Banca & Economía
2020
Edición 1244

La auditoría de la ciberseguridad

03 de agosto de 2020

• La masificación en el uso de la tecnología y el auge de la economía digital durante la última década han llevado a que la ciberseguridad se haya convertido en un eje central para el sector financiero. De hecho, en los últimos meses este tema ha pasado a un primer plano para las entidades del sector, ya que la pandemia del Covid-19 ocasionó que el número de ciberataques a nivel mundial se incrementara en un 38% entre marzo de 2019 y marzo de 2020.

• A nivel mundial diferentes organismos han realizado esfuerzos por estandarizar prácticas comunes para garantizar una adecuada gestión de la ciberseguridad. Un ejemplo de esto son los marcos del NIST, ISO e ISACA, cuya estructura puede servir como herramienta para la construcción de políticas y procedimientos de ciberseguridad a nivel local.

• En el caso colombiano, los ciberataques han sido igualmente numerosos. Según la Fiscalía, durante 2019 se reportaron 28.827 incidentes de ciberseguridad empresarial, entre los que se encuentran el hurto por medios informáticos, la violación de datos personales y el acceso abusivo al sistema informático. Según cifras recientes, esta situación se ha visto intensificada en 2020, ya que la pandemia ha sido aprovechada por los ciberdelincuentes para difundir noticias falsas, páginas web con contenido malicioso, entre otras.

• Con el fin de hacer frente a estas amenazas latentes, en Colombia se han presentado algunas iniciativas regulatorias enfocadas en fortalecer la gestión de ciberseguridad. En lo que compete a la banca, la Superintendencia Financiera de Colombia (SFC) expidió la Circular Externa N°007 de 2018, que establece los requerimientos mínimos para una adecuada administración del riesgo cibernético.

• Sin embargo, más allá de los avances alcanzados en materia normativa, esta situación pone de presente el importante rol que desempeña la Auditoría Interna de las organizaciones en la gestión de los riesgos emergentes derivados de la ciberseguridad, ya que debe contribuir a fortalecer los planes de acción ante el riesgo cibernético a partir de lineamientos y políticas que no solo integren todas las instancias de cada entidad (desde la alta gerencia hasta los usuarios), sino que se encuentren alineadas con los marcos internacionales de ciberseguridad.

Director:

Santiago Castro Gómez

ASOBANCARIA:

Santiago Castro Gómez
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

Para suscribirse a nuestra publicación semanal Banca & Economía, por favor envíe un correo electrónico a
bancayeconomia@asobancaria.com

Banca & Economía
2020
Edición 1244

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

Liz Bejarano Castillo
Sofía Rincón Coronado
Dayan Pachón Gómez

La auditoria de la ciberseguridad

Con el crecimiento del uso de la tecnología y el auge de la economía digital, la ciberseguridad se ha convertido en un eje central del negocio bancario que ha debido adaptarse para hacer frente al incremento en el volumen y la sofisticación de los ataques cibernéticos. Esta situación se ha visto intensificada debido a la pandemia del Covid-19, contingencia que ha sido aprovechada por los ciberdelincuentes para explotar las vulnerabilidades de las entidades financieras impactando gravemente sus sistemas a través de dominios maliciosos, malware y el secuestro de datos.

Según el informe "Delincuencia financiera en tiempos del Covid-19"[1] publicado por el Instituto de Estabilidad Financiera (BIS, por sus siglas en inglés), las amenazas cibernéticas relacionadas con el Covid-19 van en aumento, principalmente los ataques en *ransomware*, que en marzo de 2020 presentaron un incremento de 148% frente al mismo mes de 2019. Adicionalmente, el sector financiero es el que ha resultado más afectado, siendo el objetivo principal de los ciberataques, con un incremento del 38% respecto a marzo de 2019.

Por esta razón, es fundamental que las organizaciones cuenten con programas de auditoría robustos que permitan hacer seguimiento a los procesos asociados al riesgo cibernético. El informe "Enfoque de riesgos 2020"[2] , elaborado por la Confederación Europea de Institutos de Auditoría Interna (ECIIA, por sus siglas en inglés), concluyó que la ciberseguridad[3] y la seguridad de la información[4] continúan siendo uno de los principales riesgos a los que la Auditoría Interna debe dedicar más tiempo y esfuerzo.

