de ser accedida por personas no autorizadas podría afectar el resultado del proceso o poner en riesgo la empresa
C	**Catastrófico**	La información es CONFIDENCIAL y en caso de ser accedida por personas no autorizadas el impacto final sobre el proceso o resultado de la empresa sería muy grave

Tabla 3. Criterios de Valoración Activos de Información-Confidencialidad

Integridad		
Propiedad de salvaguardar la exactitud y estado completo de los activos.		
Criterio	**Descripción**	**Explicación**
I	**Insignificante**	La información no es crítica, y no tiene repercusión en el proceso. Si presentara errores la pérdida que origina es muy pequeña y su reconstrucción consiste en la repetición de un proceso sencillo.
ME	**Menor**	La información no es crítica pero es básica para algunas decisiones menores del proceso. La ocurrencia de un fraude o errores sobre la misma podría ocasionar pérdidas.
MO	**Moderado**	La información es crítica y sobre ella se basan algunas decisiones del proceso. La ocurrencia de un fraude o errores sobre la misma ocasionará pérdidas.
MA	**Mayor**	La información es crítica y es aquella en la cual se basan decisiones importantes del proceso. La ocurrencia de un fraude o errores sobre la misma ocasionará pérdidas importantes o severas, por lo cual, la información necesita un nivel razonable de protección contra error y fraude.

C	**Catastrófico**	La información es base para la toma de decisiones estratégicas o es fundamental para la protección de los individuos de la organización. La ocurrencia de un fraude o errores sobre la misma ocasionará pérdidas graves o catastróficas, por lo cual, la información deberá estar libre de error.

Tabla 4. Criterios de Valoración Activos de Información-Integridad

Disponibilidad		
Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.		
Criterio	**Descripción**	**Explicación**
I	**Insignificante**	El tiempo para recuperar la información no es crítico, puede esperar una semana o más sin tener consecuencia sobre el resultado del proceso.
ME	**Menor**	El tiempo máximo para recuperar la información y volver a iniciar el procesamiento debe ser menor a una semana.
MO	**Moderado**	El tiempo máximo para recuperar la información y volver a iniciar el procesamiento debe ser menor a dos días.
MA	**Mayor**	El tiempo máximo para recuperar la información y volver a iniciar el procesamiento es menor a un día.
C	**Catastrófico**	El tiempo máximo para recuperar la información y volver a iniciar el procesamiento es menor a 4 horas.

Tabla 5. Criterios de Valoración Activos de Información-Disponibilidad

Una vez realizada la valoración de la criticidad del activo, se tomarán aquellos activos secundarios con criticidad **Catastrófica** y **Mayor** para continuar con el proceso de gestión del riesgo en la seguridad de la información.

5.2.2.3 Identificación de Amenazas en los Activos de Información

Una amenaza es considerada una causa potencial de un incidente en la organización, generando así pérdidas significativas sobre los activos de información.

En razón de lo anterior, nace la necesidad de identificar las amenazas que podrían impactar los activos de información frente a su confidencialidad, integridad y disponibilidad y de esta manera asociarlas.

La metodología para gestión de riesgos MAGERIT versión 3.0 proporciona un listado de amenazas las cuales se encuentran documentadas en el **Anexo A** del presente manual. Sin embargo, es pertinente continuar en la constante retroalimentación de este listado, identificando amenazas obtenidas por los propietarios de los activos, usuarios, revisiones de incidentes, etc.

5.2.2.4 Identificación de las Vulnerabilidades en los Activos de Información

Se debe tener presente que los activos secundarios tienen vulnerabilidades que son explotadas por amenazas con el objetivo de poner en peligro los activos primarios, es por ello que deben ser identificadas. En el **Anexo B** del presente manual se proporciona un listado de vulnerabilidades los cuales se toman como referencia.

Para alcanzar un mejor resultado en esta asociación de amenazas y vulnerabilidades, se debe contar con la participación del propietario y conocedor de los activos o grupos de activos, quien puede comprender e imaginar con objetividad acciones potenciales de las amenazas.

5.2.3 Análisis del Riesgo

5.2.3.1 Identificación y Evaluación de los Controles Existentes

A partir del listado de activos, amenazas y vulnerabilidades se debe realizar la identificación y documentación de los controles existentes que mitiguen las vulnerabilidades identificadas y de esta forma reducir el nivel de riesgo. Para esta actividad es posible tomar como base los controles contenidos en la norma ISO/IEC 27002:2013.

De igual forma, se contará con los controles sugeridos por anteriores auditorías realizadas, métodos implementados y ejecutados como autocontrol al interior de las áreas, controles tecnológicos (software/hardware), políticas de la organización, procedimientos, capacitaciones, reglamentaciones, etc.. Para ello se requiere recopilar la mayor información asociada que sea provista por expertos y/o líderes de procesos.

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**, o aquellos que lo modifiquen o sustituyan.

5.2.3.2 Estimación del Riesgo

Una vez identificados y evaluados los controles existentes se calcula el nivel de riesgo aplicando los criterios de Probabilidad de Ocurrencia y de Impacto.

Los criterios definidos para valorar la frecuencia potencial de ocurrencia de una amenaza sobre un activo de información son:

Probabilidad		
Valor	**Probabilidad Cualitativa**	**Descripción**
5	Muy Alta	1 vez al día
4	Alta	1 vez cada 2 semanas
3	Media	1 vez cada 2 meses
2	Baja	1 vez cada 6 meses
1	Muy Baja	1 vez al año

Tabla 6. Criterios Probabilidad de Ocurrencia

El impacto es la magnitud del daño que podría ser causado cuando una amenaza explota una vulnerabilidad del activo o control. El impacto se mide cualitativamente a través de cuatro categorías definidas en el documento **GC-DC-487 Manual Corporativo del Sistema de Gestión de Riesgo – Numeral 5.2.30 (**Financieras, Operación/Servicio, Reputación/Imagen y Balance Social (opcional)).

