Resolución No. SB-2021-2126 - "Norma de Control para la Gestión del Riesgo Operativo"

Cumplimiento al 02 de marzo de 2022 (3 meses)

Artículo	Tema
18.2	**ARTÍCULO 18.- Administración de la Continuidad de Negocio.-** Las entidades controladas deben establecer, implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio, para garantizar su capacidad de operar de forma continua y limitar las pérdidas en caso de una interrupción grave del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya; mismo que debe contemplar eventos internos y externos, así como, las estrategias para la continuidad del negocio, de manera que contribuya a la resiliencia operativa de la entidad; por lo cual, debe contar con, al menos, con lo siguiente, pero sin limitarse a estos: **2.** La entidad debe contar con una persona o área responsable de la gestión de la continuidad de negocio, acorde al tamaño y complejidad de la entidad, que dirija el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de continuidad del negocio de la entidad. El responsable debe tener la capacitación o formación, y experiencia en el ramo.
25.1	**ARTÍCULO 25.-** Con el objeto de gestionar la seguridad de la información, para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las entidades controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya, y cumplir con las disposiciones legales y normativas vigentes en el país en esta materia; por lo cual, debe contar, al menos, con lo siguiente pero sin limitarse a: 1. Funciones y responsables de las actividades de la seguridad de la información claramente definidos, que permitan establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información, acorde al tamaño y complejidad de la entidad. Las funciones deben estar segregadas para gestionar los riesgos relacionados con la seguridad de la información.
25.4	4. Un oficial de seguridad de la información, quien es el responsable del área de seguridad de la información.
27.11 (parte modificada)	**ARTÍCULO 27.-** Con el objeto de que las transacciones realizadas a través de canales electrónicos cuenten con los controles y mecanismos para evitar el cometimiento de eventos fraudulentos o no autorizados por los usuarios y preservar la seguridad de la información, así como los recursos de los clientes a cargo de las entidades controladas; estas deben cumplir, como mínimo, con lo siguiente: 11. Requerir mecanismos de autenticación fuerte para el registro y modificación de la información referente a su número de telefonía móvil y correo electrónico, cuando los clientes los realicen por cualquier canal no presencial o presencial, en cuyo caso, deberá enviarse una notificación a los datos de contacto tanto anteriores como nuevos. La entidad deberá mantener las evidencias respectivas de dichos cambios.
27.13 (claves de tarjetas)	13. Incorporar en los procedimientos de administración de seguridad de la información la renovación de, por lo menos, una vez al año de las claves de acceso a los canales electrónicos y claves de tarjetas; las claves de banca electrónica y banca móvil deben ser diferentes de aquella por la cual se accede a otros canales electrónicos.
27.16 (gestión de tarjetas)	16. Las entidades controladas deben mantener sincronizados todos los relojes de sus sistemas de información incluidos aquellos que gestionan tarjetas y los dispositivos que estén involucrados con el uso de canales electrónicos.
27.23 (parte modificada)	23. Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de estos, incluyendo los montos máximos permitidos y los mecanismos para actualizar estos parámetros.
30.24 (parte modificada)[1]	**ARTÍCULO 30.- Banca electrónica.-** Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las entidades controladas que ofrezcan servicios por medio de este canal electrónico deben cumplir, como mínimo, con lo siguiente:

[1] El presente artículo solo tiene hasta numeral 8, por lo cual la referencia es inexacta. Ningún numeral ha sido modificado, excepto el 8.

Cumplimiento el 31 de marzo de 2022

Artículo	Tema
23	**ARTÍCULO 23.-** La entidad controlada debe generar planes y programas que le permitan dar cumplimiento a las disposiciones emanadas en la Ley Orgánica de Protección de Datos Personales.

