TABLA DE CONTENIDO

1. PROCESO

Control – Seguridad de la Información

2. INTRODUCCIÓN

Las amenazas que vulneran la seguridad de la información y ciberseguridad pueden afectar considerablemente la reputación de Grupo Aval Acciones y Valores S.A (Grupo Aval) y sus subordinadas, así como sus activos de información más importantes. Conscientes de las consecuencias, y como respuesta a su compromiso en la preservación de los pilares de seguridad de la información y ciberseguridad, Grupo Aval y sus subordinadas desarrollan la presente política corporativa para proteger y garantizar la disponibilidad, confidencialidad, Integridad y privacidad de la información y el establecimiento, implementación, mantenimiento y mejora continua de su sistema de gestión de seguridad de la información y ciberseguridad.

3. OBJETIVO

3.1 Objetivos Generales

Proteger los activos de información estratégicos de Grupo Aval y sus subordinadas, gestionando y cumpliendo los principios generales que preservan la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información mediante la definición de políticas, identificación de riesgos y controles, que fijan roles y responsabilidades de los actores clave, que intervienen en el Sistema de Gestión de Seguridad de la Información (SGSI).

3.2 Objetivos Específicos

- Establecer los lineamientos para mantener la confidencialidad, integridad, disponibilidad y privacidad de la información y ciberseguridad en Grupo Aval y sus subordinadas.
- Definir de qué manera la información debe ser protegida de forma homogénea con base en la valoración de los activos críticos de información de Grupo Aval y sus Subordinadas.
- Garantizar la gestión de riesgos de seguridad de la información y ciberseguridad en Grupo Aval y sus subordinadas.
- Establecer e implementar los controles que preserven la confidencialidad, integridad, disponibilidad y privacidad de la información en Grupo Aval y sus subordinadas.
- Fijar roles y responsabilidades de autoridades de control en materia de los pilares de seguridad de la información y ciberseguridad de Grupo Aval y sus subordinadas.
- Garantizar la aplicación de los requisitos de seguridad de la información y ciberseguridad en la continuidad del negocio y la recuperación ante desastres en Grupo Aval y sus subordinadas.
- Definir el marco general para gestionar el Sistema de Gestión de Seguridad de la Información (SGSI) que se adapte a los requerimientos del negocio y que esté acorde a los lineamientos establecidos en esta política corporativa.

4. ALCANCE

La presente Política de Seguridad de la Información y Ciberseguridad aplica a todos los Colaboradores de Grupo Aval y sus subordinadas, funcionarios temporales y proveedores que en el ejercicio de sus funciones utilicen información y servicios tecnológicos de Grupo Aval o subordinadas; deberán adoptarla de acuerdo con la naturaleza, tamaño complejidad y estructura de sus operaciones.

5. GLOSARIO

- **Activo de Información:** conocimiento o datos que tienen valor para la entidad o el individuo.
- **Administración:** Presidente, Vicepresidentes de Grupo Aval y sus subordinadas, o quienes hagan sus veces.
- **Alta Gerencia:** son las personas responsables de dirigir, ejecutar y supervisar las operaciones de la entidad bajo la dirección de la Junta Directiva.
- **Amenaza:** causa potencial de un incidente no deseado, el cual puede causar daños a un sistema o a la organización[1]
- **Apetito de Riesgo:** es la exposición al nivel de riesgo que una entidad está dispuesta a asumir en el desarrollo de su actividad con el fin de alcanzar sus objetivos estratégicos y cumplir con su plan de negocios.
- **Ciberamenaza o Amenaza Cibernética:** aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.[2]
- **Ciberespacio:** entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.[2]
- **Ciber riesgo o Riesgo Cibernético:** posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.[2]
- **Ciberseguridad:** es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.[2]
- **Colaborador:** trabajadores incluyendo Alta Gerencia, practicantes y aprendices de Grupo Aval y/o de sus subordinadas.
- **Confidencialidad:** hace referencia a la protección de información cuya divulgación no está autorizada.[1]
- **Control:** medida que tome la entidad y otras partes, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos.

[1] NTC-ISO 27000
[2] CE 007 de 2018

- **Disponibilidad:** la información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.[1]

- **Subordinadas:** corresponde a las entidades del Grupo Aval, dentro de las cuales se destacan como sus principales unidades de negocio el Banco de Bogotá, Banco Popular, Banco de Occidente, Banco AV Villas, Corficolombiana y Porvenir.

- **Estándares y Buenas Prácticas de Seguridad de la Información:** conjunto de medidas implementadas para asegurar que la información de la entidad y aquella que se encuentre en su poder sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones del negocio (confidencialidad), que esté protegida contra modificaciones no planeadas, realizadas con o sin intención (integridad), que esté disponible cuando sea requerida (disponibilidad) y que sólo sea utilizada para los propósitos con que fue obtenida (privacidad y reserva) y única y exclusivamente para fines del negocio.

- **Evaluación de Riesgos:** proceso de la entidad para identificar y analizar riesgos relevantes para el logro de sus objetivos, formando las bases para determinar cómo se deben administrar los riesgos.

- **Evento de Ciberseguridad:** ocurrencia de una situación que puede afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.[2]

- **Incidente de Ciberseguridad:** ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.[2]

- **Incidentes de Seguridad de la Información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de amenazar la seguridad de la información[4].

- **Integridad:** la información debe ser precisa, coherente y completa desde su creación hasta su destrucción.[1]

- **Magnitud Impacto:** es la pérdida (monetaria o no monetaria) generada por la materialización de un riesgo, que puede ser medida cualitativa y cuantitativamente.