ESCALA	Descripción si el riesgo se materializa	1 Financieras	2 Operación/Servicio
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, caida del servicio siendo muy difícil su recuperación. Perdida permanente o masiva de clientes, fallas de los principales proveedores.
4 MAYOR	Las consecuencias a pesar de ser severas, podrían ser gestionadas hasta cierto punto.	Pérdida Mayor o igual al 70% 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.
3 MODERADO	Las consecuencias no serían severas y, podrían ser gestionadas.	Pérdida Mayor o igual al 50% 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.
2 MENOR	Las consecuencias serían consideradas relativamente poco importantes	Pérdida Mayor o igual al 10% del margen del patrimonio mínimo	Interrupción de las operaciones de la organización por algunas horas.(menos de 12 horas) Reducción menor en estandares de calidad.
1 INSIGNIFICANTE	No hay consecuencias detectables	Pérdida Mayor o igual al 5% del margen del patrimonio mínimo	No hay interrupción de las operaciones de la organización

ESCALA	Descripción si el riesgo se materializa	3 Reputación/Imagen	4 BALANCE SOCIAL
5 CATASTRÓFICO	A la organización le sería casi imposible recuperarse o los daños serian severos	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 y corrupción o graves Incumplimientos. Maximas penalidades financieras. Graves violaciones de los derechos de los grupos de interés, o ambientales con pérdida de talento, daños, o lesiones personales severas e irreparables o pérdida de vidas. Tensas relaciones con Grupos de Interes.
4 MAYOR	Las consecuencias a pesar de ser severas, podrían ser gestionadas hasta cierto punto.	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 . Debilidad o ausencia de polítticas de RSE y Gobierno, no hay implementación de buenas prácticas. Poco involucramiento de Grupos de Interes.
3 MODERADO	Las consecuencias no serían severas y, podrían ser gestionadas.	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. Ausencia de planes integrales para implementación y seguimiento de buenas prácticas de Gobierno y RSE.
2 MENOR	Las consecuencias serían consideradas relativamente poco importantes	Afectación moderada de la reputación a nivel Interno o quejas o reacción adversa menor en publicos y medios que no requiere medidas especiales.	Glosa por parte de Entes de control sin sanciones económicas por incumplimiento de normas u obligaciones. No se cuenta con indicadores de gestión de RSE, etica y Gobierno y hay incumplimiento de buenas prácticas-
1 INSIGNIFICANTE	No hay consecuencias detectables	Afectación leve de reputación a nivel Interno o preocupación pública sin efecto duradero. No es de interés público	Escasos planes de acción y poco seguimiento a indicadores de Políticas y Planes de RSE, ética y Gobierno y aún hay incumplimiento de buenas prácticas. Se impone glosa por parte de Control Interno.

Tabla 7. Categorías de Clasificación de Impacto del Riesgo

El resultado del impacto, corresponde a la calificación con mayor escala de las cuatro categorías descritas previamente (insignificante, menor, moderado, mayor, catastrófico).

5.2.4 Evaluación del Riesgo

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

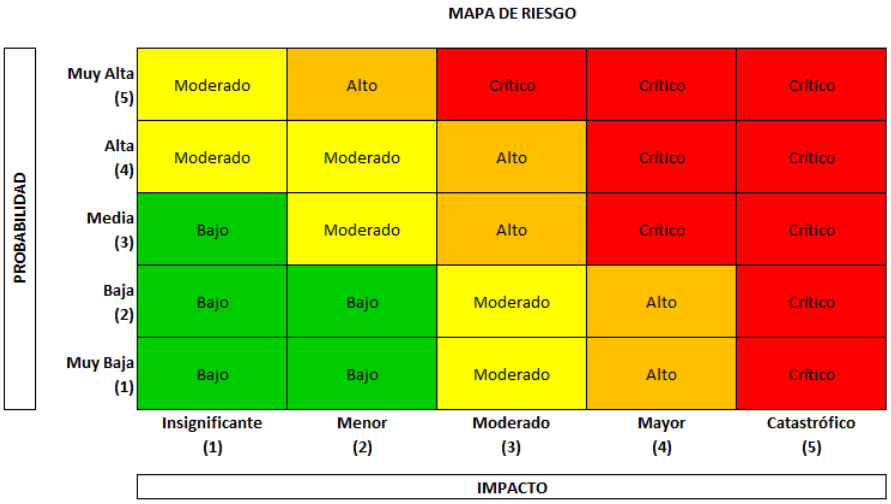


Figura 2. Mapa de Riesgos

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; 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 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 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

En esta fase de la metodología se procede a definir los planes de tratamiento para los riesgos que se encuentran ubicados en las zonas no toleradas para el **GECC**.

5.2.4.1 Zonas de Riesgo No Toleradas

Las zonas de riesgo no toleradas 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**.

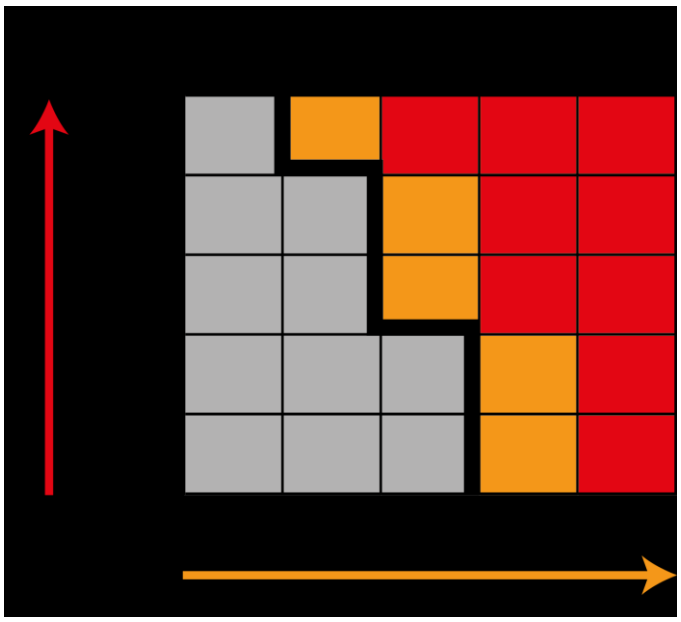


Figura 3. Zonas de Riesgo No Toleradas

5.3 TRATAMIENTO DEL RIESGO

En esta etapa se diseñan las acciones que deberán ser implementadas para que los riesgo 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, Retener, Evitar y Transferir:

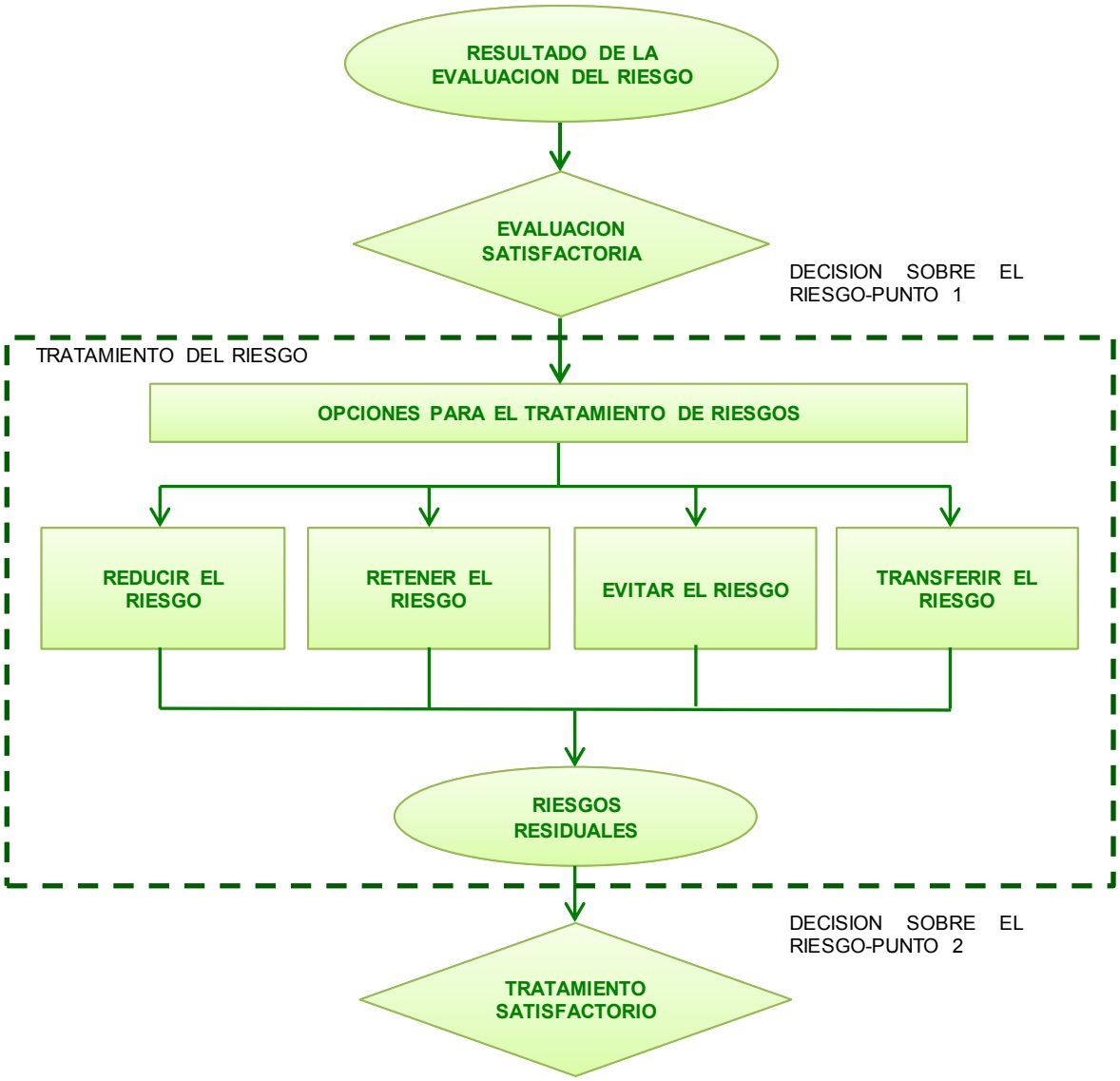


Figura 4. Actividad para el Tratamiento del Riesgo

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.

5.3.1 Opciones para el Tratamiento de los Riesgos

5.3.1.1 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.

En el proceso de selección del tratamiento es importante analizar el valor de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los mismos versus el valor de los activos que se quieren proteger.

La norma ISO/IEC 27005:2011 Gestión de los Riesgos de Seguridad de la Información, recomienda considerar algunas restricciones en la selección e implementación de los controles:

- Restricciones de tiempo
- Restricciones financieras
- Restricciones técnicas
- Restricciones operativas
- Restricciones culturales
- Restricciones éticas
- Percepciones ambientales
- Restricciones legales
- Facilidad de utilización
- Restricciones personales
- Restricciones para la integración de controles nuevos y existentes

5.3.1.2 Retener 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.

5.3.1.3 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.

5.3.1.4 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.

Por otro lado, es importante elaborar el plan, identificando el orden de prioridad en el que los riesgos deben ser tratados de manera individual (basados en la ubicación de los riesgos en el mapa de riesgos y el análisis de costo-beneficio en los controles diseñados).

5.3.2 Estimación del Riesgo Residual

A partir de la evaluación de los controles propuestos en los planes de tratamiento, y una vez calculados el porcentaje de mitigación de los controles; el nivel del riesgo residual será el resultado del desplazamiento en cuadrantes del riesgo inicial en probabilidad o impacto, como se indica en la siguiente tabla.

% MITIGACION CONTROL	No. CUADRANTES
81% - 100%	3
61% - 80%	2
41% - 60%	1
21% - 40%	0

0% - 20%	0

Si el control es preventivo, se desplaza en probabilidad y si es detectivo o correctivo se desplaza en impacto.

5.4 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 evaluar una aceptación definitiva de estos riesgos, es importante tener en cuenta los siguientes aspectos:

- Cumplimiento regulatorio.
- Políticas organizacionales del **GECC**.
- Política de seguridad de la información del **GECC**.
- Sensibilidad y criticidad de los activos de información relevantes para el **GECC**.
- Niveles de aceptación de las posibles amenazas.
- Costo y eficacia de la implementación de controles para estos riesgos.

5.5 COMUNICACIÓN Y CONSULTA DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

La fase de comunicación de riesgos involucrará la información resultante en las etapas anteriormente descritas para la Gestión de Riesgos de Seguridad de la Información y Protección de Datos Personales, 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. Dicho plan debe ser desarrollado con el objetivo de crear conciencia en seguridad de la información y evidenciar los riesgos que acechan todos los activos de información, esencialmente los que conforman los pilares de la organización, de esta manera será posible una gestión de riesgos satisfactoria y la obtención del apoyo e información que conforman los análisis.

Se recomienda que el plan de comunicación de riesgos contemple como mínimo:

- Definiciones sobre la Gestión del Riesgo de Seguridad de la Información y Protección de Datos Personales.
- Objetivos y sensibilización de la Gestión del Riesgo de Seguridad de la Información y Protección de Datos Personales.
- Avances y resultados en el proceso de implementación.
- Propuestas para el tratamiento de riesgos.
- Madurez de los controles para mitigar los riesgos.
- Tableros e indicadores clave de riesgo de seguridad de la información (KRI).
- Niveles de aceptación de riesgos residuales.
- Cambios en los niveles de riesgo.
- Estado de riesgos no tratados.
- Informes especiales sobre eventos, impactos y acciones tomadas para mitigar los riesgos.
- Actas.

Los medios para comunicar la gestión serán:

- Circulares.
- Capacitaciones.
- Informes gerenciales.
- Presentaciones.
- Campañas de concientización.
- Reuniones/Comités.