[1] Instituto de Estabilidad Financiera (2020). "Delincuencia financiera en tiempos de Covid-19". Recuperado de: https://www.bis.org/fsi/fsibriefs7.pdf
[2] Confederación Europea de Institutos de Auditoría Interna (2020) "Enfoque de riesgos 2020". Recuperado de: https://auditoresinternos.es/uploads/media_items/risk-in-focus-2020.original.pdf
[3] "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." – Superintendencia Financiera de Colombia, Circular Externa N°007 de 2019.
[4] "Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad." – Superintendencia Financiera de Colombia, Circular Externa N°.07 de 2019.

Así, la persistencia de la amenaza cibernética y los costos financieros y reputacionales asociados requieren que la Auditoría Interna realice una gestión constante de este riesgo, aunque se presenten periodos de inactividad. Adicionalmente, es necesario que los auditores se mantenga al tanto de los cambios organizacionales y operativos que pueden afectar el perfil de riesgo de seguridad de la información de la empresa.

Esta edición de Banca & Economía brinda un contexto del estado actual de la ciberseguridad y recopila los marcos internacionales sobre los cuales deben apoyarse los planes de auditoría de las entidades financieras para, finalmente, presentar los avances del Instituto de Auditores Internos de España (IAIE), que sirven de insumo para definir el papel del auditor interno frente a este riesgo. Finaliza con algunas conclusiones en este frente.

Contexto de la ciberseguridad en el sistema financiero colombiano

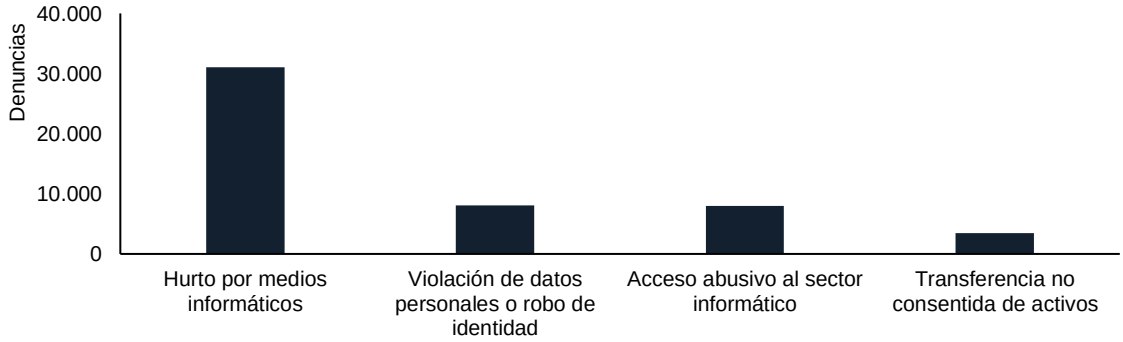
Los avances de la banca digital y los crecientes ataques cibernéticos han hecho que las entidades financieras se vean expuestas a pérdidas económicas, robos de datos y filtración de información confidencial. Según el estudio de "Tendencias del Cibercrimen en Colombia de 2019-2020"[5] el monto de pérdidas por ataques cibernéticos mediante la modalidad de compromiso de cuentas empresariales oscila entre los COP 120 millones y los COP 5.000 millones.

Asimismo, durante 2019 se reportaron 28.827 incidentes de ciberseguridad empresarial, de los cuales 17.531 casos fueron denunciados ante la Fiscalía General de la Nación. Dentro de los delitos informáticos más denunciados se encuentran: (i) el hurto por medios informáticos, con 31.058 denuncias; (ii) la violación de datos personales o robo de identidad, con 8.037 denuncias; (iii) el acceso abusivo al sistema informático, con 7.994 casos; y (iv) la transferencia no consentida de activos, con 3.425 denuncias (Gráfico 1).

De acuerdo con los más recientes boletines del Centro de Capacidades para la Ciberseguridad del Centro Cibernético de la Policía Nacional, a corte del 17 de abril de 2020 se habían detectado: (i) 212 noticias falsas desde la confirmación del primer caso de Covid-19 en Colombia; (ii) 220 alertas, generadas a través de redes sociales, prensa y canales de cooperación internacional, y (iii) 204 páginas web con contenido malicioso, de las cuales 104 fueron con *malware*, 76 con *phishing* y 24 con *spam*.