- **Pilares de Seguridad de la Información:** principios o características de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- **Privacidad:** propiedad de la información que garantiza el uso adecuado de la misma, así esté legítimamente autorizado a manejarla.[3]

- **Probabilidad de Ocurrencia:** es la posibilidad que un riesgo se materialice. Para determinar esta probabilidad se puede utilizar el análisis cualitativo o cuantitativo.

- **Proceso de Evaluación de Administración de Riesgo:** proceso de identificación y análisis de riesgos relevantes existentes y que impiden el logro de los objetivos; formando

[1] NTC-ISO 27000
[2] CE 007 de 2018
[3] Ley 1581 de 2012
[4] NTC-ISO 27000

una base para determinar cómo deben ser administrados, transferidos, controlados o asumidos.

- **Responsable de la Información - RES:** es el colaborador para quien la información fue creada con el objetivo de realizar sus funciones en el negocio y tiene la responsabilidad de administrarla, clasificarla y evaluar los riesgos que pueden afectarla. También es el primer responsable de implantar la Política de Seguridad de la Información dentro de su área y para poder realizarlo debe conocer el valor de su información, los usuarios que deben tener acceso a ella y los privilegios que requieren para su uso.

- **Reserva:** hace referencia a que la información sólo pueda ser utilizada para los propósitos con que fue obtenida del titular y única y exclusivamente para fines del negocio. Conlleva la obligación de no utilizar, revelar o distribuir la información adquirida para fines diferentes para los cuales fue obtenida del titular y única y exclusivamente para fines del negocio.

- **Riesgo:** la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

- **Riesgos Emergentes:** entiéndase por aquellos riesgos nuevos o no identificados que nunca han sido considerados previamente por la entidad, o riesgos conocidos que están evolucionando de manera inesperada, que puedan afectar no solo a una compañía sino a todo un sector o toda la economía**.**

- **Riesgo Genérico:** son todos aquellos riesgos identificados por la segunda línea de Grupo Aval/Subordinadas.

- **Riesgo Inherente (RI):** nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. En otras palabras, Riesgo Inherente es la probabilidad de que una entidad pueda incurrir una pérdida material como resultado de su exposición a, y de la incertidumbre que surge de, potenciales eventos adversos. El RI es intrínseco a cada actividad significativa y se evalúa sin tener en consideración el tamaño de esta en relación con la organización y antes de evaluar la calidad de la administración de los riesgos que ésta realiza. Para identificar y evaluar los RI a los que está expuesta una organización es esencial tener un conocimiento profundo tanto de la naturaleza de las actividades que ésta realiza como del entorno en el que opera.

- **Riesgo Residual:** también conocido como riesgo neto, es el resultado de la mitigación de los riesgos inherentes por parte de la gestión operativa y las funciones de supervisión. En otras palabras, es el riesgo que permanece tras haberse ejecutado los controles y se hayan tomado las medidas preventivas para dar respuesta a los riesgos identificados.

- **Seguridad de la Información:** preservación de la confidencialidad, integridad y disponibilidad de la información.[3]-[4] También denominada el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para preservar los pilares de la información, que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.[2]

- **Sistema de Gestión de Seguridad de la Información y Ciberseguridad:** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas,

[2] CE 007 de 2018
[3] Ley 1581 de 2012
[4] NTC-ISO 27000

planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

- **Vulnerabilidad:** debilidad de una organización que potencialmente permite que una amenaza afecte a un activo.[4] también denominada la debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio[2]

6. REGULACIÓN

El Grupo Aval y sus subordinadas deben cumplir con las regulaciones de Seguridad de la Información vigentes en el país y con regulaciones internacionales que se le obliguen a adoptar, como ejemplo se encuentran:

- **Circular Básica Jurídica de la Superintendencia Financiera (CE 029/14) Parte I Título IV Capítulo V:** Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad.
- **Circular Básica Jurídica de la Superintendencia Financiera (CE 029/14) Parte I Título III Capítulo I:** Acceso e información al consumidor financiero.
- **Circular Básica Jurídica de la Superintendencia Financiera (CE 029/14) Parte I Título I Capítulo VI:** Reglas relativas al uso de servicios de computación en la nube.
- **Circular Básica Jurídica de la Superintendencia Financiera (CE 02/14) Parte I, Título II, Capítulo I:** Canales, Medios, Seguridad y Calidad en el manejo de la información en la prestación de servicios financieros.
- **Ley 1581 de 2012 (Habeas Data):** Por la cual se dictan disposiciones generales para el tratamiento y la protección de datos personales.
- **Ley 1273 de 2009:** Protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
- **Ley 527 de 1999:** por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
- **Ley SOX**: Ley federal de los Estados Unidos de América emitida en 2002 que tiene como objetivo mejorar el ambiente de control interno de las empresas que cotizan en las bolsas de valores de los Estados Unidos; definir y formalizar responsabilidades sobre su cumplimiento para la prevención de errores contables y de reporte.
- **Ley 1266 de 2008**: Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

6.1 Otros Marcos de Referencia

Como mejores prácticas del mercado, son utilizados los siguientes marcos de referencia. De igual forma se aclara que las prácticas no pretenden ser un listado taxativas:

- **NTC-ISO-IEC 27001:2013:** esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de Seguridad de la Información, dentro del contexto de la organización. La presente norma también incluye