5.6 MONITOREO Y REVISIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES

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 de la información y protección de datos personales en el **GECC**.

Se requiere el monitoreo permanente de:

- Nuevos activos de información fruto de nuevos procesos, productos o servicios.
- Cambios en la valoración de los activos de información, requeridos por ejemplo, por nuevos enfoques estratégicos del negocio o procesos.
- Nuevas amenazas internas y externas que no se han evaluado aún y el estado de las actuales.
- Nuevas vulnerabilidades y exposición a nuevas amenazas.
- Nuevas consecuencias que aún no hayan sido evaluadas producto de la materialización de amenazas y vulnerabilidades que incidan a un nivel no aceptable de riesgo.
- Incidentes y eventos de seguridad de la información.
- Alineación de los controles con la política de seguridad de la información del **GECC**.
- Si las actividades para la implementación de controles se están ejecutando de manera esperada.
- Indicadores clave de riesgo (KRI).
- Eficacia de los planes de tratamiento implementados.

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. El equipo de Seguridad de la Información de la Unidad Corporativa de Gestión del Riesgo (UCGR) ejecutará una vez al año (o cuando sea necesario) una validación de la normatividad emitida en materia de seguridad de la información y protección de datos personales 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

Nota: Las normas de Seguridad de la Información y protección de datos personales a las cuales se les garantiza cumplimiento por parte del **GECC** se encuentran relacionadas **FT-XX-XXX Normativa Cumplimiento Seguridad Información**.

6.1.2. El equipo de Seguridad de la Información de la Unidad Corporativa de Gestión del Riesgo (UCGR) ejecutará una vez al año (o cuando sea necesario) una validación del acogimiento de las políticas y procedimientos de seguridad de la información y protección de datos personales por parte de los colaboradores, contratistas y proveedores del **GECC**.

6.2. OBJETIVO

El cumplimiento de políticas y estándares es una preocupación permanente y prioritaria dentro del programa de seguridad de la información. Es por esto que la **UCGR**, en cuanto a Seguridad de la Información, ha adoptado las buenas prácticas de la norma **NTC-ISO-IEC 27001:2013** con el fin de garantizar los siguientes objetivos:

1. Cumplimiento de requisitos legales y contractuales que aplican al **GECC** en materia de seguridad de la información.
2. Revisiones de seguridad 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 de la información:

6.2.1. Cumplimiento de requisitos legales y contractuales

El objetivo del equipo de seguridad de la información de la **UCGR** será evitar el incumplimiento de las exigencias legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y la protección de datos personales dentro del **GECC**; y 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 información de datos personales.
- Reglamentación de controles criptográficos.

6.2.2. Revisiones de seguridad de la información

El objetivo del equipo de Seguridad de la Información de la **UCGR** 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.

6.3. METODOLOGÍA

La siguiente es la metodología definida por la **UCGR** para cumplir los objetivos propuestos frente a Seguridad de la Información:

Figura 5. Metodología para la Gestión de Cumplimiento

6.3.1. Alcance de las fases de la metodología de cumplimiento

6.3.1.1. Identificación de los requisitos de cumplimiento

a) Listado de requisitos legales y contractuales objeto de cumplimiento.
b) Listado de políticas, normas y procedimientos objeto de cumplimiento.
c) Entendimiento del alcance de los requisitos de cumplimiento.

Nota: El equipo de Seguridad de la Información de la **UCGR** utilizará el formato **FT-XX-XXX Análisis GAP de Cumplimiento** para registrar los elementos objeto de cumplimiento, su estado actual de cumplimiento y recomendaciones para el tratamiento de los mismos.

6.3.1.2. Análisis de la situación actual [GAP] e identificación de brechas

a) Identificación de actores asociados a los requisitos de cumplimiento (empresas, unidades, procesos, cargos, etc.).
b) Definición de escalas de valoración de cumplimiento (0 - 100%).
c) Valoración de cumplimiento para cada uno de los requisitos (entrevistas de verificación con los responsables) – Definición porcentaje de cumplimiento soportado en las escaladas definidas por el negocio.

d) Identificación de brechas para cada uno de los requisitos de cumplimiento.

6.3.1.3. Definición de planes de acción y responsables de cumplimiento

a) Definición de actividades e iniciativas requeridas para el cierre de las brechas resultantes del GAP.
b) Definición de recursos requeridos para la gestión de las actividades e iniciativas propuestas (humanos, físicos, económicos).
c) Gestión de recursos requeridos para la ejecución de las actividades e iniciativas propuestas.
d) Generar proyectos internos que sean administrados por las áreas responsables del tema correspondiente en el **GECC.**

6.3.1.4. Monitoreo y seguimiento al cumplimiento

a) Cumplimiento de las actividades e iniciativas registradas en el plan de acción dentro de las fechas establecidas.
b) Acciones correctivas para la normalización de desviaciones en los planes de trabajo establecidos.

7. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

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 **UCGR** define un procedimiento estándar de Gestión de Incidentes de Seguridad de la Información y Protección de Datos Personales, soportado en la buenas prácticas de la guía técnica colombiana **GTC-ISO-27035:2013**, y su alineación con el procedimiento **TI-PR-058 Gestión de Incidentes** desarrollado por la Unidad de Tecnología Informática (UTI) bajo las mejores prácticas, roles y responsabilidades de ITIL.

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

a. Detectar, reportar y evaluar incidentes de seguridad de la información y protección de datos personales de forma eficaz y oportuna.
b. Responder a incidentes de seguridad de la información y protección de datos personales, y hacer su gestión.
c. Detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información y protección de datos personales.
d. Mejorar continuamente la seguridad de la información, la protección de datos personales y la gestión de incidentes con el apoyo de los diferentes actores del proceso.

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

7.2. FASES DE LA GESTIÓN DE INCIDENTES

Figura 6. Fases de la gestión de incidentes de seguridad de la información - GTC-ISO-27035

7.2.1. Planificación y preparación

7.2.1.1. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

Todos los colaboradores, contratistas y proveedores de las empresas y unidades del **GECC** tienen la responsabilidad de detectar y reportar los incidentes de seguridad de la información y protección de datos personales que son ocasionados por accidentes, errores o actos maliciosos intencionados, robo, apropiación indebida, extorsión, fraude, espionaje o eventos ambientales; de tal forma que la **UCGR** gestione de manera eficaz y oportuna la solución y respuesta de los mismos.

La Gerencia Corporativa de Gestión Humana y las áreas que hacen sus veces en el **GECC** son responsables de difundir y dar a conocer la Política a todos los colaboradores.

La misma debe ser conocida, adoptada y aplicada por todos los colaboradores, contratistas y proveedores de las empresas y unidades del **GECC**.

