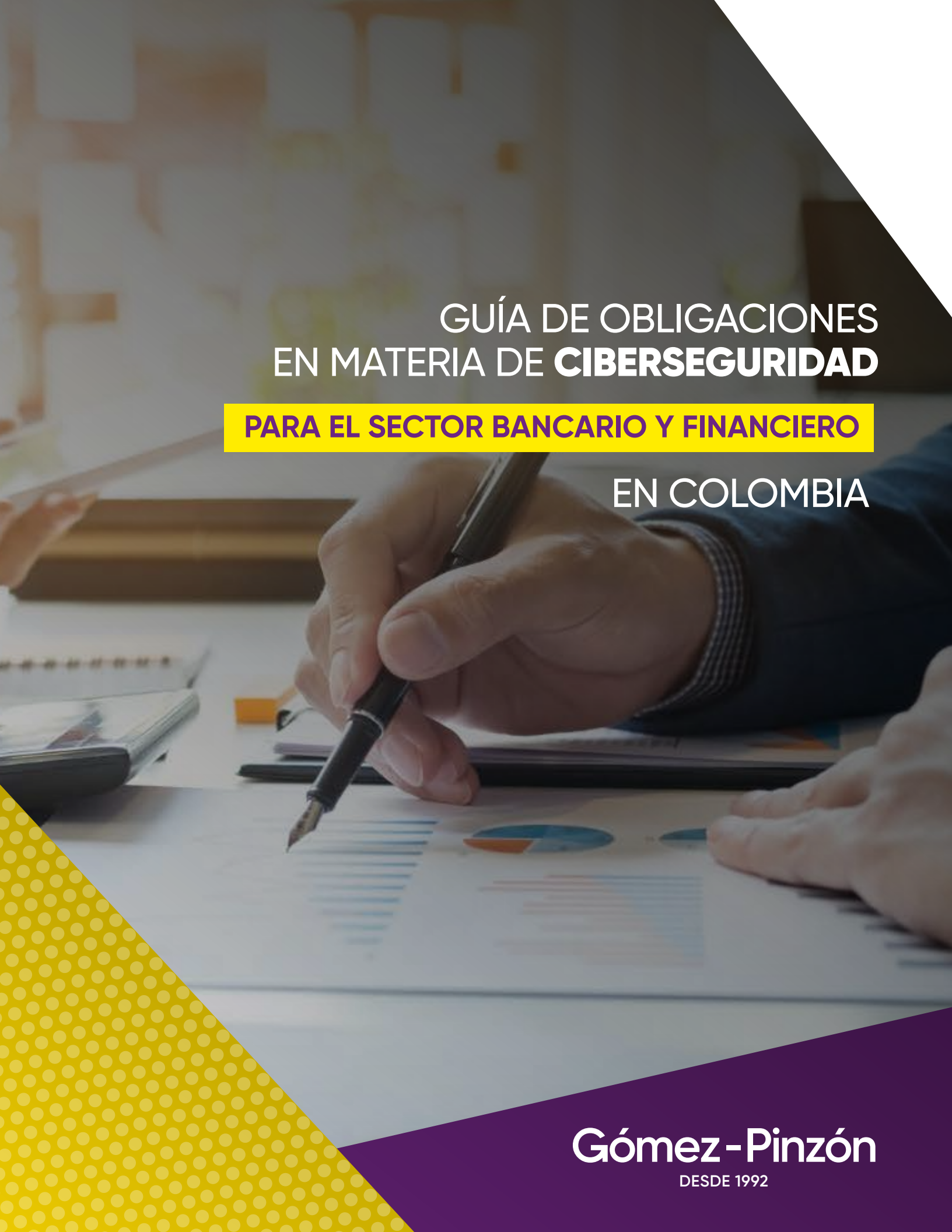


GUÍA DE OBLIGACIONES EN MATERIA DE **CIBERSEGURIDAD**

PARA EL SECTOR BANCARIO Y FINANCIERO

EN COLOMBIA

Gómez-Pinzón

DESDE 1992

Introducción:

Uno de los activos más importantes que tienen las instituciones financieras son los datos de sus consumidores. Este activo les ha permitido entender más acerca de sus propios negocios, así como lograr direccionar sus productos y servicios a audiencias más proclives al consumo. Sin embargo, de la mano de la optimización del uso de la información también se han desarrollado las técnicas para el acceso no autorizado a la misma, así como su robo.