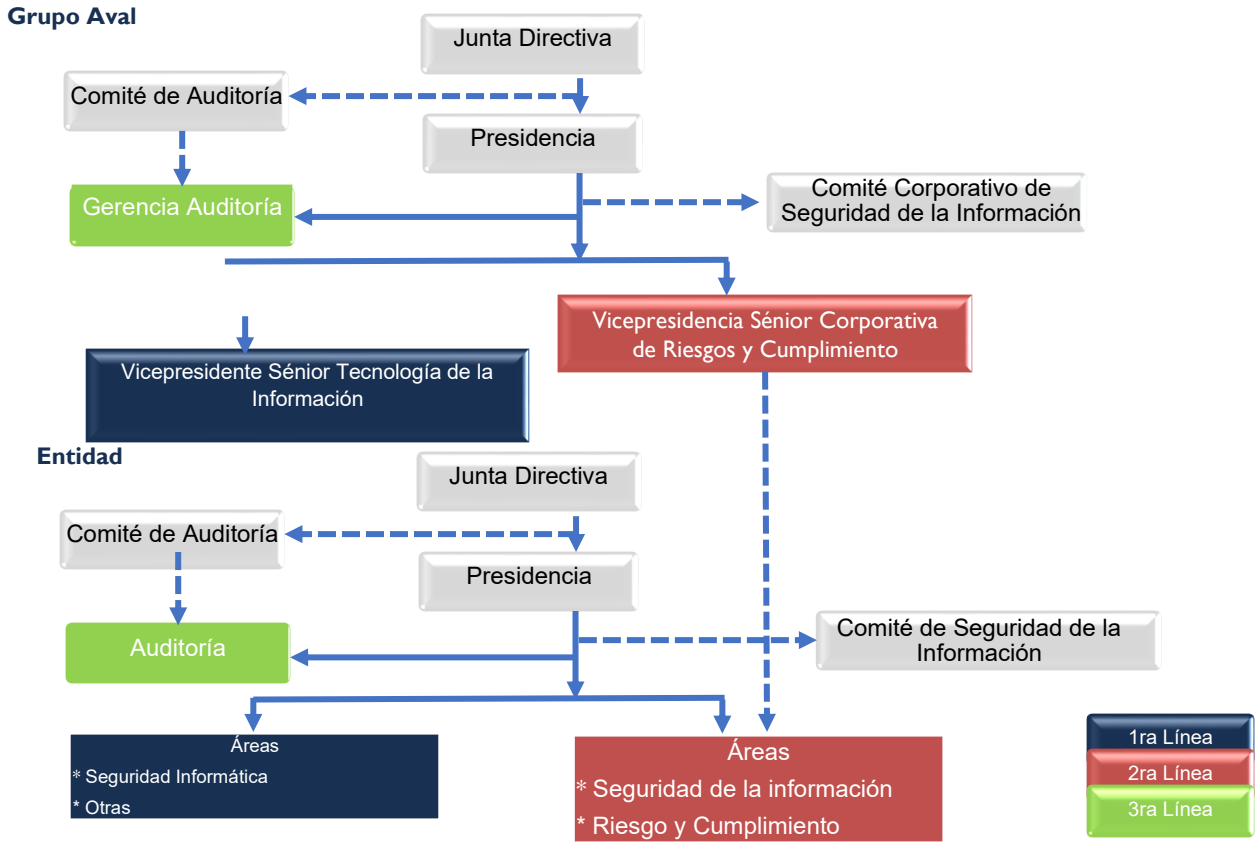
los requisitos para la valoración y el tratamiento de riesgos de Seguridad de la Información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicados a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

- **ISO/IEC 27000:** es un grupo de estándares internacionales titulados: Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Visión de conjunto y vocabulario. Tiene como fin ayudar a organizaciones de todo tipo y tamaño a implementar y operar un Sistema de Gestión de la Seguridad de la Información (SGSI).
- **ISO/IEC 27701:** estándar que especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de privacidad de la información.
- **Framework de Ciberseguridad NIST:** marco de trabajo basado en estándares, directrices y prácticas existentes para que las organizaciones gestionen el riesgo de ciberseguridad.

7. RESPONSABILIDADES DE LOS USUARIOS

7.1 Gobierno para la Gestión de Seguridad de la Información y Ciberseguridad

Grupo Aval y sus subordinadas deben estructurar las funciones y responsabilidades frente al Riesgo de Seguridad de la Información y Ciberseguridad y frente a la gestión en esta materia, de acuerdo con la Política Corporativa para la Gestión Integral de Riesgos; este marco de referencia define el esquema de las tres líneas, considerando (i) la gestión por línea de negocio, (ii) una función de gestión de riesgo de Seguridad de la Información independiente, y (iii) una revisión independiente.



7.1.1 Primera Línea

La primera línea la constituyen las áreas de Seguridad TI y todos los Colaboradores de Grupo Aval y sus subordinadas. La Política de Seguridad de la Información y Ciberseguridad reconoce a las áreas de seguridad informática y demás Colaboradores como responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos e incidentes de seguridad de la información y ciberseguridad inherentes a los productos, actividades, procesos y sistemas de seguridad. Quienes conforman esta línea de defensa deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas.

Así mismo deben cumplir con políticas y procedimientos definidos por la Organización, contribuyendo a una sólida cultura en seguridad de la información y ciberseguridad.

7.1.2 Segunda Línea

Esta línea está conformada por el área de Riesgos o equivalentes de cada entidad, la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de todas las obligaciones de riesgo en seguridad de la información y ciberseguridad.

El Oficial de Seguridad de la Información también puede desempeñar la función de Director Riesgos, Director Cumplimiento o equivalente. Este responsable debe presentar los resultados de gestión directamente a la Alta Gerencia o al Comité de Auditoría (o al Comité que la Junta Directiva designe). En caso de separación de tareas, la relación entre los oficiales previamente citados y sus respectivas funciones debe definirse y conocerse con claridad. Así mismo, debe contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el Sistema de Gestión de Seguridad de la Información. Para ello, debe estar plenamente familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios y los riesgos de Seguridad de la Información derivados del negocio, incluyendo temas específicos de ciberseguridad.