El despliegue de la Política de Gestión de Incidentes de Seguridad de la Información y Protección de Datos Personales será aprobado por la Presidencia Ejecutiva y se encuentra publicado en el documento **XX-XX-XXX Política de Seguridad de la Información del Grupo Empresarial Cooperativo Coomeva (GECC)**.

7.2.1.2. La **UCGR** define y presenta a las instancias respectivas para su aprobación, las Políticas para la Gestión de Riesgos de Seguridad de la Información (Numeral 4.2. del presente Manual), las cuales deben ser dadas a conocer a los colaboradores, contratistas y proveedores del **GECC** por parte de la Gerencia Corporativa de Gestión Humana, la Gerencia Corporativa Administrativa y las áreas que hacen sus veces en el **GECC**.

7.2.1.3. El Jefe Corporativo de Seguridad de la Información o el Coordinador de Seguridad de la Información lideran el **EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ISIRT – INFORMATION SECURITY INCIDENT RESPONSE TEAM)**; el cual estará conformado por el personal de Seguridad de la Información de la **UCGR**, los líderes técnicos de la Unidad de Tecnología Informática (UTI) y los líderes de los procesos o servicios afectados; quienes se reunirán en una mesa de trabajo cuando se presente un incidente que afecte de manera considerable los activos de información del **GECC**, con el fin de definir acciones conjuntas que permitan llegar a una respuesta eficaz y oportuna sobre el mismo. Los incidentes de seguridad de la información y protección de datos personales reportados durante el mes serán presentados en el **COMITÉ TÉCNICO CORPORATIVO DE SEGURIDAD DE LA INFORMACIÓN**, con el fin de conocer las tendencias, categorías y tratamiento de los mismos, sin perjuicio de las líneas de reporte que formalmente se establezcan por parte de la **UCGR**.

7.2.1.4. Los colaboradores, contratistas y proveedores del **GECC** tienen la responsabilidad de identificar y registrar los eventos de seguridad de la

información y protección de datos personales a través de los medios definidos que son establecidos por la organización:

- *Mesa de Servicio:* Único punto de contacto para el registro de eventos e incidentes de seguridad de la información.
- *Intranet:* Registro directo a través de la herramienta de gestión de casos publicada en la intranet corporativa http://appmesadeservicio.coomeva.com.co/usdk.

Nota: Para una descripción más detallada del proceso de identificación, registro y gestión de incidentes según la **GTC-ISO-27035** referirse al **Anexo C – Diagrama de flujo de eventos e incidentes de seguridad de la información**.

7.2.1.5. Los Analistas de Seguridad de la Información de la **UCGR** son los responsables de revisar y analizar los eventos reportados por los colaboradores, contratistas y proveedores del **GECC** a través de los medios establecidos por la organización, con el fin de iniciar la gestión y categorización sobre aquellos que realmente puedan considerarse como un incidente de seguridad de la información, o dirigirlos y las áreas que hacen sus veces en el **GECC**.

7.2.1.6. Los Analistas de Seguridad de la Información de la **UCGR** solicitarán el apoyo del Jefe Corporativo o Coordinador de Seguridad de la Información cuando se presenten incidentes que ameriten la reunión del EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ISIRT).

7.2.1.7. La Jefatura Corporativa de Seguridad de la Información será la encargada de liderar los procesos de capacitación y sensibilización de los usuarios (colaboradores, contratistas y proveedores) relacionados con la gestión de incidentes de seguridad de la información y protección de datos personales.

7.2.1.8. La Jefatura Corporativa de Seguridad de la Información será la encargada de liderar y documentar las pruebas que se programen sobre el esquema de gestión de incidentes de seguridad de la información definido por la **UCGR**.

7.2.2. **Detección y reporte**

7.2.2.1. Los colaboradores, contratistas y proveedores del **GECC** tienen la responsabilidad de detectar y reportar los eventos de seguridad de la información y protección de datos personales a través de los medios establecidos por la organización. Para un mayor detalle, referirse a la **Fase de Planificación y preparación – Numeral 7.2.1.4** del presente documento. La información mínima requerida para el registro del evento de seguridad de la información se presenta en el documento **GC-FT-XXX Reporte de Eventos de Seguridad de la Información**.

7.2.3. **Evaluación y decisiones**

7.2.3.1. Los Analistas de Seguridad de la Información de la **UCGR** o quienes hagan sus veces en el **GECC** tienen la responsabilidad de analizar los eventos reportados por los colaboradores, contratistas y proveedores del **GECC**, y definir si estos efectivamente representan un incidente de seguridad de la información para el trámite correspondiente de los mismos. En caso de ser necesario, los Analistas de Seguridad de la Información validarán los incidentes reportados con el Coordinador o Jefe Corporativo de Seguridad de la Información para definir su categorización con incidente de seguridad.

7.2.3.2. Los Analistas de Seguridad de la Información de la **UCGR** o quienes hagan sus veces en el **GECC** tienen la responsabilidad de documentar en forma detallada el incidente sobre la herramienta de gestión de casos, con el fin dar respuesta al mismo. Cuando sea requerido, el Jefe Corporativo o Coordinador de Seguridad de la Información, apoyarán el proceso de documentación con el fin de agilizar el tratamiento del incidente registrado. La información detallada para dar respuesta al incidente de seguridad de la información se presenta en el **GC-FT-XXX Reporte de Incidentes de Seguridad de la Información**.

7.2.3.3. Los Analistas de Seguridad de la Información de la **UCGR** o quienes hagan sus veces en el **GECC** tienen la responsabilidad de categorizar el incidente reportado para el manejo estadístico correspondiente.

Categorías de incidentes

- Desastre natural
- Disturbios sociales
- Daño físico
- Fallas de infraestructura
- Perturbación por radiaciones
- Falla eléctrica
- Malware
- Ataque técnico
- Violación de reglas
- Compromiso de las funciones
- Riesgo de la información
- Contenidos peligrosos
- Otros incidentes

Nota: Para una descripción más detallada de las categorías de incidentes, referirse al **Anexo E - Categorías de incidentes de seguridad de la información**.

7.2.4. **Respuestas**

7.2.4.1. El equipo de Seguridad de la Información de la **UCGR** o quienes hagan sus veces en el **GECC** tiene la responsabilidad de dar respuesta a los incidentes de Seguridad de la Información que afecten los servicios tecnológicos corporativos, dentro de los tiempos acordados según la prioridad del incidente (Crítico – 2 hrs, Moderado – 4 hrs, Menor – 8 hrs). Cuando sea requerido, el equipo de Seguridad de la Información coordinará la contratación y realización de una Investigación Forense de Seguridad de la Información que permita identificar a detalle el origen, responsable y comportamiento del incidente. De igual forma, garantizará la cadena de custodia correspondiente en caso que el incidente tenga un tratamiento judicial.