Por otra parte, la Interpol indicó que en marzo de 2020 su Unidad de Crímenes Financieros había respondido a 30

Gráfico 1. Delitos cibernéticos más denunciados durante 2019



Fuente: Policía Nacional. "Tendencias del Cibercrimen en Colombia de 2019-2020"

[5] Tendencias Cibercrimen Colombia 2019 – 2020. "Tendencias de Cibercrimen en Colombia 2019-2020". Recuperado de: https://caivirtual.policia.gov.co

casos, bloqueado 18 cuentas bancarias y congelado alrededor de 730.000 dólares por transacciones presuntamente fraudulentas. Al respecto, entre las modalidades identificadas por el organismo se resaltan las estafas telefónicas y correos con *phishing* y *malware*[6].

De esta forma, con el fin de hacer frente a las amenazas latentes, en Colombia se han presentado algunas iniciativas regulatorias enfocadas en fortalecer la gestión de ciberseguridad. Dentro de ellas se encuentran: (i) la Ley 1273 de 2009, que creó un nuevo bien jurídico titulado "la protección de la información y los datos"; (ii) la Ley 1581 de 2012, que dispuso mecanismos de protección para salvaguardar los datos personales registrados en cualquier base de datos; (iii) la Ley 1621 de 2013, que fortaleció el marco jurídico que permite a los organismos de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y (iv) el CONPES 3854 de 2016 que actualizó la política de ciberseguridad.

Adicionalmente, para el sector financiero se dispuso la Circular Externa N°007 de 2018 de la SFC, por medio de la cual se establecen los requerimientos mínimos que deben implementar las entidades supervisadas para una adecuada administración del riesgo cibernético.

Lo anterior da cuenta de que la ciberseguridad se ha convertido en un eje central de las organizaciones y que es necesario adoptar políticas internas para fortalecer la capacidad de identificar y responder a un ciberataque.

Marcos internacionales de ciberseguridad

Con la llegada de la era digital diferentes organismos internacionales han realizado esfuerzos por establecer buenas prácticas comunes para garantizar una adecuada gestión del riesgo cibernético. A continuación, se presentarán los tres marcos de ciberseguridad más relevantes desarrollados por entidades de estandarización que pueden servir como herramienta para la construcción de políticas y procedimientos de ciberseguridad a nivel local.

Marco para la mejora de la seguridad cibernética en infraestructuras críticas – NIST

El *"Marco para la mejora de la seguridad cibernética en infraestructuras críticas"*[7] (CSF) del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) es una herramienta para la gestión de riesgos de ciberseguridad de los Estados Unidos (EEUU), que habilita la innovación tecnológica y se ajusta a cualquier tipo de organización. Este fue concebido bajo algunos requerimientos como: (i) identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica; (ii) proporcionar un enfoque prioritario, flexible, repetible, basado en el rendimiento y rentabilidad; (iii) ayudar a identificar, evaluar y gestionar el riesgo cibernético; (iv) incluir orientación para medir el desempeño de la implementación del Marco de Ciberseguridad, e (v) identificar áreas de mejora que deben abordarse a través de la colaboración futura con sectores particulares y organizaciones que desarrollan estándares.

De esta forma, el CSF no plantea nuevos controles ni procesos, sino que agrupa los controles planteados por los principales estándares de la industria internacionalmente reconocidos, como son el NIST SP 800-53[8], ISO 27001 y COBIT 5, entre otros. A continuación se presentan los tres principales elementos que componen el CSF:

- *Framework Core*: es un conjunto de actividades y resultados de ciberseguridad deseados, organizados en categorías y alineados con referencias informativas a estándares aceptados por la industria.

- Niveles de implementación: describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización exhiben las características definidas en el Marco. Contemplan cuatro niveles: parcial, riesgo informado, repetible y adaptado.

- Perfiles: se refieren a la alineación de los objetivos organizacionales, la tolerancia al riesgo y la destinación

[6] Banca & Economía. Edición 1234. (2020). "Alianzas del sector público y privado para combatir el crimen financiero en tiempos del COVID-19". Recuperado de: https://www.asobancaria.com/wp-content/uploads/1234VF.pdf
[7] Instituto Nacional de Estándares y Tecnología (NIST). "Marco para la mejora de la seguridad cibernética en infraestructuras críticas". Recuperado de: https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf
[8] El marco NIST SP 800-53 dicta los controles de seguridad y privacidad para organizaciones y sistemas de información federales de Estados Unidos. Recuperado de: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

de recursos para conseguir los resultados deseados del *Framework Core*. Los perfiles se pueden utilizar para identificar oportunidades de mejora en materia de ciberseguridad comparando un perfil "actual" con un perfil "objetivo".