7.1.3 Tercera Línea

La tercera línea juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de la seguridad de la información y ciberseguridad, así como las políticas, estándares y procedimientos de los sistemas, rindiendo cuentas al Comité de Auditoría o al que se designe. Las personas encargadas de auditorías internas que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control. Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

7.2 Roles y Responsabilidades

Para dar cumplimiento a los objetivos de la Política de Seguridad de la Información y Ciberseguridad, se han definido los siguientes actores clave en la gestión de seguridad de la información:

Actor	Actividades	
	De Ejecución	**De Supervisión**
Junta Directiva	• Aprobar la Política de Seguridad de la Información y Ciberseguridad. • Estudiar y aprobar el Apetito de Riesgo de las entidades. • Velar porque se cuente con los recursos técnicos y humanos suficientes para gestionar adecuadamente la seguridad de la información y ciberseguridad y otras cuando apliquen • Exigir el cumplimiento de las normas y regulaciones gubernamentales de seguridad de la información y ciberseguridad. • Participar en programas de concientización y capacitación en temas de seguridad de la información y ciberseguridad.	• Supervisar la Seguridad de la Información y Ciberseguridad en Grupo Aval y las subordinadas, comprendiendo los riesgos y asegurando que estos sean gestionados.
Alta Gerencia	• Evaluar el seguimiento del nivel de madurez y monitoreo de las políticas propuestas del Sistema de gestión de Seguridad de la Información. • Evaluar los informes que le presente el Oficial de Seguridad de la Información y Ciberseguridad sobre los resultados de la evaluación de efectividad del programa de Seguridad de la Información y Ciberseguridad, propuestas de mejora en materias de Ciberseguridad y resumen de los incidentes que afectaron a la entidad • Promover la aplicación y apropiación de buenas prácticas de seguridad de la información y ciberseguridad. • Garantizar la evaluación de seguridad de la información y ciberseguridad de todos sus activos de información sin excepción. • Fortalecer la cultura de seguridad de la información de los Colaboradores de Grupo Aval y sus subordinadas, que administren activos de información. Cada entidad debe evaluar la necesidad de sensibilizar en seguridad de la información a sus proveedores críticos que acceden a los activos de información.	• Supervisar la seguridad de la información y ciberseguridad en Grupo Aval y las subordinadas, comprendiendo los riesgos y asegurando que estos sean gestionados. • Liderar el GERI - Grupo Ejecutivo Respuesta Incidente de Seguridad de la Información, aplica para Grupo Aval.
Comité Corporativo de Seguridad de la Información	• Proveer principios, directrices y lineamientos Corporativos de seguridad de la información y ciberseguridad, tomar las acciones preventivas y correctivas pertinentes para las entidades del Grupo Aval. • Identificar, evaluar e incluir los requerimientos de seguridad de la información y ciberseguridad en las iniciativas corporativas realizadas para las entidades.	• Monitorear el cumplimiento a nivel corporativo de las políticas del Sistema de gestión de Seguridad de la Información y Ciberseguridad en cada entidad. • Monitorear el cumplimiento a nivel internos de las Políticas del Sistema de Gestión de

Actor	Actividades	
	De Ejecución	De Supervisión
	• Tomar decisiones relacionadas con la seguridad de la información y ciberseguridad de las entidades. • Socializar actividades y proyectos que sean de interés común y/o impacten a las entidades. • Generar retroalimentación de las jornadas de seguridad y diagnósticos de los SGSI realizados y contribuir a la mejora continua de la postura de Seguridad de la Información. • Definir principios, directrices y lineamientos corporativos de seguridad de la información y ciberseguridad. • Definir requerimientos de seguridad de la información y ciberseguridad en las iniciativas corporativas realizadas para las entidades. • Socializar actividades y proyectos que sean de interés común y/o impacten a las Empresas del servicio.	Seguridad de la Información y Ciberseguridad en cada entidad.
Comité de Riesgos-Entidades (O quien haga sus veces)	• Aprobar las directrices que crean convenientes, en cada una de las entidades, para el mejoramiento de la Gestión de Seguridad de la Información. • Monitorear la Gestión realizada por las entidades por medio de los reportes consolidados que se le presentan periódicamente. Como resultado de esta revisión puede proponer la generación o modificación de lineamientos corporativos que pueden afectar a una o a todas las entidades del Conglomerado, según se requiera.	• Conocer el resultado de la Gestión de Seguridad de la Información y Ciberseguridad realizada por parte de las subordinadas directas., mediante un tablero de control. • Conocer los Incidentes de Seguridad de la Información presentados en las entidades y que hayan tenido impacto significativo, reportados por las entidades que conforman la Organización y los planes de acción llevados a cabo para la mitigación de estos.
Comité Ejecutivo de Seguridad de la Información (CESI), aplica para Grupo Aval.	• Informar los acuerdos y decisiones de seguridad de la información y ciberseguridad. • Generar retroalimentación de las jornadas de seguridad y diagnósticos de los SGSI realizados y contribuir a la mejora continua de la postura de seguridad de la información. • Informar principios, directrices y lineamientos de seguridad de la información y ciberseguridad, verificar el desarrollo de proyectos de seguridad de la información y ciberseguridad, velar el nivel de seguridad de la información por medio del análisis de los indicadores y tomar las acciones preventivas y correctivas pertinentes para Grupo Aval • Identificar, evaluar e incluir los requerimientos de seguridad de la información y ciberseguridad en las iniciativas corporativas. • Socializar actividades y proyectos que sean de interés común. • Fomentar el desarrollo de seguridad de la información en Grupo Aval • Aprobar los cambios y homologaciones de la arquitectura de seguridad de la información • Aprobar los planes de acción para mitigar los riesgos identificados por los RES.	• Monitorear el cumplimiento a nivel interno de las Políticas del Sistema de Gestión de Seguridad de la Información y Ciberseguridad en Grupo Aval.