7.2.4.2. El equipo de Seguridad de la Información de la **UCGR** o quienes hagan sus veces en el **GECC** tiene la responsabilidad de acordar con el usuario final el tiempo requerido para gestionar el incidente de seguridad de la información registrado; siempre y cuando éste no afecte la disponibilidad de los servicios tecnológicos corporativos.

7.2.4.3. El equipo de Seguridad de la Información de la **UCGR** o quienes hagan sus veces en el **GECC** tiene la responsabilidad de garantizar la recuperación del negocio ante el incidente de seguridad presentado.

7.2.5. **Lecciones aprendidas**

7.2.5.1. El equipo de Seguridad de la Información de la **UCGR** o quienes hagan sus veces en el **GECC** tiene la responsabilidad de documentar las lecciones aprendidas resultantes del proceso de gestión de incidentes, con el objetivo de garantizar la base de conocimiento.

7.2.5.2. El equipo de Seguridad de la Información de la **UCGR** o quienes hagan sus veces en el **GECC** realizará como mínimo una (1) vez al año la revisión y mejora de los procesos de gestión de riesgos y gestión de incidentes de seguridad 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 de la Información, 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 **UCGR** 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 Unidad Corporativa de Gestión del 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. ____del ___ de _____ de 2016.

Anexo A – Amenazas de Seguridad de la Información

GRUPO DE AMENAZA	ID AMENAZA	NOMBRE	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	DESCRIPCION
Desastres Naturales (Sin Intervención Humana)	A1	Fuego (Sin Intervención Humana)	✗	✗	√	Incendios: Posibilidad de que el fuego causado por un desastre natural acabe con recursos del sistema.
	A2	Daños por agua (Sin Intervención Humana)	✗	✗	√	Inundaciones: Posibilidad de que el agua acabe con recursos del sistema.
	A3	Desastres naturales	✗	✗	√	Otros incidentes que se producen sin intervención humana: Rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.
Origen Industrial (Con Intervención Humana)	A4	Fuego (Con Intervención Humana)	✗	✗	√	Incendios: Posibilidad de que el fuego generado por fallas industriales acabe con recursos del sistema.
	A5	Daños por agua (Con Intervención Humana)	✗	✗	√	Escapes, fugas, inundaciones: Posibilidad de que el agua acabe con los recursos del sistema.
	A6	Desastres industriales	✗	✗	√	Otros desastres debidos a la actividad humana: Explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc.
	A7	Contaminación mecánica	✗	✗	√	Vibraciones, polvo, suciedad, etc.
	A8	Contaminación electromagnética	✗	✗	√	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.

	A9	Avería de origen físico o lógico	✗	✗	√	Fallos en los equipos y/o fallos en los programas. Puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen de fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
	A10	Corte del suministro eléctrico	✗	✗	√	Cese de la alimentación de potencia.
	A11	Condiciones inadecuadas de temperatura y/o humedad	✗	✗	√	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: Excesivo calor, excesivo frío, exceso de humedad, etc.
	A12	Fallo de servicios de comunicaciones	✗	✗	√	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.
	A13	Interrupción de otros servicios y suministros esenciales	✗	✗	√	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante, etc.
	A14	Degradación de los soportes de almacenamiento de la información	✗	✗	√	Como consecuencia del paso del tiempo.
	A15	Emanaciones electromagnéticas	√	✗	✗	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (Receptores de radio) derivándose una fuga de información.
Errores y Fallos No Intencionados	A16	Errores de los usuarios	✗	√	√	Equivocaciones de las personas cuando usan los servicios, datos, etc.
	A17	Errores del administrador	√	√	√	Equivocaciones de personas con responsabilidades de instalación y

						operación.
	A18	Errores de monitorización (Log)	✗	√	✗	Inadecuado registro de actividades: Falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.
	A19	Errores de configuración	√	√	√	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: Privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
	A20	Deficiencias en la organización	✗	✗	√	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.
	A21	Difusión de software dañino	√	√	√	Propagación inocente de virus, espías (Spyware), gusanos, troyanos, bombas lógicas, etc.
	A22	Errores de re-encaminamiento	√	√	✗	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.
	A23	Errores de secuencia	✗	√	✗	Alteración accidental del orden de los mensajes transmitidos.
	A24	Escapes de información	√	✗	✗	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
	A25	Alteración de la información	✗	√	✗	Alteración accidental de la información.
	A26	Introducción de información	✗	√	✗	Inserción accidental de información incorrecta.

		incorrecta				
	A27	Degradación de la información	✗	√	✗	Degradación accidental de la información.
	A28	Destrucción de información	✗	✗	√	Pérdida accidental de información.
	A29	Divulgación de información por indiscreción	√	✗	✗	Revelación por indiscreción.
	A30	Vulnerabilidades de los programas (Software)	√	√	√	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
	A31	Errores de mantenimiento / actualización de programas (Software)	✗	√	√	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
	A32	Errores de mantenimiento / actualización de equipos (Hardware)	✗	✗	√	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
	A33	Caída del sistema por agotamiento de recursos	✗	✗	√	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
	A34	Indisponibilidad accidental del personal	✗	✗	√	Ausencia accidental del puesto de trabajo: Enfermedad, alteraciones del orden público, guerra bacteriológica, etc.
Ataques Intencionados	A35	Manipulación de la configuración	√	√	√	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: Privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
	A36	Suplantación de la identidad del usuario	√	√	✗	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de éste para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la organización o por personal contratado temporalmente.

