

1. OBJETIVO

Definir los lineamientos para el Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI) en Grupo Aval Acciones y Valores S.A. y sus subsidiarias (Grupo), con el fin de preservar los pilares de seguridad de la información: confidencialidad, integridad, disponibilidad y privacidad de los activos de información, asegurando el cumplimiento de los requisitos normativos, legales y regulatorios.

2. ALCANCE

Aplica al Grupo, así como a colaboradores temporales y proveedores que, en el ejercicio de sus funciones, utilicen información y servicios tecnológicos y quienes deberán adoptar esta política conforme a la naturaleza, tamaño, complejidad, apetito de riesgo y estructura de sus operaciones.

3. DECLARACIÓN DE COMPROMISO

El Grupo está comprometido con la implementación de esta política, la cual se fundamenta en la gestión estructurada y estratégica de los riesgos asociados al negocio y al relacionamiento con sus proveedores, así como en la prevención de posibles daños a su imagen y reputación.

4. LINEAMIENTOS

Generales

Los siguientes lineamientos aplican al Grupo y orientan la gestión de la seguridad de la información y la ciberseguridad:

- Proteger sus activos ante posibles amenazas, vulnerabilidades, eventos e incidentes que puedan afectar la seguridad de la información.
- Promover la formación continua y la responsabilidad individual en el manejo de la información.
- Garantizar relaciones seguras con los proveedores y gestionar los riesgos de seguridad de la información y ciberseguridad asociados a su cadena de suministros, exigiendo el cumplimiento de estándares de seguridad de la información y promoviendo la gestión colaborativa de los riesgos compartidos.
- Adoptar tecnologías emergentes con un enfoque seguro, evaluando los riesgos desde la fase de diseño y asegurando la protección de los datos a lo largo de todo su ciclo de vida.
- Asegurar la aplicación de los requisitos de seguridad de la información y ciberseguridad en la continuidad del negocio y la recuperación ante desastres apalancándose en la estrategia de resiliencia.
- Establecer el marco general para la gestión del SGSI, asegurando su alineación con los requerimientos del negocio, los lineamientos definidos en la presente política y las disposiciones legales y normativas aplicables.
- Establecer los lineamientos para la protección homogénea de la información, considerando la valoración y clasificación de los activos críticos de información y los niveles de riesgo asociados a estos.
- Establecer con base en el análisis de riesgos, las estrategias y los proyectos la implementación de controles que preserven los pilares de información.

- Implementar la metodología de la gestión de riesgos, que deben comprender las siguientes etapas: identificación, medición, monitoreo y control. Este proceso se debe hacer por lo menos una vez al año o cuando ocurran circunstancias especiales.
- Implementar un proceso para monitorear regularmente los perfiles de riesgos y las exposiciones a pérdidas importantes.
- Realizar diagnósticos de seguridad de la información basados en normas, estándares y/o marcos de referencia reconocidos que respalden la gestión de seguridad de la información y ciberseguridad, por la norma ISO 27001/IEC y Framework de Ciberseguridad NIST, con el fin de evaluar el nivel de seguridad y madurez en el que se encuentran las entidades.
- Dar cumplimiento a las regulaciones vigentes aplicables a cada entidad en materia de seguridad de la información y ciberseguridad.
- Cumplir con el protocolo de comunicación de la Vicepresidencia Corporativa de Riesgos y Cumplimiento, utilizando mecanismos como instrucciones generales y conceptos.
- Cumplir con el envío oportuno de los reportes requeridos para el monitoreo del SGSI, de acuerdo con las fechas establecidas y el protocolo de comunicaciones definido por la Vicepresidencia Corporativa de Riesgos y Cumplimiento.
- Informar de manera inmediata a Grupo Aval sobre cualquier incidente de seguridad de la información y ciberseguridad que pueda afectar o haya afectado la confidencialidad, integridad, disponibilidad o privacidad de la información de la entidad. Esta notificación deberá realizarse conforme a los criterios de clasificación y severidad establecidos por la estructura del Grupo Ejecutivo de Respuesta a Incidentes (GERI), asegurando su oportuno escalamiento.
- Mantener una base de datos consolidada y actualizada de todos los incidentes de seguridad de la información y ciberseguridad y los relacionados con la afectación de datos personales, dando aplicación al pilar de privacidad de la información, clasificada según el tipo de incidente y/o evento de seguridad, el nivel de impacto y el plan de remediación implementado. Así mismo, la gestión de dichos incidentes deberá incluir análisis de causa raíz, lecciones aprendidas y seguimiento a los planes de remediación. Esta base de datos deberá estar adecuadamente etiquetada y/o protegida, garantizando la confidencialidad y sensibilidad de la información contenida, y permitiendo una gestión eficaz de los riesgos asociados.
- Desarrollar y ejecutar de forma periódica planes de cultura de seguridad de la información y ciberseguridad, y estrategias de comunicación dirigidas a los colaboradores.
- Evaluar y gestionar los riesgos asociados al uso de tecnologías emergentes, incluyendo soluciones basadas en Inteligencia Artificial (IA), asegurando que su utilización se realice bajo criterios de seguridad de la información y ciberseguridad, protección de datos, cumplimiento regulatorio y uso responsable de la información.
- Establecer indicadores con sus respectivos límites para el monitoreo del Sistema de Riesgo de Seguridad de la Información y Ciberseguridad.