Actor	Actividades	
	De Ejecución	De Supervisión
	• Aprobar el cronograma anual de pruebas de penetración con base en la propuesta elaborada por el área de seguridad TI.	
Vicepresidencia Sénior Corporativa de Riesgo y Cumplimiento (o quien haga sus veces)	• Preparar reportes de seguridad de la información y ciberseguridad para el Comité Ejecutivo y cualquier otro comité que se defina. • Reportar el estado actual del Sistema de Gestión de Seguridad de la Información y Ciberseguridad en las entidades a la Vicepresidencia de Riesgo o quien haga sus veces. • Definir los lineamientos de mejora en los procesos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, en consenso con las entidades. • Cumplir con las demás responsabilidades que sean definidas para la Alta Gerencia.	• Entidades Matrices: Recibir y consolidar información de seguridad de la información y ciberseguridad de sus subordinadas para generar reportes de monitoreo periódicos de acuerdo con el protocolo de comunicación definido. • Mantener actualizados los lineamientos de seguridad de la información y ciberseguridad aprobados por el Comité Corporativo de Seguridad de la Información Grupo Aval - entidades. • Apoyar y aprobar los lineamientos de mejora en los procesos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.
Vicepresidencia Sénior Tecnología de la Información	• Hacer seguimiento a los indicadores de seguridad de ciberseguridad de las entidades. • Definir los lineamientos de ciberseguridad de la tecnología en consenso con las entidades. • Hacer seguimiento a los proyectos de implementación de nuevos controles de ciberseguridad en las entidades. • Apoyar a las entidades en la atención de incidentes de alto impacto y/o transversales en el Grupo. • Convocar al Grupo Ejecutivo de Respuesta de Incidentes cuando sea requerido por algún incidente. • Cumplir con las demás responsabilidades que sean definidas para la Alta Gerencia.	• Entidades Matrices: Recibir y consolidar información de ciberseguridad de sus subordinadas. • Mantener actualizados los lineamientos de ciberseguridad aprobados por el Comité Corporativo de Ciberseguridad de las entidades. • Apoyar y aprobar los lineamientos de ciberseguridad de la tecnología del Grupo.
Líder Seguridad de la Información	• Presentar el informe de Gestión establecido por su entidad Matriz directa • Participar el Comité Ejecutivo de Seguridad de la Información de su entidad. • Adoptar y socializar las mejores prácticas sugeridas en el Comité. • Propiciar la actualización del inventario de riesgos de seguridad de la información y ciberseguridad. • Adoptar los lineamientos establecidos. • Apoyar a la primera línea en el proceso de identificación de riesgos y controles, la determinación de su criticidad y verificación del cumplimiento de los planes de acción establecidos en la gestión de incidentes de seguridad de la información y ciberseguridad.	• Conocer los Incidentes de Seguridad de la Información y las medidas que se han implementado para mitigarlos. • Monitorear el resultado de evaluación de Riesgos. • Definir y monitorear indicadores clave de desempeño sobre la gestión de seguridad de información y ciberseguridad.
Líder de Seguridad TI	• Apoyar al líder de Seguridad de información en la preparación del informe de Gestión establecido por Grupo Aval.	• Analizar los incidentes de alto impacto de Seguridad de la Información y Ciberseguridad reportados por sus subordinadas y los propios e

Actor	Actividades	
	De Ejecución	De Supervisión
	• Participar en el Comité Ejecutivo de Seguridad de la Información de su entidad cuando sea necesario. • Adoptar y socializar las mejores prácticas sugeridas en el Comité. • Informar al líder de Seguridad de Información sobre nuevos riesgos identificados y de manera particular sobre nuevos riesgos de ciberseguridad. • Adoptar los lineamientos establecidos. • Apoyar a la segunda línea en el proceso de identificación de riesgos y controles, así como en su evaluación. • Implementar y operar las herramientas de seguridad TI y ciberseguridad.	implementar los planes de remediación • Velar porque se adopten medidas para responder a los incidentes presentados y para prevenir futuros incidentes. • Adoptar las mejores prácticas vigentes en el mercado con respecto a respuestas a incidentes. • Definir y monitorear indicadores clave de desempeño sobre la gestión de Seguridad TI y Ciberseguridad.
Responsables de la información	• Identificar, clasificar y proteger la información bajo su responsabilidad, conocer los riesgos a los que podría estar expuesta y velar porque se provean los mecanismos necesarios para que estos riesgos se mitiguen a niveles aceptables, considerando costo-beneficio para su área de negocio y la organización. • Conocer los riesgos de Seguridad de Información que le son aplicables. • Con el apoyo de la segunda línea, identificar los controles clave para mitigar los riesgos identificados. • Llevar a cabo la ejecución de los controles para mitigar los riesgos (Autocontrol). • Definir y ejecutar los planes de acción para mitigar los riesgos de seguridad de la información a su cargo. • Reportar a las áreas de Seguridad TI y de seguridad de información, cualquier incidente de seguridad de información y de manera particular cualquier evento material de ciberseguridad.	Vigilar y velar que su equipo de trabajo dé cumplimiento a la política de seguridad y Ciberseguridad.
Auditoría Interna	• Adelantar las pruebas de auditoría que considere apropiadas de acuerdo con el plan de trabajo anual probado por el Comité de Auditoría en cada entidad.	Evaluar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad.