Debido a los riesgos físicos y tecnológicos a los que se enfrentan las empresas de los diferentes sectores, la regulación sectorial ha establecido obligaciones en materia de seguridad de la información para mitigar su acceso no autorizado. En ese sentido, la no adopción de estándares de seguridad de la información no solo representa un riesgo para la empresa en cuanto al robo de data valiosa, sino también una fuente de incumplimiento normativo que da lugar a sanciones.

De ese modo, entendiendo esta pluralidad de riesgos en materia de seguridad de la información, en esta sección abordará las principales obligaciones que deben cumplir las entidades financieras en esta materia y sus respectivas sanciones.

Obligaciones:

1. Obligaciones en materia de seguridad y calidad de la información para la realización de operaciones

1.1 Para garantizar la confidencialidad, integralidad, disponibilidad, efectividad, eficiencia y confiabilidad de la información, todas las entidades vigiladas por la Superintendencia Financiera de Colombia -SFC-, salvo las entidades exceptuadas, enunciadas en el numeral 1.7. de esta sección, deben cumplir con las siguientes obligaciones:

- Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad (Subnumeral 2.3.3.1.1., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Gestionar la seguridad de la información, para lo cual pueden tener como referencia el estándar ISO 27000, o el que lo sustituya, entre otras obligaciones (Subnumeral 2.3.3.1.2., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

1.2 En la tercerización de sus servicios, todas las entidades vigiladas por la SFC, salvo las entidades exceptuadas, enunciadas en el numeral 1.7. de esta sección, tienen la obligación de:

- Celebrar contratos en los que delimiten los niveles de servicio y operación; contemplen cláusulas de confidencialidad frente a la información manejada; propiedad de la información; restricciones sobre el software empleado; normas de seguridad informática y física a ser aplicadas; procedimientos ante la alteración o manipulación de dispositivos o información; y procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez terminado el servicio, entre otras obligaciones (Subnumeral 2.3.6., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

1.3 En la implementación y uso de biometría como factor de autenticación[2] electrónica, todas las entidades vigiladas por la SFC, salvo las entidades exceptuadas, enunciadas en el numeral 1.7. de esta sección, tienen la obligación de:

- Verificar la identidad del cliente contra las bases de datos de la Registraduría Nacional del Estado Civil, los operadores de servicios ciudadanos digitales o de identidad digital autorizados, o contra sus propias bases de datos (Subnumeral 2.3.9., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Establecer controles en la captura inicial de las muestras biométricas de los clientes que aseguren que la información se obtenga directamente del titular del dato, entre otras obligaciones (Subnumeral 2.3.9.5., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC Jurídica de la SFC).

- Almacenar las plantillas biométricas utilizando sistemas de tokenización o algoritmos de cifrado fuertes como AES256, RSA, 3DES o superiores, al usar sus bases de datos propias (Subnumeral 2.3.9., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Adoptar en el almacenamiento de esta información estándares de seguridad de datos biométricos como ISO 24741:2007 y 24745:2011 (Subnumeral 2.3.9.1., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

1.4 Dependiendo del tipo de canal que utilicen (internet, banca móvil, operaciones por medio de códigos QR y prestación de nuevos canales), todas las entidades vigiladas por la SFC, salvo las entidades exceptuadas enunciadas en el numeral 1.7. de esta sección, deberán cumplir con obligaciones específicas, como se referirá a continuación.

Internet

Cuando las entidades ofrezcan la realización de operaciones por Internet tendrán la obligación de:

[2] La autenticación refiere a un conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario. Los factores de autenticación son: algo que se sabe, algo que se tiene, algo que se es (Subnumeral 2.2.6.1., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC Jurídica de la SFC).

- Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura (Subnumeral 3.4.9.1., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC Jurídica de la SFC).

- Realizar como mínimo 2 veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de operaciones monetarias por este canal (Subnumeral 3.4.9.2., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC Jurídica de la SFC).

- Implementar mecanismos que permitan verificar constantemente que no sean modificados los enlaces (links) de su sitio web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS, entre otras obligaciones (Subnumeral 3.4.9.6., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

Banca móvil

Cuando las entidades ofrezcan la realización de operaciones por medio de la banca móvil[3] tendrán la obligación de:

- Contar con mecanismos de autenticación de 2 factores para la realización de operaciones monetarias y no monetarias, entre otras obligaciones (Subnumeral 3.4.11.1., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Operaciones por medio de códigos QR[4]

Las entidades que ofrezcan la realización de pagos utilizando códigos QR tendrán la obligación de:

- Tener como referencia el estándar internacional para aceptar pagos EMVCo LLC, versión 1.0 EMV® QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode, emitido en julio de 2017, o aquellos que lo modifiquen, sustituyan o adicionen (Subnumeral 2.3.4.13., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

[3] La Banca móvil se entiende como el canal en el cual el dispositivo móvil es utilizado para realizar operaciones bien sea asociando su número de línea al servicio, o empleando apps (aplicaciones informáticas diseñadas para ser ejecutadas en teléfonos celulares, tabletas y otros dispositivos móviles). Sin embargo, los servicios que se presten a través de dispositivos móviles y utilicen navegadores Web, son considerados banca por internet." (Subnumeral 3.4.11.1., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

[4] El código QR (Quick Response Code): Es un código de respuesta rápida, bidimensional, con estructura cuadrada. Tiene la capacidad de almacenar datos codificados, es de fácil lectura y tiene mayor capacidad de almacenamiento que los códigos universales de productos (UPC por sus siglas en inglés) o códigos de barras. Puede ser estático (su contenido no cambia, generalmente impreso) o dinámico (cambia su contenido para cada compra, generado por software en tiempo real) (Subnumeral 2.2.11., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Gestionar los riesgos que se puedan derivar de la realización de este tipo de operaciones, entre otras obligaciones (Subnumeral 2.3.4.13.4., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Prestación de servicios a través de nuevos canales

Las entidades que decidan iniciar la prestación de servicios a través de canales diferentes a los que tiene en uso tienen la obligación de:

- Adelantar un análisis de riesgos del nuevo canal. Dicho análisis debe ser puesto en conocimiento de la junta directiva y los órganos de control.

- Remitir a la SFC, con al menos 15 días calendario de antelación a la fecha prevista para el inicio de la distribución de servicios a través del nuevo canal, entre otras obligaciones (Subnumeral 2.3.4.10., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

1.5 Obligaciones en materia de seguridad y calidad de la información para establecimientos de crédito

Particularmente, los establecimientos de crédito tienen la obligación de

- Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes y definir procedimientos para la confirmación oportuna de las operaciones monetarias que no correspondan a sus hábitos (Subnumeral 2.1. y 2.3.3.1.13, Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Cifrar y evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados cuando envíen información entre oficinas y los sitios centrales de las entidades, entre otras obligaciones (Subnumeral 2.3.4.1.5., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

1.6 Obligaciones en materia de seguridad y calidad de la información establecimientos de crédito, los administradores de sistemas de pago de bajo valor, las sociedades especializadas en depósitos y pagos electrónicos y las entidades vigiladas que permitan la ejecución de órdenes electrónicas para la transferencia de fondos, la compra, venta o transferencia de títulos valores y la emisión de pólizas de seguros, por sistemas de acceso remoto para clientes, Internet o dispositivos móviles

Estas entidades son las únicas que tienen la obligación de:

- Implementar análisis de sus vulnerabilidades en materia de seguridad de la información para lo que deben generar de manera automática por lo menos 2 veces al año un informe consolidado de las vulnerabilidades encontradas, así como deben tomar las medidas para remediarlas (Subnumeral 2.3.7. Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Usar herramientas homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización en el análisis de vulnerabilidades, entre otras obligaciones (Subnumeral 2.3.7.5., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