Cumplimiento al 02 de junio de 2022 (6 meses)

Artículo	Tema
4 (primer inciso)	**ARTÍCULO 4.-** En el marco de la administración integral de riesgos, las entidades controladas definirán políticas, procesos, procedimientos y metodologías para la administración del riesgo operativo como un riesgo específico; y, definirán y adoptarán un modelo basado en el esquema de tres líneas de defensa, considerando su objeto social, tamaño, naturaleza, complejidad de sus operaciones y demás características propias: a) **Primera línea de defensa.-** Áreas del negocio y operativas, responsables del diseño y evaluación de sus controles y la implementación de acciones preventivas y correctivas para hacer frente a las deficiencias de personas, procesos y tecnología de la información. b) **Segunda línea de defensa.-** Áreas especializadas que tienen la función de monitorear y hacer contraposición de los controles diseñados y evaluados en la primera línea y el monitoreo de la evolución de los riesgos operativos. c) **Tercera línea de defensa.-** Área de control cuya función es asegurar de forma independiente y objetiva, las prácticas del gobierno y de la administración de riesgos operativos en cada línea de defensa.
10	**ARTÍCULO 10.-** Las entidades controladas deben definir una política de comunicación formal sobre los eventos de riesgo operativo que deban informar interna o externamente y que esté sujeta a revisión periódica, en función de las estrategias organizacionales. Además, deben implementar un proceso para evaluar el impacto de la información a comunicar en función a su gestión de riesgos.
16 (segundo inciso)	**ARTÍCULO 16.- Eventos externos.-** (…) La gestión de los riesgos relacionados con eventos externos debe formar parte de la administración de la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio.
18 (primer inciso)	**ARTÍCULO 18.- Administración de la Continuidad de Negocio.-** Las entidades controladas deben establecer, implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio, para garantizar su capacidad de operar de forma continua y limitar las pérdidas en caso de una interrupción grave del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya; mismo que debe contemplar eventos internos y externos, así como, las estrategias para la continuidad del negocio, de manera que contribuya a la resiliencia operativa de la entidad; por lo cual, debe contar con, al menos, con lo siguiente, pero sin limitarse a estos: 1. Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: un miembro del directorio, quien lo presidirá, el representante legal de la entidad, los funcionarios responsables de las unidades de: riesgos, tecnología de la información, seguridad de la información, talento humano, y, el responsable de la continuidad del negocio quien actuará como secretario. Los representantes de cada una de las áreas relacionadas con los procesos críticos de la entidad y auditoría interna participarán con voz ~~sin voto~~. El representante legal podrá delegar su participación solamente a quien le subrogue estatutariamente en sus funciones. En caso de ausencia temporal o definitiva del miembro del directorio de la entidad del sector financiero público, el comité será presidido por el representante legal, en cuyo caso esta presidencia no será delegable. El comité de continuidad del negocio expedirá un reglamento en donde se establezcan, como mínimo, el objetivo, sus funciones y responsabilidades. Las reuniones de este comité se realizarán, al menos, trimestralmente, o cuando se las requiera. El comité de continuidad del negocio debe dejar evidencia de las decisiones adoptadas, las cuales deben ser conocidas y aprobadas por el comité de administración integral de riesgos.