8. DECLARACIÓN DE COMPROMISO

Grupo Aval y sus subordinadas están comprometidos con la Política de Seguridad de la Información y Ciberseguridad, promoviendo una cultura de cumplimiento y control de acuerdo con los principios establecidos por el sistema de gestión de Seguridad de la Información y Ciberseguridad por lo anterior deben:

- Prevenir los daños a la imagen y reputación a través de la adopción y cumplimiento de la Política de Seguridad de la Información y Ciberseguridad.
- Promover continuamente una cultura de seguridad de la información y ciberseguridad.
- Gestionar de manera estructurada y estratégica los riesgos de seguridad de la información y ciberseguridad asociados al negocio y su relacionamiento con terceros.

Cada colaborador, funcionario temporal y tercero, es responsable por aplicar los criterios definidos en esta política y por ajustar sus actuaciones de acuerdo con los valores corporativos

y lineamientos establecidos en seguridad de la información y ciberseguridad, de igual forma es responsable de reportar los incidentes de los que pudiera llegar a tener conocimiento.

9. LINEAMIENTOS GENERALES

La Alta Gerencia de Grupo Aval y sus subordinadas reconocen la importancia de proteger adecuadamente la información de amenazas que puedan afectar la continuidad del negocio, por lo anterior establece el desarrollo de actividades para la protección de los activos de información, gestión y administración de riesgos de Seguridad de la Información y ciberseguridad, protección de datos personales, cultura de seguridad y las conductas que deben adoptar todos los Colaboradores de Grupo Aval y sus subordinadas, por consiguiente, todos los funcionarios temporales y proveedores que en el ejercicio de sus actividades utilicen información y servicios tecnológicos en el Grupo Aval y sus subordinadas deben velar por: el cumplimiento de los requisitos y pilares de la seguridad de la información y ciberseguridad, protegiendo los activos de información de la organización, preservando la confidencialidad, integridad, disponibilidad y privacidad de la información; por lo anterior, Grupo Aval y sus subordinadas acogen las siguientes políticas sobre las cuales se fundamenta y estructura el Sistema de Gestión de Seguridad de la Información (SGSI). Tales Políticas son expresiones de la gerencia para una presentación y valoración justa y transparente de riesgos de seguridad de la información y ciberseguridad. Lo anterior permite hacer una adecuada identificación de los controles que mitigan razonablemente los riesgos identificados.

9.1 Proteger la Confidencialidad, Integridad, Disponibilidad, Privacidad y no repudio de la Información

Todos los Colaboradores de Grupo Aval y sus subordinadas deben proteger y asegurar, la confidencialidad, Integridad, disponibilidad y privacidad de la información, de tal manera que la información:

- ✓ Solo sea accedida por personal autorizado.
- ✓ Sea concisa, precisa, incidiéndose en la exactitud.
- ✓ Esté disponible en el momento que sea requerida.
- ✓ Sea accedida legítimamente y utilizada para lo que se autorizó.

9.2 Adoptar y Mantener una Sólida Cultura de Seguridad de la Información y Ciberseguridad

Las tres líneas deben tomar la iniciativa en el establecimiento de una sólida cultura de seguridad de la información y ciberseguridad donde:

- La primera línea debe ser ejemplo y replicador de una sólida cultura y conciencia en seguridad de la información y ciberseguridad, en el cumplimiento de políticas y procedimientos organizacionales definidos.
- La segunda línea debe definir y ejecutar las actividades de concienciación y cultura, que abarquen a todos los Colaboradores, sobre las políticas y procedimientos organizacionales de seguridad de la información y ciberseguridad.
- La tercera línea debe monitorear la ejecución y el cumplimiento de cultura y concienciación de seguridad de la información y ciberseguridad.

9.3 Implementar y Mantener un Sistema de Gestión Integral de Riesgos de Seguridad de la Información y Ciberseguridad

Todos los Colaboradores de Grupo Aval y sus subordinadas deberá utilizar un marco de control interno generalmente aceptado donde defina los elementos que se espera que estén presentes y funcionando en un sistema de control interno efectivo. Para el efecto se deberá alinear con la metodología corporativa de Administración de Riesgo Operativo - SARO (evaluación riesgo inherente, riesgo residual y mapa de calor) y con las Metodologías Corporativas de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad.

9.4 Determinar el Apetito de Riesgo, el Nivel de Tolerancia y la Capacidad de Riesgo

La Alta Gerencia y la segunda línea de Grupo Aval y sus subordinadas deberán determinar el Apetito de Riesgo, el nivel de tolerancia y la capacidad máxima al riesgo, considerando el efecto de la naturaleza de sus operaciones y líneas de negocio, así como los tipos y niveles de riesgo de seguridad de la información y ciberseguridad que cada entidad están dispuestas a asumir en cada uno de estos niveles. Las Juntas Directivas de las entidades deben aprobar el Apetito de Riesgo, el nivel de tolerancia y la capacidad máxima al riesgo.

9.5 Evaluación de Riesgos de Seguridad de la Información y Ciberseguridad

Grupo Aval y sus subordinadas deben contar con un proceso para identificar, evaluar, documentar, gestionar y mitigar los riesgos de seguridad de la información y ciberseguridad. Este proceso se hace por lo menos una vez al año o cuando circunstancias especiales ocurran, identificando riesgos y evaluando su probabilidad e impacto, el cual debe estar alineado con las metodologías corporativas de gestión de riesgos de seguridad de la información y ciberseguridad.