Adicionalmente, el *Framework Core* incluye cinco funciones, que actúan como la columna vertebral de los demás elementos (Gráfico 2).

Gráfico 2. Marco de ciberseguridad del NIST

Fuente: NIST. Marco para la mejora de la seguridad cibernética en infraestructuras críticas

- Identificar: permite desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. Las actividades que engloban esta función son fundamentales para el uso efectivo del marco.

- Proteger: describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento que atente a la ciberseguridad.

- Detectar: define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad, permitiendo su descubrimiento oportuno. Los ejemplos de categorías de resultados dentro de esta función incluyen: anomalías y eventos, monitoreo continuo de seguridad y procesos de detección.

- Responder: incluye actividades necesarias para tomar medidas frente a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial ataque. Algunos ejemplos de categorías de esta función son: planificación de respuesta, comunicaciones, análisis, mitigación y mejoras.

- Recuperar: permite identificar las actividades necesarias para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se haya deteriorado como consecuencia de un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

En este sentido, con el fin de implementar el CSF, el marco ha planteado algunas estrategias que facilitan su uso. Dentro de estas se destaca *la* "Creación o mejora de un programa de ciberseguridad"[9], que implica siete pasos para su ejecución y desarrollo: (i) priorizar y determinar el alcance; (ii) orientación; (iii) crear un perfil actual; (iv) realizar una evolución de riesgos; (v) crear un perfil objetivo; (vi) determinar, analizar y priorizar las brechas, e (vii) implementar el plan de acción.

Sin embargo, llevar a cabo dicha implementación también resulta ser un desafío dado que el CSF no utiliza ningún estándar específico para satisfacer los controles de ciberseguridad, lo que dificulta su adecuación a los diferentes sectores, industrias e incluso países.

De igual forma, este desafío se encuentra acompañado del compromiso de la alta dirección para la adopción de una estrategia de ciberseguridad, la cultura del riesgo

[9] Instituto Nacional de Estándares y Tecnología (NIST). "Un abordaje integral de la Ciberseguridad". Recuperado de: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

organizacional y la falta de profesionales calificados para poder liderar estos procesos, lo cual dependerá de cada jurisdicción.

ISO 27001:seguridad de la información

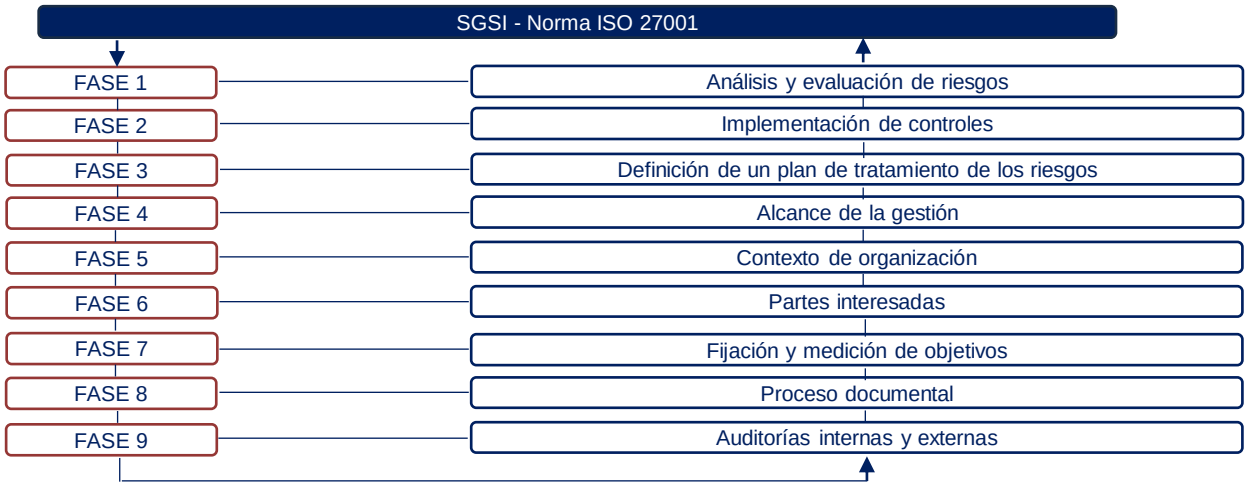
La Organización Internacional de Estandarización (ISO), a través de las normas recogidas en ISO 27001[10] (un marco internacional de las mejores prácticas para un sistema de gestión de seguridad de la información que ayuda a identificar y a reducir los riesgos), proporciona un Sistema de Gestión de la Seguridad de la Información (SGSI), que contempla medidas orientadas a proteger la información de una organización, tanto propia como de terceros, contra cualquier tipo de riesgo o amenaza, de tal manera que se garantice la continuidad de las actividades.