	A37	Abuso de privilegios de acceso	√	√	✗	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
	A38	Uso no previsto	✗	✗	√	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: Juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
	A39	Difusión deliberada de software dañino	√	√	√	Propagación intencionada de virus, espías (Spyware), gusanos, troyanos, bombas lógicas, etc.
	A40	Re-encaminamiento intencional de mensajes	√	√	✗	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.
	A41	Alteración de secuencia	✗	√	✗	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.
	A42	Acceso no autorizado	√	√	✗	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

	A43	Análisis de tráfico	√	✗	✗	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "Monitorización del tráfico".
	A44	Interceptación de información (Escucha)	√	✗	✗	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
	A45	Modificación de la información (Intencional)	✗	√	✗	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
	A46	Introducción de falsa información	✗	√	✗	Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio.
	A47	Corrupción de la información (Intencional)	✗	√	✗	Degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
	A48	Destrucción de la información (Intencional)	✗	✗	√	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
	A49	Divulgación de información (Intencional)	√	✗	✗	Revelación intencional de información.
	A50	Manipulación de programas	√	√	✗	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
	A51	Denegación de servicio	✗	✗	√	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

	A52	Robo	√	✗	√	La sustracción de información provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de activos de información, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
	A53	Ataque destructivo	✗	✗	√	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la organización o por personas contratadas de forma temporal.
	A54	Ocupación no autorizada	√	✗	√	Cuando las instalaciones son invadidas por personas que no han sido autorizadas.
	A55	Indisponibilidad deliberada del personal	✗	✗	√	Ausencia deliberada del puesto de trabajo: Como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc.
	A56	Extorsión	√	√	✗	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
	A57	Ingeniería social	√	√	✗	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

Anexo B – Vulnerabilidades de Seguridad de la Información

VULNERABILIDADES SEGURIDAD DE LA INFORMACIÓN	
ID	**Descripción Vulnerabilidad**
V1	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento
V2	Ausencias de esquemas de reemplazo periódico.
V3	Susceptibilidad a la humedad, el polvo y la suciedad.
V4	Sensibilidad a la radiación electromagnética
V5	Ausencia de un eficiente control de cambios en la configuración
V6	Susceptibilidad a las variaciones de voltaje
V7	Susceptibilidad a las variaciones de temperatura
V8	Almacenamiento de equipos sin protección
V9	Falta de cuidado en la disposición final
V10	Deficiente sistema de enfriamiento
V11	Deficiente Sistema de respaldo eléctrico
V12	Deficiente sistema contra incendios
V13	Copia no controlada
V14	Ausencia o insuficiencia en el control de los activos que se encuentran fuera de las instalaciones.
V15	Incumplimiento de las condiciones técnicas y/o ambientales provistas por el fabricante.
V16	Fallas o degradación de equipos.
V17	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
V18	Ausencia de sistemas y/o procedimientos de monitoreo de la red.
V19	Conexión deficiente y/o desorganización del cableado estructurado eléctrico.
V20	Punto único de falla.
V21	Ausencia o insuficiencia de actualizaciones.
V22	Configuraciones por defecto.
V23	Ausencia o insuficiencia de pruebas de software
V24	Defectos bien conocidos en el software
V25	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo
V26	Asignación errada de los derechos de acceso
V27	Software ampliamente distribuido
V28	En términos de tiempo utilización de datos errados en los programas de aplicación.
V29	Interfaz de usuario compleja
V30	Ausencia de documentación

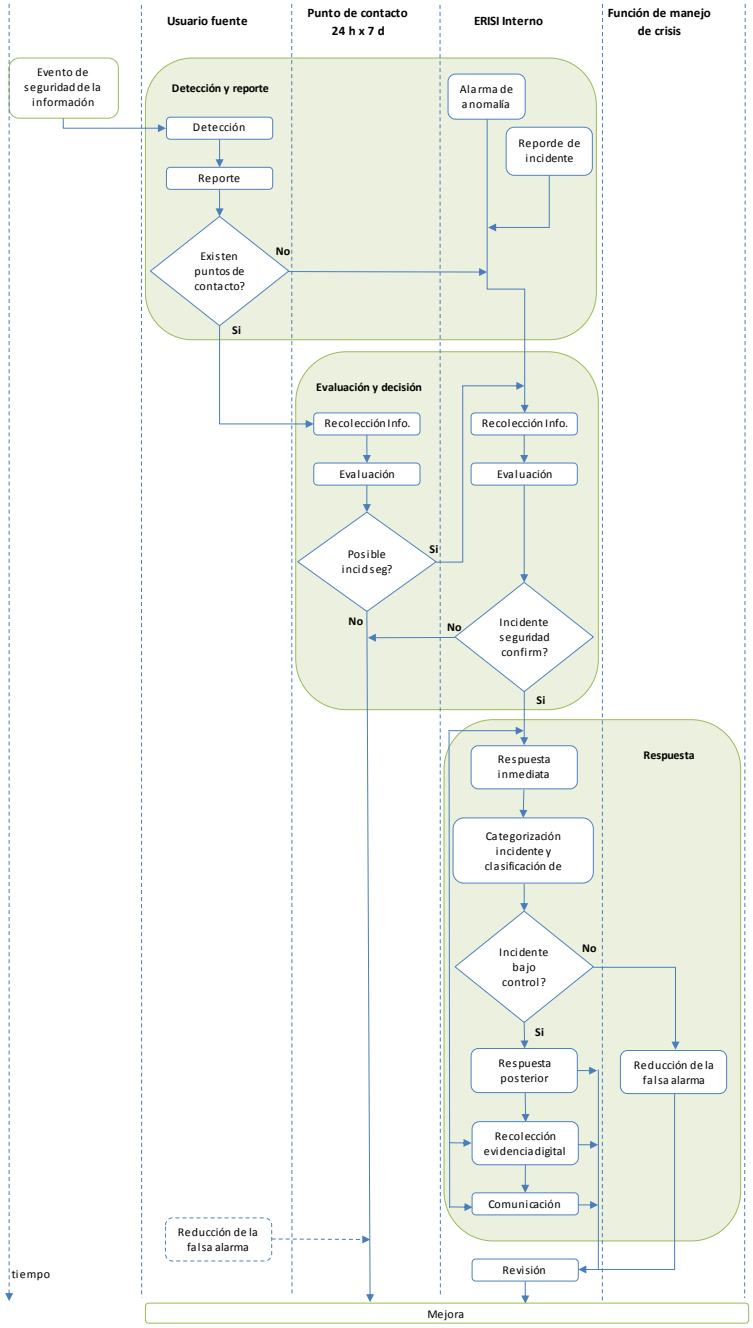
V31	Configuración incorrecta de parámetros
V32	Fechas incorrectas
V33	Ausencia o deficiencia de esquema de autenticación y/o gestión de las sesiones en las aplicaciones
V34	Tablas de contraseñas sin protección
V35	Gestión deficientes de las contraseñas
V36	Habilitación de servicios innecesarios
V37	Software nuevo o inmaduro
V38	Especificaciones incompletas o no claras para los desarrolladores
V39	Descarga y uso no controlados de software
V40	Ausencia o insuficiencia de copias de respaldo.
V41	Ausencia de la protección física de la edificación, puertas y ventanas
V42	Falla en la producción de informes de gestión
V43	Ausencia de pruebas de envío o recepción de mensajes
V44	Líneas de comunicación sin protección
V45	Tráfico sensible sin protección
V46	Conexión deficiente de los cables.
V47	Punto único de falla
V48	Ausencia de identificación y autentificación de emisor y receptor
V49	Arquitectura insegura de la red
V50	Transferencia de contraseñas en claro
V51	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)
V52	Conexiones de red pública sin protección
V53	Dependencia de personal clave, ausentismo y/o personal insuficiente.
V54	Ausencia de controles y verificaciones en los procesos de selección y contratación de personal.
V55	Insuficiente entrenamiento, capacitación o sensibilización.
V56	Uso incorrecto de software y hardware
V57	Falta de conciencia acerca de la seguridad
V58	Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros.
V59	Trabajo no supervisado del personal externo o de limpieza
V60	Ausencia o insuficiencia de acuerdos de nivel de servicio, clausulas contractuales y/o acuerdos de confidencialidad con terceras partes.
V61	Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad
V62	Ausencia o insuficiencia en la definición y formalización de roles, funciones y responsabilidades.
V63	Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables.
V64	Falta de segregación de funciones o incorrecta aplicación de las mismas.
V65	Incumplimiento de políticas o procedimientos internos.