9.6 Supervisar la Administración del Sistema de Gestión de Seguridad de la Información y Ciberseguridad

La Alta Gerencia y la segunda línea deben establecer, aprobar y revisar periódicamente el “Sistema de Gestión de Seguridad de la Información y Ciberseguridad”, Así mismo, debe supervisar la Administración para asegurarse de que las políticas, procesos y sistemas se aplican eficazmente en todos los niveles de decisión.

9.7 Gestionar el Cambio

La Alta Gerencia y la segunda línea deben asegurar que haya un proceso de aprobación que evalúe plenamente los riesgos de seguridad de la información y ciberseguridad en todos los nuevos procesos, actividades, productos y sistemas críticos, así como que se identifiquen nuevas amenazas. Por ejemplo, cada vez que se realicen cambios sobre alguna aplicación que impacte el negocio, se lleva a un comité de cambios donde se evalúan los posibles riesgos que traería la implementación de dicho cambio.

9.8 Realizar Seguimiento y Presentar Informes

La segunda línea de Grupo Aval y sus subordinadas deben implementar un proceso para monitorear regularmente los perfiles de riesgo de Seguridad de la Información y las exposiciones a pérdidas importantes. Adicionalmente debe realizar un diagnóstico de seguridad de la información basados en normas, estándares y marcos de referencia que respalden la gestión de seguridad de la información y ciberseguridad ISO 27000 y Framework de Ciberseguridad NIST con el fin de calcular el nivel de seguridad y madurez en el que ese encuentra Grupo Aval y las subordinadas, Indicadores Corporativos, Evolución de Riesgos y Evolución de Controles. De manera específica deberán trabajarse en este mismo sentido los riesgos de ciberseguridad.

9.9 Controlar y Mitigar

La primera y segunda línea de Grupo Aval y las subordinadas deben tener un fuerte "ambiente de control", estructurado mediante políticas, procedimientos, estándares, sistemas, controles internos adecuados y la ponderada mitigación o compensación de riesgos.

Con lo anterior, la primera línea de defensa debe contar con controles generales de accesos, privilegios, actualizaciones en los siguientes aspectos mínimos:

- ✓ Supervisión de controles de accesos físicos.
- ✓ Supervisión de controles de accesos lógicos.
- ✓ Supervisión y protección de contraseñas.
- ✓ Supervisión protección de los puertos de configuración y acceso remoto.
- ✓ Restricción de la instalación de aplicaciones por parte del usuario final.
- ✓ Asegurar que los sistemas operativos estén "parchados" con las actualizaciones o en su defecto que los controles implementados mitiguen la posibilidad de materialización de un incidente.
- ✓ Asegurar que las aplicaciones de software se actualicen regularmente.
- ✓ Restricción de los privilegios administrativos (es decir la capacidad de instalar software o cambiar los ajustes de configuración de una computadora).

9.10 Asegurar que el Sistema de Gestión de Seguridad de Información y Ciberseguridad Opera en Situaciones de Contingencia

La segunda línea o Líderes de Seguridad de la Información de Grupo Aval y sus subordinadas deben velar porque en los planes de continuidad del Negocio se incluyan y se implementen los controles necesarios sobre los pilares de la seguridad de la información y ciberseguridad.

9.11 Garantizar el Cumplimiento de la Ley Vigente Aplicable

Es obligación de las tres líneas de Grupo Aval y sus subordinadas dar cumplimiento a todas las normas de los reguladores vigentes que le aplique a cada entidad relacionadas con Seguridad de la Información y Ciberseguridad.

9.12 Seguridad en Nuevas Tecnologías y Riesgos Emergentes

Es importante implementar un plan de seguridad de la información y ciberseguridad, con relación a las nuevas tecnologías. Para monitorear, desarrollar e implementar estrategias de remediación de los riesgos emergentes, donde se debe:

- Establecer políticas de seguridad sobre las tecnologías que se implementen en Grupo Aval y sus subordinadas.
- Adoptar procedimientos de clasificación de la información, gestión y administración de usuarios, definición de responsables y propietarios, de la información que se va a procesar en las nuevas tecnologías para determinar y aplicar los controles de seguridad de la información y ciberseguridad.
- Establecer la gestión y monitoreo de los riesgos cibernéticos y riesgos de terceros que surgen de la implementación de las nuevas tecnologías como lo son los riesgos operacionales, financieros, regulatorios, organizacionales y tecnológicos.
- Incluir en el plan de continuidad del negocio los requisitos y controles de seguridad para reanudar las operaciones orientadas en los sistemas automatizados y servicios digitales.

- Supervisar el cumplimiento del trabajo que desempeñan los sistemas automatizados, asegurando que estos sistemas se adhieran a los requerimientos regulatorios y a las políticas de la organización, en materia de seguridad.

9.13 Modelo de Evaluación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad

Para la identificación de riesgos y la aplicación de controles de seguridad de la información y ciberseguridad, Grupo Aval y sus subordinadas adoptan y dan a conocer el modelo de evaluación de seguridad de la información y ciberseguridad. Este modelo tiene como propósito evaluar el nivel de madurez del sistema de gestión de seguridad de la información e identificar las oportunidades de mejora que permitan fortalecerlo, basados en los dominios y controles propuestos en la norma NTC-ISO 27001:2013 y en el Framework de Ciberseguridad NIST.