En este sentido, los principales objetivos del SGSI se enfocan en proteger la confidencialidad, integridad y disponibilidad de la información, por lo cual es un sistema basado en el ciclo de mejora continua. De acuerdo con lo anterior, el SGSI se fundamenta en nueve fases[11] para llevar a cabo su implementación, como se observa en el Gráfico 3.

Paralelo a las fases que se deben tener en cuenta para llevar a cabo la implementación de un SGSI, también es fundamental considerar como foco central de este sistema la evaluación de los riesgos, para lo cual se debe contar con una metodología apropiada para los requerimientos del negocio. Para esto, la norma sugiere una metodología específica, la cual debe identificar:

- Los activos de información y sus respectivos responsables.
- Las vulnerabilidades de cada activo que lo hacen susceptible de sufrir ataques o daños.
- Las amenazas contra la información.
- Los requisitos legales y contractuales que la organización está obligada a cumplir con sus clientes, socios o proveedores.
- Los riesgos, es decir, la probabilidad de que sus amenazas o vulnerabilidades puedan causar un daño total o parcial al activo de la información, en relación con su disponibilidad, confidencialidad e integridad.

Gráfico 3. Fases de un SGSI basado en la Norma 27001



Fuente: Norma ISO 27001. *"Aspectos clave de su diseño e implementación";* elaboración de Asobancaria.

[10] Normas ISO 27001. "ISO 27001 Seguridad de la Información". Recuperado de: https://www.normas-iso.com/iso-27001/
[11] Norma ISO 27001. "Aspectos clave de su diseño e implementación". Recuperado de: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Así mismo, esta metodología debe:

- Calcular el riesgo, a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = impacto x probabilidad de la amenaza).

- Tener un plan de tratamiento del riesgo, en el cual se seleccionen los controles adecuados para cada riesgo, los que a su vez estarán orientados a asumir, reducir, eliminar y transferir el riesgo.

En este sentido, la Gestión de Seguridad de la Información ISO 27001 genera algunos beneficios para las entidades, tales como: (i) identificación de los riesgos y determinación de controles para gestionarlos o eliminarlos; (ii) flexibilidad para adaptar controles a todas las áreas de la organización; (iii) muestra de cumplimiento y consolidación de estatus como proveedor preferido; y (iv) garantía de protección de datos a los clientes.

COBIT 5 – ISACA

La Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés) a partir de las referencias de NIST y de ISO 27001, publicó el documento “Implementando el Marco de Ciberseguridad del NIST usando COBIT 2019” que tiene el objetivo de integrar los estándares internacionales de ciberseguridad con los principios clave del marco COBIT 5, que involucra el gobierno con la gestión de las tecnologías de la información (TI) para evaluar el estado en que se encuentran la ciberseguridad en una organización.

De esta forma, el marco de COBIT 5 expone cinco principios que toda entidad debe seguir para adoptar una adecuada gestión de las tecnologías de la información:

1. Satisfacer las necesidades de los accionistas: el marco de ciberseguridad debe considerar las necesidades de los accionistas, alineando los objetivos y metas empresariales a los objetivos de TI a través del concepto “cascada de metas". De esta forma, plantea la optimización de recursos al obtener un nivel aceptable de riesgo.