Protección de la confidencialidad, integridad, disponibilidad, privacidad y no repudio de la información

- Mantener la información protegida mediante controles mínimos aceptables de acuerdo con el apetito de riesgo de cada entidad.
- Implementar mecanismos de validación, verificación continua y tecnologías que fortalezcan la inalterabilidad de los datos.
- Garantizar la accesibilidad de la información y los servicios en el momento requerido, mediante estrategias de resiliencia como monitoreo proactivo, la recuperación ante desastres y la escalabilidad.

- Proteger los datos personales tanto en procesos manuales como automatizados, así como en análisis masivos mediante tecnologías emergentes, asegurando transparencia, consentimiento, tratamiento de datos de acuerdo con su ciclo de vida y protección frente a sesgos, conforme a principios éticos y normativos.
- Contar con registros y evidencias trazables de cada transacción o interacción con la información, mediante el uso de mecanismos como firmas digitales o tecnologías que garanticen la autenticidad, integridad y responsabilidad de las acciones realizadas.

Implementar y mantener el Sistema de Gestión de Riesgos

- Utilizar como marco de control interno el modelo COSO (Committee on Sponsoring Organizations of the Treadway Commission), en coherencia con la Política de Gestión Integral, asegurando su adecuada implementación y funcionamiento.
- Adoptar un enfoque sistemático, estructurado y dinámico, que permita la mejora continua del sistema, la toma de decisiones informadas y la asignación eficiente de recursos.
- Implementar y mantener un proceso de gestión de riesgos de terceros que contemple la identificación, medición, monitoreo y control de los riesgos asociados a los proveedores y a sus cadenas de suministro, de acuerdo con su nivel de criticidad e impacto en la Entidad.
- Gestionar el riesgo de seguridad de la información y ciberseguridad conforme al apetito de riesgo, el nivel de tolerancia y la capacidad máxima, considerando la naturaleza de las operaciones y líneas de negocio.

Gestionar el cambio

- Asegurar la existencia de un proceso de gestión de cambios que incorpore principios de seguridad por diseño y por defecto, contemplando la identificación de amenazas, así como la evaluación, clasificación y mitigación de los riesgos de seguridad de la información y ciberseguridad asociados a cambios en procesos, canales, productos, servicios, aplicaciones y sistemas de información críticos. Este proceso debe estar alineado con la metodología de gestión de riesgos establecida e integrado a un esquema de revisión y aprobación de cambios, donde se evalúe y defina el tratamiento de los riesgos derivados.

Controlar y mitigar

- Contar con un ambiente de control alineado con el modelo COSO, estructurado mediante políticas, procedimientos, estándares, sistemas, así como roles y responsabilidades claramente definidos.
- Implementar un proceso continuo de gestión de vulnerabilidades que incluya su identificación, análisis, priorización y tratamiento, garantizando una remediación oportuna.
- Realizar simulacros periódicos de ciberseguridad que contemplen escenarios como ataques de denegación de servicio (DDoS), ransomware, malware y ataques a servicios en la nube, entre otros. Estos deberán articularse con los planes de continuidad del negocio y de recuperación ante desastres, así como con el Protocolo Corporativo de Gestión de Incidentes de Ciberseguridad administrado por Aval Valor Compartido (AVC), e incluir la validación de la recuperación de los servicios críticos, la continuidad del negocio, la efectividad de los planes de respuesta y la capacidad de restablecimiento frente a incidentes de ciberseguridad.

- Asegurar la capacidad de recuperación oportuna de los servicios y activos de información ante incidentes de seguridad de la información y ciberseguridad, conforme a los lineamientos corporativos establecidos.