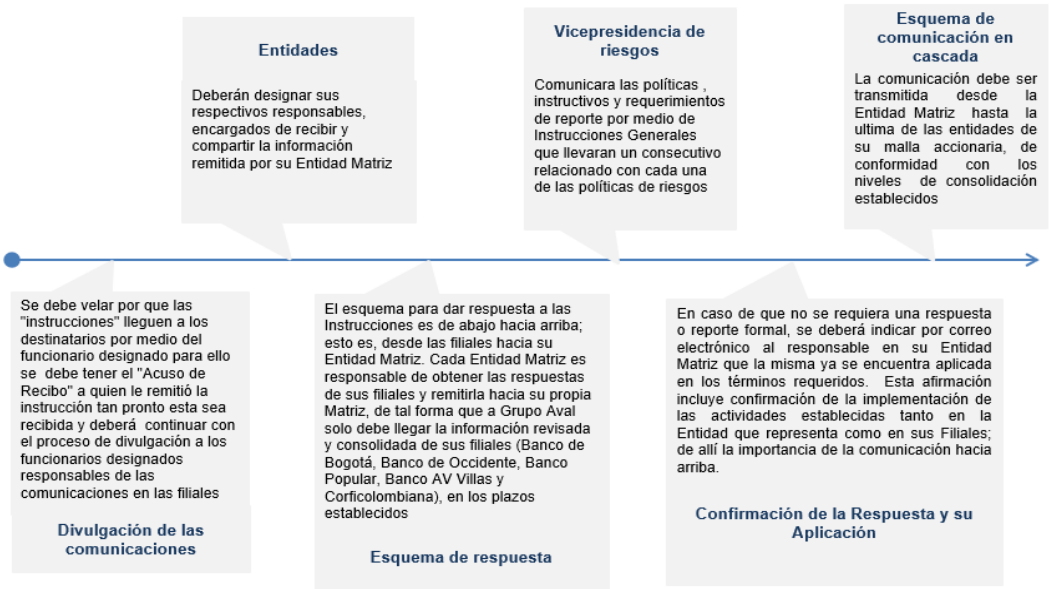
9.14 Comunicación Líderes de Seguridad de la Información

Para propender por la estandarización de la aplicación del cumplimiento de la presente política en todo el Grupo, se establecerá como mecanismo de información oficial los siguientes:

Instrucciones Generales, donde incluirá actividades, por lo general metodológicas, Previa evaluación, análisis y acuerdo con los especialistas competentes de cada una de las entidades el Equipo Seguridad de la Información Corporativo (Grupo Aval) emite instrucción general a Presidentes, Líderes de Seguridad de la Información y cuando aplique dueños de proceso de los cuatro bancos, Corficolombiana y Porvenir. Estos a su vez divulgan la Instrucción General a sus pares de las filiales respectivas y algunas veces a otras áreas de interés según se indique en la Instrucción. Lo anterior en cumplimiento del protocolo de comunicación definido por la Vicepresidencia Sénior Corporativa de Riesgos y Cumplimiento de Grupo Aval.

Conceptos, son aclaraciones o ampliación de información, útiles para dar cumplimiento las instrucciones generales, generalmente comunicaciones por medio de correo electrónico institucional. El Equipo Seguridad de la Información Corporativo emite conceptos a los Líderes de Seguridad de la Información de los cuatro bancos, Corficolombiana y Porvenir, así como filiales adicionales en casos especiales, y éstos a su vez divulgan los conceptos a los Líderes de Seguridad de la Información de las filiales respectivas siguiendo el protocolo de comunicación.

Dentro del proceso de comunicación corporativo Grupo Aval y sus subordinadas ha establecido el protocolo de comunicación con el fin de que la información emitida llegue a los niveles requeridos de manera clara y oportuna, así:



9.15 Reportes

Con el fin de facilitar el monitoreo de cumplimiento, serán solicitados diferentes reportes de gestión que constituyan un efectivo apoyo para la administración; éstos deberán ser veraces, comprensibles, completos y oportunos.

Así mismo, las subordinadas deberán informar a Grupo Aval aquellos incidentes seguridad de la información y ciberseguridad que hayan afectado de manera significativa la confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad en el momento en que estos sucedan, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlos. Adicionalmente cada entidad deberá tener una base de datos consolidada de incidentes de seguridad de la información y ciberseguridad clasificada en tipo de incidente, impacto y plan de remediación, así como, que este reporte se encuentre protegido dada la sensibilidad de esta información.

9.16 Capacitación y Entrenamiento

Dentro del proceso de inducción de un Colaborador nuevo y al menos anualmente para la totalidad de los Colaboradores debe realizarse una capacitación y/o actualización sobre seguridad de la información y ciberseguridad. La capacitación y entrenamiento se puede brindar en forma continua, virtual o presencial a los Colaboradores de Grupo Aval y sus subordinadas, con el propósito de fortalecer los conceptos y asegurar la continuidad y sostenibilidad de Sistema de Gestión de Seguridad de la Información. Cada entidad deberá evaluar la necesidad de sensibilizar en seguridad de la información a sus proveedores críticos que acceden a los activos de información.

9.17 Investigaciones y Sanciones

Grupo Aval y sus subordinadas reconocen que en el evento de incumplimiento de esta política y demás actividades que se deriven de ella, las entidades y las personas responsables por su incumplimiento podrán ser objeto de acciones disciplinarias por parte de Grupo Aval de acuerdo con las políticas internas de la entidad relacionadas con el manejo de Incidentes de

Seguridad de la Información. Lo anterior, sin perjuicio de la eventual responsabilidad que pudiera derivarse por el incumplimiento de la normatividad aplicable a Seguridad de la Información.

9.18 Aplicación a Grupo Aval Acciones y Valores S. A.

Esta política Corporativa de Seguridad de la Información y Ciberseguridad aplica a Grupo Aval. Cualquier excepción será documentada y soportada por la Vicepresidencia Senior Corporativa de Riesgo y Cumplimiento.