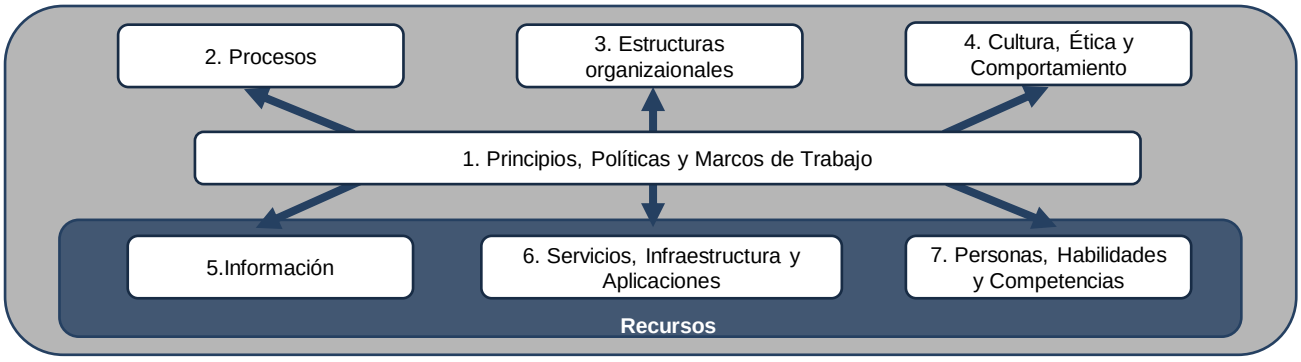
2. Considerar la empresa de extremo a extremo: el marco plantea que se deben tener en cuenta todas las funciones y procesos de la organización, asumiendo el gobierno de TI y la gestión de TI desde una perspectiva global, con el fin de cubrir todas las necesidades corporativas.

3. Aplicar un único modelo de referencia integrado: el marco COBIT 5 busca integrar e incorporar los estándares más relevantes de la industria, con el fin de que las empresas utilicen COBIT como un marco integral para el gobierno y la administración de las TI.

4. Facilitar un enfoque holístico: COBIT 5 propone unos habilitadores como factores mínimos para que el gobierno y la gestión de TI funcionen de manera correcta para optimizar los recursos y la información.

   De esta forma, COBIT 5 plantea establecer principios, políticas y marcos para la gestión de TI en el día a día

Gráfico 4. Enfoque Holístico COBIT 5



Fuente: ISACA – COBIT 5.

a través de la estructuración de procesos enfocados en la consecución de los objetivos de TI. Para ello, define unas estructuras organizacionales claves para las decisiones de gobierno y la necesidad de esparcir la cultura de TI en todos los empleados de la entidad. Lo anterior, con el fin de salvaguardar los recursos de la organización, como la información, los servicios, la infraestructura y las aplicaciones, y el activo más importante, las personas.

5. Separar el gobierno de la gestión: el gobierno es responsabilidad de la Junta Directiva, mientras la administración está bajo el liderazgo del CEO.

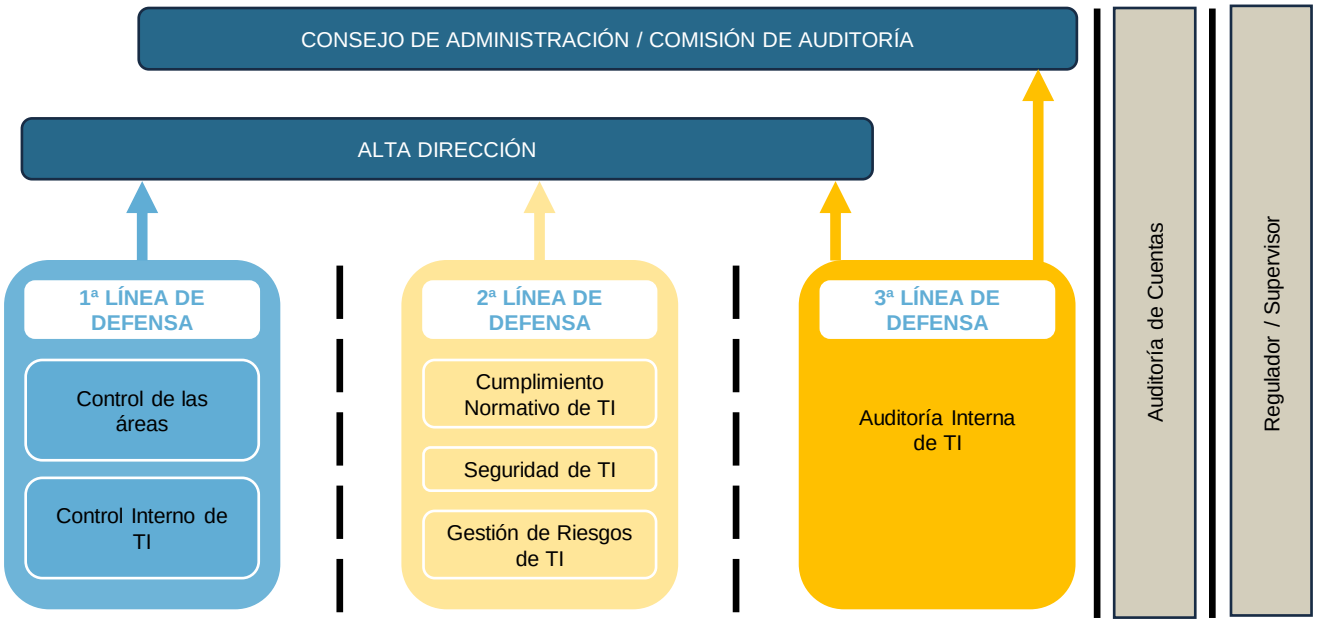
El rol del auditor interno frente a la ciberseguridad