Seguridad en nuevas tecnologías y riesgos emergentes

- Establecer políticas o lineamientos de seguridad para la adopción y uso de nuevas tecnologías, considerando los riesgos asociados.
- Adoptar procedimientos de identificación, clasificación, gestión y administración de usuarios de los activos críticos de la información (joyas de la corona), así como la definición de responsables y propietarios de la información, que permitan determinar y aplicar los controles de seguridad en el uso de nuevas tecnologías.
- Incorporar la seguridad desde las etapas iniciales de diseño y desarrollo, mediante la aplicación de principios de seguridad, así como la implementación de medidas de monitoreo, detección y recuperación posteriores al despliegue para garantizar la resiliencia.
- Establecer la gestión y monitoreo de los riesgos cibernéticos y riesgos de proveedores que surgen de la implementación de las nuevas tecnologías.
- Garantizar que los ambientes utilizados para la continuidad del negocio cuenten con controles mínimos de seguridad de la información, equivalentes a los establecidos para los ambientes productivos, con el fin de minimizar la exposición a vulnerabilidades y proteger la información durante escenarios de contingencia de acuerdo con los lineamientos corporativos.
- 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.

4.1 INVESTIGACIONES Y SANCIONES

El Grupo reconoce que cualquier incumplimiento a esta política, así como a las actividades y procedimientos relacionados con la seguridad de la información y Ciberseguridad, será objeto de una investigación exhaustiva para determinar las causas y responsabilidades correspondientes.

5. ROLES Y RESPONSABILIDADES

El Grupo debe estructurar de manera integral las funciones y responsabilidades asociadas a la gestión de riesgos, conforme al modelo de las tres líneas, considerando: (i) la gestión ejercida por cada línea de negocio, (ii) la gestión de las áreas de riesgo y cumplimiento, y (iii) la función de revisión independiente de la administración, en concordancia con lo establecido en la Política Integral para la Gestión de Riesgos y Cumplimiento.

En este contexto, y para dar cumplimiento a los objetivos de esta política, se han definido los siguientes actores clave en la gestión de seguridad de la información y ciberseguridad:

Junta Directiva de las entidades u órgano que haga sus veces

Sin perjuicio de las funciones asignadas en otras disposiciones es responsabilidad de la Junta Directiva u órgano que haga sus veces:

- Aprobar la Política de Seguridad de la Información y Ciberseguridad y sus actualizaciones.
- Proveer los recursos necesarios para la adecuada gestión del SGSI.

- Conocer y pronunciarse respecto de los informes de gestión del SGSI.
- Pronunciarse sobre la evaluación periódica de Seguridad de la Información y Ciberseguridad, que realicen los órganos de control.
- Impartir, cuando lo considere pertinente, las directrices para el mejoramiento de la Gestión de Seguridad de la Información y Ciberseguridad.
- Participar en programas de concientización y capacitación en el SGSI.

Comité de Riesgos y Delegado de Ciberseguridad de la Junta Directiva de Grupo Aval Acciones y Valores S.A.

- Realizar el seguimiento a los resultados de la gestión de seguridad de la información y ciberseguridad y emitir las correspondientes recomendaciones cuando resulte necesario.
- Recomendar a la Junta Directiva las acciones correctivas y/o de mejora sobre los temas de Seguridad de la información y Ciberseguridad, cuando se prevea la posible materialización de riesgos que puedan impactar a Grupo Aval o a sus entidades subordinadas.
- Presentar a la Junta Directiva los resultados acciones correctivas y/o de mejora tomadas cuando por su materialidad se considere necesario.

Alta Gerencia de las entidades

- Evaluar el nivel de madurez y monitoreo de las políticas propuestas del SGSI.
- Evaluar los informes que presenten los líderes de Seguridad de la Información y Ciberseguridad sobre los resultados de la evaluación de efectividad del programa de seguridad de la información y ciberseguridad, las propuestas de mejora en materia de ciberseguridad y los incidentes relevantes que hayan afectado 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 sobre la totalidad de los activos de información.
- Fortalecer la cultura de seguridad de la información en los colaboradores que administren activos de información, así como promover la sensibilización en proveedores críticos con acceso a dichos activos.
- Supervisar la gestión de la seguridad de la información y ciberseguridad, asegurando la adecuada comprensión y gestión de los riesgos asociados.
- Asegurar, a través de la segunda línea, la existencia de un proceso de aprobación de cambios que incorpore principio de seguridad por diseño y seguridad por defecto.
- Para Grupo Aval acciones y Valores S.A. liderar el Grupo Ejecutivo Respuesta Incidente de Seguridad de la Información (GERI).

Comité Ejecutivo de Seguridad de la Información (CESI) de Grupo Aval Acciones y Valores S.A.