1.7 Obligaciones de las entidades exceptuadas.

Las entidades exceptuadas de las anteriores obligaciones, es decir, Fondo Nacional de Garantías-FNG-, Fondo de Garantías de Instituciones Financieras -FOGAFÍN-., Fondo de Garantías de Entidades Cooperativas-FOGACOOP-, Fondo Financiero de Proyectos de Desarrollo-FONADE-, los Almacenes Generales de Depósito, los Fondos de Garantía que se constituyan en el mercado de valores, los Fondos Mutuos de Inversión, las Sociedades Calificadoras de Valores y/o Riesgo, las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior, los Corredores de Seguros y de Reaseguros, los Comisionistas Independientes de Valores, las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación, tienen la obligación de:

- Proteger la información cuya divulgación no está autorizada (Subnumeral 2.3.1.1., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Manejar la información de manera integral, de modo que sea precisa, coherente y completa desde su creación hasta su destrucción. (Subnumeral 2.3.1.2., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Propender por la disponibilidad de la información de modo que esté en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso (Subnumeral 2.3.1.3., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Garantizar la pertinencia de la información lo que implica su entrega oportuna, correcta y consistente (Subnumeral 2.3.2.1., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

- Velar por que el procesamiento y suministro de información se haga utilizando de la mejor manera posible los recursos (Subnumeral 2.3.2.2., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).
- Propender porque la información se apropiada para la administración de la entidad y el cumplimiento de sus obligaciones (Subnumeral 2.3.2.3., Capítulo I, Titulo II, Parte I, Circular Básica Jurídica de la SFC).

2. Obligaciones en materia de seguridad de la información y la ciberseguridad[5]

2.1 En materia de seguridad de la información y la ciberseguridad, todas las entidades vigiladas por la SFC, salvo las entidades exceptuadas, enunciadas en el numeral 2.3. de esta sección, tienen la obligación de contar con un sistema integral de gestión del riesgo de ciberseguridad que deberá incluir:

- Una política que contenga los principios, procedimientos y lineamientos para la gestión de la seguridad de la información y riesgo de ciberseguridad en la entidad (Subnumeral 3.1., Capítulo V, Titulo IV, Parte I, Circular Básica Jurídica de la SFC).
- Una unidad al interior de la entidad que gestione los riesgos de seguridad de la información y la ciberseguridad (Subnumeral 3.2., Capítulo V, Titulo IV, Parte I, Circular Básica Jurídica de la SFC).
- Contar con un sistema de gestión para la ciberseguridad, para lo cual se pueden tomar como referencia el estándar ISO 27032, NIST con sus publicaciones SP800 y SP1800, ISF (Information Security Forum), CIS Critical Security Controls (CSC) o Cobit 5 for Information Security, y sus respectivas actualizaciones (Subnumeral 3.3., Capítulo V, Titulo IV, Parte I, Circular Básica Jurídica de la SFC).
- Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito, entre otras obligaciones (Subnumeral 3.4., Capítulo V, Titulo IV, Parte I, Circular Básica Jurídica de la SFC).

[5] La ciberseguridad refiere al 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 (Subnumeral 2.6., Capítulo V, Titulo IV, Parte I, Circular Básica Jurídica de la SFC).

2.2 Para gestión de la seguridad de la información y la ciberseguridad todas las entidades vigiladas por la SFC, salvo las exceptuadas, enunciadas en el numeral 2.3. de esta sección, tienen la obligación de:

- Prever medidas en materia prevención; protección y detección de eventos que puedan comprometer la ciberseguridad de la organización; respuesta y comunicación de los mismos; y recuperación y aprendizaje de dichos eventos (Subnumeral 4, Capítulo V, Titulo IV, Parte I, Circular Básica Jurídica de la SFC).