	El comité de continuidad del negocio debe tener, al menos, las siguientes responsabilidades, pero sin limitarse a: a) Evaluar y supervisar el sistema de gestión de continuidad del negocio; b) Monitorear la implementación del plan de continuidad del negocio y asegurar el alineamiento de este con la metodología de administración de la continuidad del negocio; c) Proponer para la revisión y aceptación del comité de administración integral de riesgos, el plan de continuidad del negocio y sus actualizaciones; d) Revisar el presupuesto del plan de continuidad del negocio y ponerlo en conocimiento del comité de administración integral de riesgos; e) Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y, f) Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad del negocio.
19.1	**ARTÍCULO 19.-** El marco de referencia del sistema de gestión de continuidad del negocio debe contener, al menos, lo siguiente, pero sin limitarse a: 1. Alcance del sistema de gestión de continuidad en términos del negocio que considere los procesos críticos.
19.2	2. Políticas, estrategias, objetivos, procesos, procedimientos, metodologías, planes operativos y presupuesto para la administración de la continuidad del negocio, que deben ser revisados y aceptados por el comité de continuidad del negocio; y, propuestos por el comité de administración integral de riesgos, para la posterior aprobación del directorio. Esta documentación debe ser difundida y comunicada a todo el personal involucrado, de tal forma que se asegure su cumplimiento.
19.3	3. Funciones y responsables de las actividades de continuidad de las operaciones, que permitan cumplir con el criterio de resiliencia para la disponibilidad de las operaciones, acorde al tamaño y complejidad de los procesos administrados por el negocio.
24.6 (primer inciso)	**ARTÍCULO 24.-** Para mantener el control de los servicios provistos por terceros. incluidas las empresas de servicios auxiliares del sistema financiero, las entidades controladas deben implementar un proceso integral para la administración de proveedores de servicios que incluya las actividades previas a la contratación, suscripción, cumplimiento y renovación del contrato; para lo cual, deben cumplir, por lo menos, con lo siguiente, pero sin limitarse a: 6. Para el caso de contratación de servicios de infraestructura, plataforma y/o software, conocido como computación en la nube, las entidades controladas deben identificar y gestionar los riesgos asociados a estos servicios; adicionalmente, deben: a) Informar a la Superintendencia de Bancos sobre el detalle de los servicios asociados a los procesos críticos a ser contratados que incluya entre otros: el tipo de servicio contratado, el detalle del servicio alojado, la arquitectura tecnológica contratada, la elasticidad en tiempo real, según aplique; el análisis de los riesgos operativos, legales, tecnológicos, de seguridad y continuidad a los que se exponen al adoptar este servicio; así como los controles para mitigarlos; b) Los centros de procesamiento de datos principal y/o alterno, contratados en la nube deben haber sido implementados siguiendo el estándar TIA-942 o superior y contar como mínimo con la certificación TIER III o su equivalente para diseño, implementación y operación y así garantizar la disponibilidad de los servicios brindados; c) El proveedor de servicios en la nube debe contar, para los servicios ofertados, como mínimo, con certificación ISO 27001 en seguridad de la información, así como, la implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube), ISO 27018 (protección de información personal en la nube) y/o aquella que aplique conforme el servicio ofertado; d) Contar con informes de auditorías de seguridad relacionadas con el servicio contratado, con base en el perfil de riesgo del proveedor de servicios en la nube, por lo menos una (1) vez al año, con el fin de identificar amenazas y vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que brindan. Los procedimientos de auditoría deben ser ejecutados por personas o empresas especializadas en seguridad de la información en la nube e independientes al proveedor, aplicando estándares vigentes y reconocidos a nivel internacional. El proveedor de servicios en la nube debe definir y ejecutar planes de acción para gestionar las vulnerabilidades detectadas; y, e) Los acuerdos o contratos que suscriba la entidad controlada con el proveedor de servicios en la nube, adicional a los establecidos en la presente sección de esta norma, deben contemplar entre otros aspectos los siguientes:

	e.1 La información proporcionada por la entidad controlada no puede ser utilizada para ningún propósito diferente al establecido en los contratos, inclusive bajo el modelo de subcontrataciones; **e.2** La entrega a la entidad controlada de informes y certificaciones que demuestren la calidad, desempeño y efectividad en la gestión de los servicios contratados, así como la vigencia de las certificaciones enunciadas en el presente artículo; y, **e.3** Borrado seguro de los datos en los medios de almacenamiento cuando finalice el contrato, cuando lo solicite la entidad controlada o cuando el proveedor de servicios en la nube elimine y/o reemplace dichos medios.
26.2 (tercer inciso)	**ARTÍCULO 26.-** Las entidades controladas deben establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información que incluya, al menos, lo siguiente, pero sin limitarse a: 2. (…) La entidad controlada debe asegurar mecanismos para que sus empleados cumplan con lo establecido en el sistema de seguridad de la información, así como, proporcionar la capacitación y actualizaciones periódicas relacionadas con el mismo.
26.3	3. Inventario de activos de información acorde al alcance del sistema de gestión de seguridad de la información con, al menos, su clasificación en términos de: valor en función de la pérdida, daño o deterioro que supone un riesgo para la consecución de los objetivos de la entidad, requerimientos legales, propietario, custodio y ubicación.
26.11.c	11. Para considerar la existencia de un apropiado ambiente de gestión de seguridad de la información, la unidad responsable de la seguridad de la información debe establecer y controlar la implementación, con las áreas correspondientes de, al menos, lo siguiente, pero sin limitarse a: c) Procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios. Además, se deberá controlar la eliminación de la información crítica en las bases de datos o repositorios de los proveedores de la entidad después de que presten sus servicios.
26.11.p	p) Procedimientos de difusión, comunicación, entrenamiento y concienciación del sistema de gestión de seguridad de la información, a las partes interesadas internas y externas, según corresponda.
27.2 (para la gestión de tarjetas)	**ARTÍCULO 27.-** Con el objeto de que las transacciones realizadas a través de canales electrónicos cuenten con los controles y mecanismos para evitar el cometimiento de eventos fraudulentos o no autorizados por los usuarios y preservar la seguridad de la información, así como los recursos de los clientes a cargo de las entidades controladas; estas deben cumplir, como mínimo, con lo siguiente: 2. Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como, en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos y para la gestión de tarjetas, de tal manera que, se garantice permanentemente la seguridad; se debe generar informes trimestrales dirigidos al comité de seguridad de la información.
27.4 (para la gestión de tarjetas)	4. Realizar como mínimo una vez al año, o cuando la situación lo amerite, una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por canales electrónicos y para la gestión de tarjetas; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad, se deberá efectuar una prueba adicional. Las pruebas de vulnerabilidad y penetración deben ser efectuadas por personas natural o jurídica independientes a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las entidades deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas. Los informes de las pruebas de vulnerabilidad deben estar a disposición de la Superintendencia de Bancos, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior.
27.19 (parte modificada)	19. Las entidades controladas deben poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) u otro medio, para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana; a través de este centro de atención se podrá suspender, bloquear o cancelar el uso de los servicios de canales electrónicos y/o tarjetas con el respectivo procedimiento de seguridad y autenticación del cliente.
27.21 (parte modificada)	21. Las entidades controladas deben enviar a sus clientes mensajes en línea, a través de mensajería móvil y correo electrónico u otro mecanismo, de manera simultánea, notificando la ejecución de transacciones monetarias realizadas mediante cualquiera de los canales electrónicos disponibles y/o mediante cualquier medio de pago.

29 (primer inciso)	**ARTÍCULO 29.- Puntos de venta (POS y PIN Pad).-** Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los dispositivos de puntos de venta, las entidades controladas deben sujetarse a las medidas de seguridad dispuestas en canales electrónicos y banca electrónica de esta norma, en lo que aplique; y, cumplir, como mínimo, con lo siguiente: 1. Establecer procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta (POS y PIN Pad) en los establecimientos comerciales confirmen su identidad a fin de asegurar que este personal cuenta con la debida autorización. 2. A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones monetarias efectuadas a través de los dispositivos de puntos de venta (POS o PIN Pad), éstos deben permitir establecer sus comunicaciones de forma inalámbrica segura.