- Aprobar el Manual de Seguridad de la Información y Ciberseguridad y sus actualizaciones.
- Verificar la gestión de Seguridad de la Información y Ciberseguridad, velando por el cumplimiento de los lineamientos impartidos desde este Comité.
- Analizar y aprobar la ejecución de las iniciativas o requerimientos para la implementación de las estrategias de Seguridad de la Información y Ciberseguridad.
- Impartir lineamientos de Seguridad de la Información y Ciberseguridad para los colaboradores.

- Conocer, apoyar y velar por el desarrollo de Seguridad de la Información y Ciberseguridad.

Comité Corporativo de Seguridad de la Información (Grupo Aval y entidades)

El Comité Corporativo de Seguridad de la Información está conformado por Grupo Aval y sus principales entidades. Desde Grupo Aval, la Dirección Senior de Cumplimiento son quienes actúan como secretarios. Los representantes de las entidades en este comité serán los Oficiales Responsables de Seguridad de la Información, sus deliberaciones y conclusiones del comité son registradas en actas.

Quorum deliberatorio y decisorio

Habrà quorum para deliberar y decidir cuándo se encuentre presente la mayoría simple de sus miembros.

Funciones:

- Definir principios, directrices y lineamientos corporativos.
- Tomar las acciones preventivas y correctivas pertinentes para los temas que surjan en las Entidades del Grupo.
- Identificar, evaluar e incluir los requerimientos en las iniciativas corporativas realizadas para las entidades, desde el punto de vista de gestión de riesgo.
- Socializar actividades y proyectos que sean de interés común y/o impacten a las entidades para la gestión de riesgos.
- Centralizar el análisis de situaciones particulares de riesgo para evaluar su impacto.
- Evaluar anualmente o cuando se requiera los riesgos y la metodología de calificación.

Vicepresidencia Corporativa de Riesgo y Cumplimiento de Grupo Aval Acciones y Valores S.A.

- Presentar a aprobación de la Junta Directiva y divulgar la Política de Seguridad de la Información y Ciberseguridad que permita la adecuada gestión del riesgo.
- Reportar el estado actual del Sistema de Gestión de Seguridad de la Información al Comité de Riesgos de Junta Directiva de Grupo Aval en temas que sean considerados de mayor relevancia.
- Definir, promover y apoyar 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.

Vicepresidencia Corporativa de Tecnología Grupo Aval Acciones y Valores S.A.

- Definir, promover y apoyar la aprobación de los lineamientos de ciberseguridad asociados a la tecnología del Grupo, en coordinación con las entidades.
- Mantener actualizados los lineamientos de ciberseguridad aprobados por el Comité Corporativo de Ciberseguridad.
- Hacer seguimiento a los indicadores de seguridad de la información y ciberseguridad del Grupo.
- Hacer seguimiento a los proyectos de implementación de nuevos controles de ciberseguridad del Grupo.
- Apoyar la atención de incidentes de seguridad de la información y ciberseguridad de alto impacto y/o de carácter transversales en el Grupo.
- Convocar al Grupo Ejecutivo de Respuesta de Incidentes sea requerido por algún incidente.

- Recibir y consolidar la información de ciberseguridad de sus subsidiarias.
- Reportar el estado actual de Ciberseguridad al Comité de Riesgos de Junta Directiva de Grupo Aval en temas que sean considerados de mayor relevancia.
- Cumplir con las demás responsabilidades que sean definidas por la Alta Gerencia.

Líder de Seguridad de la Información en las entidades y en Grupo Aval

- Participar en el Comité Ejecutivo de Seguridad de la Información de su entidad y adoptar y socializar las mejores prácticas definidas en este.
- Presentar los reportes e informes de gestión establecidos por Grupo Aval Acciones y Valores S.A, así como aquellos que se hayan determinado por su casa matriz o al interior de la entidad.
- Propiciar la actualización del inventario de riesgos de seguridad de la información y ciberseguridad.
- Adoptar los lineamientos establecidos en esta política y demás lineamientos corporativos, en materia de seguridad de la información y ciberseguridad.
- 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 definidos para la gestión de incidentes de seguridad de la información y ciberseguridad.
- Conocer los incidentes de seguridad de la información, así como las medidas implementadas para su mitigación.
- Monitorear los resultados de la evaluación de riesgos.
- Definir y monitorear indicadores clave de desempeño para la gestión de seguridad de información y ciberseguridad.
- Reportar a la Vicepresidencia Corporativa de Riesgos y Cumplimiento, o quien haga sus veces, el estado actual del SGSI.