2.3 Las entidades exceptuadas, es decir, el Fondo Nacional de Garantías (FNG), Fondo Financiero de Proyectos de Desarrollo (FONADE), los Almacenes Generales de Depósito, los Fondos de Garantía que se constituyan en el mercado de valores, los Fondos Mutuos de Inversión, los Fondos Ganaderos, las Sociedades Calificadoras de Valores y/o Riesgo, las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior, los Corredores de Seguros y de Reaseguros, los Comisionistas Independientes de Valores, las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación, tienen la obligación de:

- Hacer periódicamente una autoevaluación del riesgo de ciberseguridad y seguridad de la información, que incluya una identificación de las mejoras a implementar en su Sistema de Administración de Riesgo Operativo (SARO), entre otras obligaciones (Subnumeral 1, Capítulo V, Titulo IV, Parte I, Circular Básica Jurídica de la SFC).

- Mantener los resultados de la autoevaluación, así como el plan de acción para implementar los ajustes a que nube haya lugar a disposición de la SFC (Subnumeral 1, Capítulo V, Titulo IV, Parte I, Circular Básica Jurídica de la SFC).

3. Obligaciones en materia de uso de servicios computacionales en la nube

Todas las entidades sometidas a la inspección y vigilancia de la SFC pueden soportar todos sus procesos y actividades en servicios computacionales en la nube para ello tendrán la obligación de:

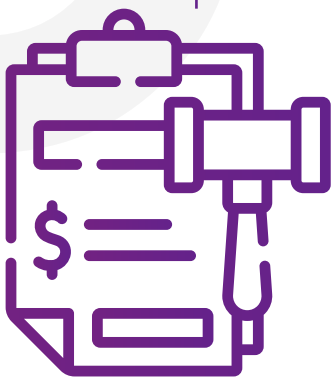
- Contemplar dentro de su SARO la gestión efectiva de los riesgos derivados de la utilización de servicios computacionales en la nube. (Subnumeral 3.1., Capítulo VI, Título I, Parte I, Circular Básica Jurídica de la SFC)

- Suscribir acuerdos o contratos que contemplen la existencia de planes de continuidad; resolución de incidentes; condiciones de seguridad de la información y ciberseguridad de los servicios en la nube y las condiciones establecidas para proteger la privacidad y confidencialidad de los datos de los clientes; y la obligación del proveedor del servicio de informar, en cuanto le sea posible, a la entidad vigilada sobre cualquier evento o situación que pudiera afectar significativamente la prestación del servicio (Subnumeral 4, Capítulo VI, Título I, Parte I, Circular Básica Jurídica de la SFC).

- Verificar que el proveedor de servicios en la nube cuente y mantenga vigente, al menos, la certificación ISO 27001, y de observancia a los estándares o buenas prácticas, tales como ISO 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (SOC1, SOC2, SOC3), entre otros (Subnumeral 3.4., Capítulo VI, Título I, Parte I, Circular Básica Jurídica de la SFC)

Posibles Sanciones:

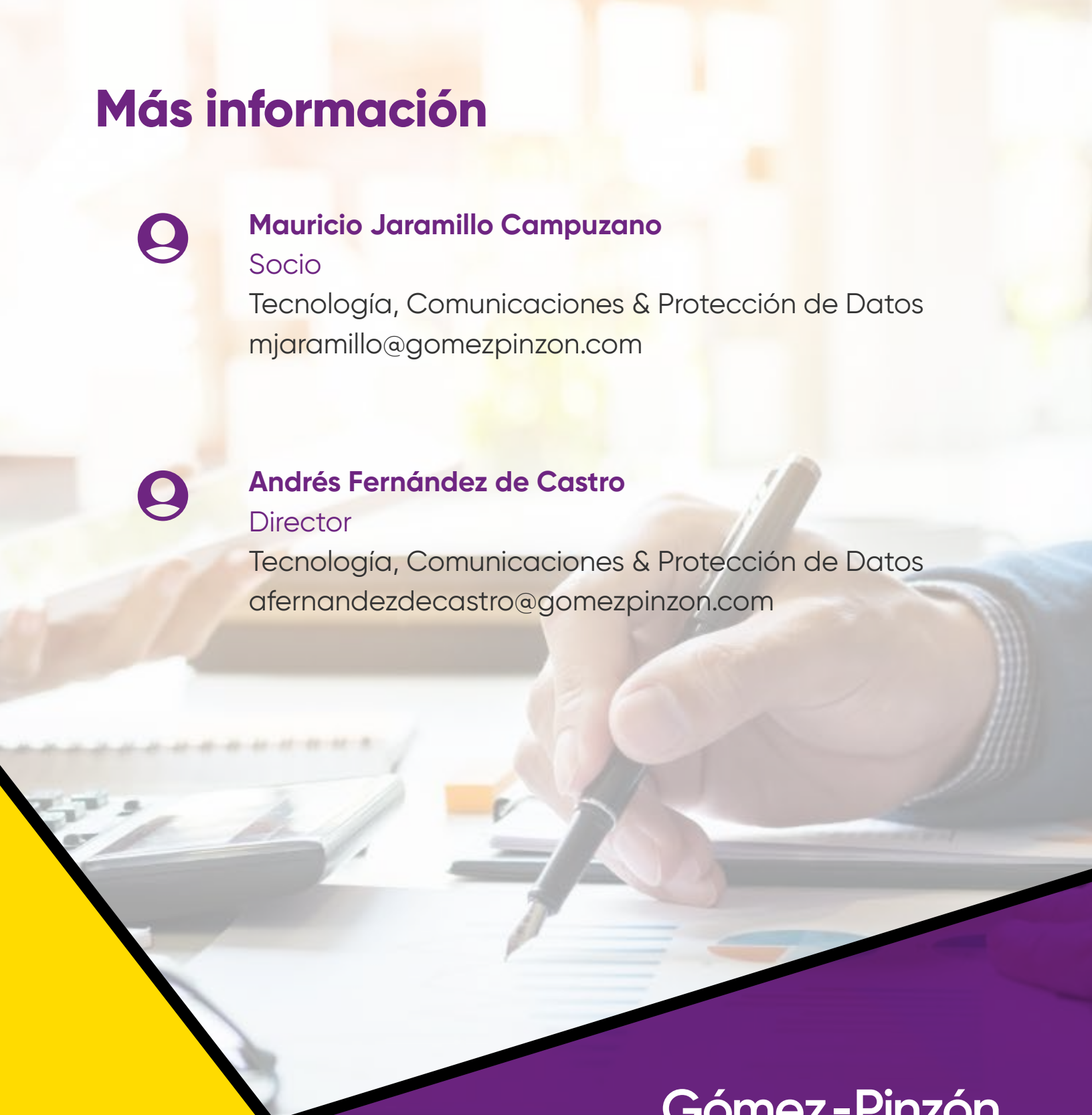
El incumplimiento de estas obligaciones puede acarrear la imposición de sanciones por parte de la SFC a sus entidades vigiladas, así como a los directores, administradores, representantes legales, revisores fiscales u otros funcionarios o empleados de estas. Entre ellas se destacan amonestaciones, clausura de las oficinas, multas personales hasta de COP$ 296.588.569 e institucionales COP$ 1.488.107.392 por parte de la SFC representación (Artículo 208, 209, 210 Estatuto Orgánico del Sistema Financiero) y por la SIC, por violación de las normas de protección de datos personales hasta de 2.000 SMLMV, entre otros (Artículo 23, Ley 1581 de 2012 y Artículo 18 Ley 1266 de 2008).



Más información

Mauricio Jaramillo Campuzano
Socio
Tecnología, Comunicaciones & Protección de Datos
mjaramillo@gomezpinzon.com

Andrés Fernández de Castro
Director
Tecnología, Comunicaciones & Protección de Datos
afernandezdecastro@gomezpinzon.com



Gómez-Pinzón
DESDE 1992

Canal GP 30
Gómez-Pinzón
@GPALegal

BOGOTÁ
Calle 67 # 7-35 Of. 1204
Edificio Caracol
Bogotá, Colombia
Tel: +57 601 319 2900

MEDELLÍN
Cra. 43A # 1- 50 Of. 209
San Fernando Plaza
Medellín, Colombia
Tel: +57 604 444 3815