Cumplimiento al 02 de septiembre de 2022 (9 meses)

Artículo	Tema
4 (último inciso-primera evaluación)	**ARTÍCULO 4.-** (3 líneas de defensa) Las entidades controladas deben asegurar que se realicen, de forma continua, evaluaciones integrales del riesgo operativo, de proyectos en curso y nuevos productos.
6 (segundo inciso)	Las entidades controladas deben implementar mecanismos de cuantificación periódica sobre los eventos de pérdidas producidos por este tipo de riesgos, que permitan reevaluar la declaración de tolerancia institucional ante el riesgo operativo.
14.2	**ARTÍCULO 14.- Factor Personas.-** Las entidades controladas deben administrar el capital humano de forma que les permita gestionar los riesgos asociados a este factor. Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las entidades controladas deben: 2. La entidad controlada debe asegurar que se mantengan actualizados los acuerdos de confidencialidad relacionados con los procesos que ejecuta el empleado y los riesgos asociados a las funciones que desempeña.
14.3	3. La entidad controlada debe determinar responsabilidades y deberes de seguridad de la información que permanezcan vigentes después del cambio de funciones o de la terminación de la relación laboral, conforme lo establecido en el acuerdo de confidencialidad.
17	**ARTÍCULO 17.-** Las entidades controladas deben desarrollar e implementar planes de respuesta y recuperación para gestionar los incidentes con relación a los aspectos definidos en esta norma, que puedan afectar el normal funcionamiento de sus servicios, especialmente, de sus servicios críticos en línea con la tolerancia al riesgo definida por la entidad, conforme a mejores prácticas de la industria, de manera que contribuya a la resiliencia operativa de la entidad; para lo cual, las entidades controladas deben considerar, al menos, lo siguiente pero sin limitarse a: 1. Asignar un gestor de incidentes, quien deberá encargarse de la trazabilidad hasta finalizar la atención de los incidentes; y, su respectivo registro en la base de conocimiento. 2. Establecer políticas, procesos, procedimientos y metodologías para la gestión de incidentes, que puedan afectar a los factores de riesgo operativo. 3. La gestión de incidentes debe abarcar el ciclo de vida del incidente, que incluya entre otros: registro, priorización en función de la gravedad, análisis, escalamiento, solución, monitoreo, lecciones aprendidas y reporte a las partes interesadas tanto internas como externas. 4. Ejecutar pruebas controladas de gestión de incidentes. 5. Mantener una base de conocimiento de respuesta a incidentes y recuperación que incluya recursos internos y de terceros, según aplique, para respaldar las capacidades de respuesta y reanudación de los servicios. Los procedimientos asociados deben revisarse, probarse y actualizarse periódicamente por las áreas involucradas; además, deben identificar y mitigar las causas fundamentales para evitar la repetición en serie de incidentes. Las entidades controladas deben comunicar a la Superintendencia de Bancos los incidentes que afecten a sus servicios críticos, conforme a las disposiciones emitidas por el organismo de control.
19.8	**ARTÍCULO 19.-** El marco de referencia del sistema de gestión de continuidad del negocio debe contener, al menos, lo siguiente, pero sin limitarse a:

	8. Procedimientos de pruebas del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o, al menos, una vez al año; las pruebas deben incluir el alcance y el detalle de los aspectos a probar, así como las conclusiones y recomendaciones obtenidas como resultado de su ejecución. Además, la entidad debe monitorear, evaluar y verificar que se mantengan actualizados los planes de contingencia y/o continuidad de las compañías contratadas que soportan los servicios críticos de la entidad, y que estos sean debidamente probados con la intención de precautelar los servicios brindados e incluirlos dentro de las pruebas anuales de continuidad de la entidad. El resultado de las pruebas debe ser comunicado a las instancias correspondientes.
19.9	9. Procedimientos para monitorear, medir y evaluar el desempeño y eficacia del sistema de gestión de la continuidad del negocio.
19.12	12. La entidad debe mantener una base de conocimiento de las lecciones aprendidas en función del resultado de las pruebas realizadas al plan de continuidad del negocio, eventos de continuidad materializados, debilidades encontradas en las revisiones efectuadas por la administración de la continuidad del negocio, entre otros.
20.10	**ARTÍCULO 20.- Plan de continuidad del negocio.-** Las entidades controladas deben contar con un plan de continuidad del negocio que considere como mínimo lo siguiente, pero sin limitarse a: 10. Las entidades que tengan dependencia tecnológica y/u operativa con su matriz en el exterior deben tener su plan de continuidad local, conforme la presente norma, y deberá estar correlacionado con las estrategias del plan de continuidad de su casa matriz.
24.2.L	**ARTÍCULO 24.-** Para mantener el control de los servicios provistos por terceros. incluidas las empresas de servicios auxiliares del sistema financiero, las entidades controladas deben implementar un proceso integral para la administración de proveedores de servicios que incluya las actividades previas a la contratación, suscripción, cumplimiento y renovación del contrato; para lo cual, deben cumplir, por lo menos, con lo siguiente, pero sin limitarse a: 2. Establecer políticas, procesos y procedimientos que aseguren la contratación de servicios en función de los requerimientos de la entidad controlada, y garanticen que los contratos incluyan, como mínimo, las siguientes cláusulas: L) Informes de auditoría externa sobre el cumplimiento de los aspectos relacionados con la seguridad de la información y continuidad del negocio referidos en la presente norma, practicados por personal o empresas independientes con experiencia acreditada en el ramo.
24.6.c	6. Para el caso de contratación de servicios de infraestructura, plataforma y/o software, conocido como computación en la nube, las entidades controladas deben identificar y gestionar los riesgos asociados a estos servicios; adicionalmente, deben: c. El proveedor de servicios en la nube debe contar, para los servicios ofertados, como mínimo, con certificación ISO 27001 en seguridad de la información, así como, la implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube), ISO 27018 (protección de información personal en la nube) y/o aquella que aplique conforme el servicio ofertado;
24.6.d	d. Contar con informes de auditorías de seguridad relacionadas con el servicio contratado, con base en el perfil de riesgo del proveedor de servicios en la nube, por lo menos una (1) vez al año, con el fin de identificar amenazas y vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que brindan. Los procedimientos de auditoría deben ser ejecutados por personas o empresas especializadas en seguridad de la información en la nube e independientes al proveedor, aplicando estándares vigentes y reconocidos a nivel internacional. El proveedor de servicios en la nube debe definir y ejecutar planes de acción para gestionar las vulnerabilidades detectadas; y,
26.5	**ARTÍCULO 26.-** Las entidades controladas deben establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información que incluya, al menos, lo siguiente, pero sin limitarse a: 5. Metodología de gestión de riesgos de seguridad de la información, mediante la cual, se identifique los niveles de protección que necesitan cada activo de información de manera que permita preservar los criterios de confidencialidad, integridad y disponibilidad del activo de información; la metodología deberá considerar las definiciones de apetito y tolerancia de riesgo de la entidad controlada y algún elemento adicional que se considere necesario para alinear la metodología de gestión de riesgo de seguridad de la información a la metodología de la gestión del riesgo operativo.
26.10	10. Ejecución de auditorías externas orientadas a evaluar la seguridad de la información, que incluya aspectos del sistema de gestión de seguridad de la información y de ciberseguridad, por lo menos, una (1) vez al año, o cuando la situación lo amerite, con el fin de identificar opciones de mejora y mitigar los riesgos que podrían afectar a la presentación de la confidencialidad, integridad y disponibilidad de la información. Los procedimientos

	de auditoría deben ser ejecutados por personal independiente a la entidad, formado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional.
26.11.a	11. Para considerar la existencia de un apropiado ambiente de gestión de seguridad de la información, la unidad responsable de la seguridad de la información debe establecer y controlar la implementación, con las áreas correspondientes de, al menos, lo siguiente, pero sin limitarse a: a) Procedimientos para el manejo de activos de la información, que deben desarrollarse e implementarse de acuerdo con el esquema de clasificación adoptado por la entidad.