V66	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
V67	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
V68	Ubicación geográfica de las instalaciones en una zona de alto impacto por eventos externos(desastres naturales, orden público, entre otros)
V69	Red energética inestable
V70	Ausencia o insuficiencia de controles de monitoreo de las instalaciones (por ej. detección o extinción de incendios, líquidos Inflamables)
V71	Ausencia o insuficiencia de planes de emergencia y simulacros de evacuación.
V72	Falla en los servicios esenciales (internet, teléfonos, aire acondicionado, energía, agua,etc).
V73	Ausencia o insuficiencia de mantenimiento preventivo/ correctivo.
V74	Ausencia de procedimiento formal para el registro y retiro del usuarios
V75	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso
V76	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes.
V77	Ausencia de auditorías (supervisiones) regulares
V78	Ausencia de procedimientos de identificación y valoración de riesgos
V79	Ausencia en los reportes de fallas en los registros de operadores y administradores.
V80	Respuesta inadecuada del mantenimiento del servicio
V81	Ausencia de procedimiento de control de cambios eficaz
V82	Falta de procedimiento formal para el control de la documentación del SGSI
V83	Ausencia de procedimiento formal para la supervisión del registro del SGSI
V84	Ausencia de procedimiento formal para la autorización de la información disponible al público
V85	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
V86	Ausencia de planes de continuidad
V87	Ausencia de políticas sobre el uso del correo electrónico
V88	Ausencia de procedimientos para la introducción del software en los sistemas operativos
V89	Ausencia de registros en las bitácoras (logs) de administrador y operario.
V90	Ausencia de procedimientos para el manejo de información clasificada
V91	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos
V92	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados

V93	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información.
V94	Ausencia de política formal sobre la utilización de computadores portátiles
V95	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla
V96	Ausencia de autorización de los recursos de procesamiento de la información
V97	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad
V98	Ausencia de revisiones regulares por parte de la gerencia
V99	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
V100	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales
V101	Ausencia o insuficiencia de un procedimiento para el manejo de comunicaciones externas
V102	Acceso no controlado a información sensible/confidencial.
V103	Documentación insuficiente o desactualizada.
V104	Eliminación de información sin borrado seguro.
V105	Ausencia o insuficiencia de un proceso para clasificar y etiquetar la información
V106	Ausencia o insuficiencia de procedimientos de monitoreo de los recursos de procesamiento de información.
V107	Almacenamiento de información de forma no segura o Inadecuada
V108	Ausencia conexiones remotas seguras para empleados y/o terceros ubicados fuera de las instalaciones de la empresa
V109	Fallas de inyección en las consultas SQL, LDAP, Comandos SO, Interpretes XML, Encabezados SMTP, Argumentos de programas, etc.
V110	Falla de seguridad en aplicaciones web (secuencia de comandos en sitios cruzados XSS)
V111	Referencia directa insegura a objetos
V112	Configuración de seguridad incorrecta
V113	Inexistente control de acceso a nivel de funcionalidades
V114	Falsificación de peticiones en sitios cruzados (CSRF)
V115	Uso de componentes /bibliotecas de programación con vulnerabilidades conocidas

V116	Redirecciones y reenvíos de páginas a sitios no validos

Anexo C – Diagrama de Flujo de Eventos e Incidentes de Seguridad de la Información



Anexo D – Categorías de Incidentes de Seguridad de la Información

Categoría	Descripción
Incidente de desastre natural	La pérdida de seguridad de la información es causada por desastres naturales que están por fuera del control humano
Incidente de disturbios sociales	La pérdida de seguridad de la información es causada por la inestabilidad de la sociedad
Incidente de daño físico	La pérdida de seguridad de la información es causada por acciones físicas accidentales o deliberadas
Incidente de fallas de infraestructura	La pérdida de seguridad de la información es causada por fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información
Incidente de perturbación por radiaciones	La pérdida de seguridad de la información es causada por perturbaciones debidas a radiaciones
Incidente de falla eléctrica	La pérdida de seguridad de la información es causada por fallas en los sistemas de información o en instalaciones no técnicas relacionadas, al igual que problemas humanos no intencionales que dan como resultado la no disponibilidad o destrucción de los sistemas de información
Incidente de malware	La pérdida de seguridad de la información es causada por programas maliciosos creados y divulgados en forma deliberada. Un programa malicioso se inserta en los sistemas de información para afectar la confidencialidad, la integridad o disponibilidad de los datos, las aplicaciones o sistemas operativos, y/o afectar la operación normal de los sistemas de información
Incidente de ataque técnico	La pérdida de seguridad de la información es causada por el ataque a sistemas de información, a través de redes u otros medios técnicos, ya sea mediante el aprovechamiento de las vulnerabilidades de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, lo que da como resultado un estado anormal de los sistemas de información, o daño potencial a las operaciones presentes del sistema
Incidente de violación de reglas	La pérdida de seguridad de seguridad de la información es causada por violación de las reglas en forma accidental o deliberada
Incidente de compromiso de las funciones	La pérdida de seguridad de la información es causada al poner en riesgo en forma accidental o deliberada las funciones de los sistemas de información en cuanto a seguridad
Incidente de puesta en riesgo de la información	La pérdida se seguridad de la información es causada al poner en riesgo en forma accidental o deliberada la seguridad de la información, por ejemplo, en cuanto a confidencialidad, integridad, disponibilidad, etc.
Incidente relacionado con contenidos peligrosos	La pérdida de seguridad de la información es causada por la propagación de contenido indeseable a través de redes de

	información, lo que pone en peligro la seguridad nacional, la estabilidad social y/o la seguridad y beneficios públicos
Otros incidentes	No clasificados en ninguna de las categorías de incidentes anteriores