Líder de Ciberseguridad en las entidades y en Grupo Aval

- Apoyar al Líder de Seguridad de la información en la preparación del informe de gestión establecido por Grupo Aval Acciones y Valores S.A.
- Participar en el Comité Ejecutivo de Seguridad de la Información de su entidad cuando sea requerido, y adoptar y socializar las mejores prácticas definidas en este.
- Informar al Líder de Seguridad de la Información de la entidad sobre nuevos riesgos identificados y de manera particular sobre nuevos riesgos de ciberseguridad.
- Adoptar los lineamientos establecidos en esta política y demás lineamientos corporativos, en materia de seguridad de la información y ciberseguridad.
- 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.
- Analizar los incidentes de seguridad de la información y ciberseguridad de alto impacto, tanto propios como reportados por sus subsidiarias, e implementar los planes de remediación correspondientes.
- 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 en las entidades y en Grupo Aval

- Identificar, clasificar y proteger la información bajo su responsabilidad, conocer los riesgos a los que está expuesta y asegurar la implementación de mecanismos que permitan su mitigación a niveles aceptables, considerando criterios de costo-beneficio para el área de negocio y la organización.
- Conocer los riesgos de seguridad de información y ciberseguridad que aplican a su gestión.
- Identificar, con el apoyo de la segunda línea, los controles clave para mitigar los riesgos identificados.
- Ejecutar los controles definidos para la mitigación de los riesgos, en el marco del autocontrol.
- Definir y ejecutar los planes de acción para mitigar los riesgos de seguridad de la información y ciberseguridad a su cargo.
- Reportar a las áreas de seguridad de la información y ciberseguridad cualquier incidente de seguridad de la información, en especial los eventos materiales de ciberseguridad.
- Supervisar que su equipo de trabajo cumpla con la política de seguridad de la información y ciberseguridad.

Auditoría Interna (quien haga sus veces) en las entidades y en Grupo Aval

- 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 del Grupo.
- Evaluar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad.

6. REGULACIÓN

El Grupo debe cumplir con la regulación vigente en materia de seguridad de la información y ciberseguridad, tanto a nivel nacional como internacional, cuando resulte aplicable; entre ellas se incluyen:

- Leyes: 527 de 1999, 1266 de 2008, 1273 de 2009, 1581 de 2012, 1978 de 2019 y 2300 de 2023.
- Ley Sarbanes-Oxley – SOX.
- Decretos: 1377 de 2013 y 338 de 2022.
- Circular Básica Jurídica de la Superintendencia Financiera de Colombia.
- Cualquier otra aplicable.

Mejores Prácticas

- ISO/IEC 2700:2018 e ISO/IEC 27001:2022
- Framework de Ciberseguridad NIST
- El Grupo deberá considerar el cumplimiento de los requisitos normativos, legales y regulatorios aplicables al uso de tecnologías emergentes, incluyendo Inteligencia Artificial (IA), en materia de seguridad de la información, protección de datos personales y gestión de riesgos.
- Cualquier otra aplicable

7. GLOSARIO

Administración: presidente, vicepresidentes de Grupo Aval y sus subsidiarias, o quienes hagan sus veces.

Área: Seg.Información	Código: GRC-PO-Seg.Info.-2	Versión: 4
-----------------------	----------------------------	------------

Alta Gerencia: es la persona o grupo de personas con responsabilidad por la conducción de las operaciones de la entidad. Para algunas entidades en ciertas jurisdicciones, la Gerencia incluye algunas o todas aquellas personas que tienen relación con la gobernabilidad; por ejemplo, los miembros de la Junta Directiva.

Amenaza: causa potencial de un incidente no deseado que puede provocar daño a un sistema, organización.

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.

Confidencialidad: hace referencia a la protección de información cuya divulgación no está autorizada.

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.

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: 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.

Incidente: 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.

Integridad: la información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

Inteligencia artificial (IA): tecnología que permite a los sistemas informáticos realizar tareas que normalmente requieren inteligencia humana, mediante el análisis de datos, automatización de decisiones o generación de contenido.

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

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.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información. 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.

Sistema de Gestión de Seguridad de la Información y Ciberseguridad: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Subsidiarias: corresponde a las entidades del Grupo Aval, dentro de las cuales se destacan como sus principales unidades de negocio el Banco de Bogotá, Banco de Occidente, Banco AV Villas, Banco Popular, Corficolombiana, Porvenir, Aval Fiduciaria, AVC, GOU Payments y Aval Casa de Bolsa.

Vulnerabilidad: debilidad de una organización que potencialmente permite que una amenaza afecte a un activo, 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.