Esta era digital presenta un importante reto para la gestión de la Auditoría Interna, la cual ha tenido que adaptar sus capacidades a los riesgos emergentes derivados de la ciberseguridad. Lo anterior no es ajeno al negocio bancario, que ha debido robustecer sus sistemas para afrontar el riesgo cibernético, no solo en materia de identificación de ataques, sino también en la creación de prácticas para instruir a toda la organización.

Como se evidenció en el apartado anterior, los ciberataques han generado que se construya un nuevo paradigma alrededor de la seguridad informática, que ya no solo debe basarse en chequeos regulatorios y controles, sino también en la implementación de metodologías que protejan la integridad de los sistemas, detecten y den respuesta efectiva a los incidentes.

En este contexto, la Guía de Supervisión[12] del IAIE puede servir de insumo para garantizar una gestión proactiva de la ciberseguridad, que vaya acompañada de la identificación anticipada de riesgos, la gestión continua de

Gráfico 5. Modelo de las Tres Líneas de Defensa adaptado al riesgo de la Ciberseguridad



Fuente: Confederación Europea de Instituciones de Auditoría Interna / Federación de Asociación de Gestión de Riesgos-2013.

[12] Instituto de Auditores Internos de España (IAIE). "Ciberseguridad: Guía de Supervisión". Recuperado de: https://auditoresinternos.es//

amenazas y la implementación de estrategias de ciber-resiliencia. De esta forma, al reconocer que la ciberseguridad es un tema transversal a todas las áreas de la organización, la guía propone adaptar el Modelo de las Tres Líneas de Defensa al riesgo cibernético, con el fin de establecer los controles necesarios para mitigar los riesgos derivados de la ciberseguridad.

En este sentido, la primera línea de defensa es la encargada de gestionar los riesgos en el día a día y la responsable de realizar procedimientos de control interno. Debe también poner en funcionamiento todas las medidas necesarias para que tanto los empleados como los usuarios sean conscientes de que son la puerta de entrada del riesgo cibernético. Para ello, necesita generar controles como la gestión de accesos y el cifrado de información, y promover la educación en materia de ciberseguridad, para propender por el uso adecuado de los dispositivos móviles, las redes wifi seguras, la apertura de correos electrónicos sospechosos, entre otras cosas.

La segunda línea de defensa compuesta por el área de gestión de riesgos, cumplimiento normativo y seguridad de los sistemas, debe establecer un modelo de aseguramiento que facilite la realización de revisiones proactivas de ciberseguridad, en donde se establezcan metodologías para monitorear los controles, proveer un mapa de riesgos completo, y establecer sistemas de reporte horizontal y vertical de incidentes que afecten la ciberseguridad.

Finalmente, la tercera línea de defensa que recae sobre la Auditoría Interna debe ser completamente independiente de las demás líneas y proveer garantías de control interno a los órganos de gobierno de la entidad. Para esto, es necesario alinearse con el modelo de aseguramiento definido por la segunda línea y evaluar sus bondades y deficiencias para establecer su Plan de Auditoría incorporando sus propios análisis y participando en ejercicios de revisión técnica que le permitan identificar riesgos no encontrados por las líneas inferiores.

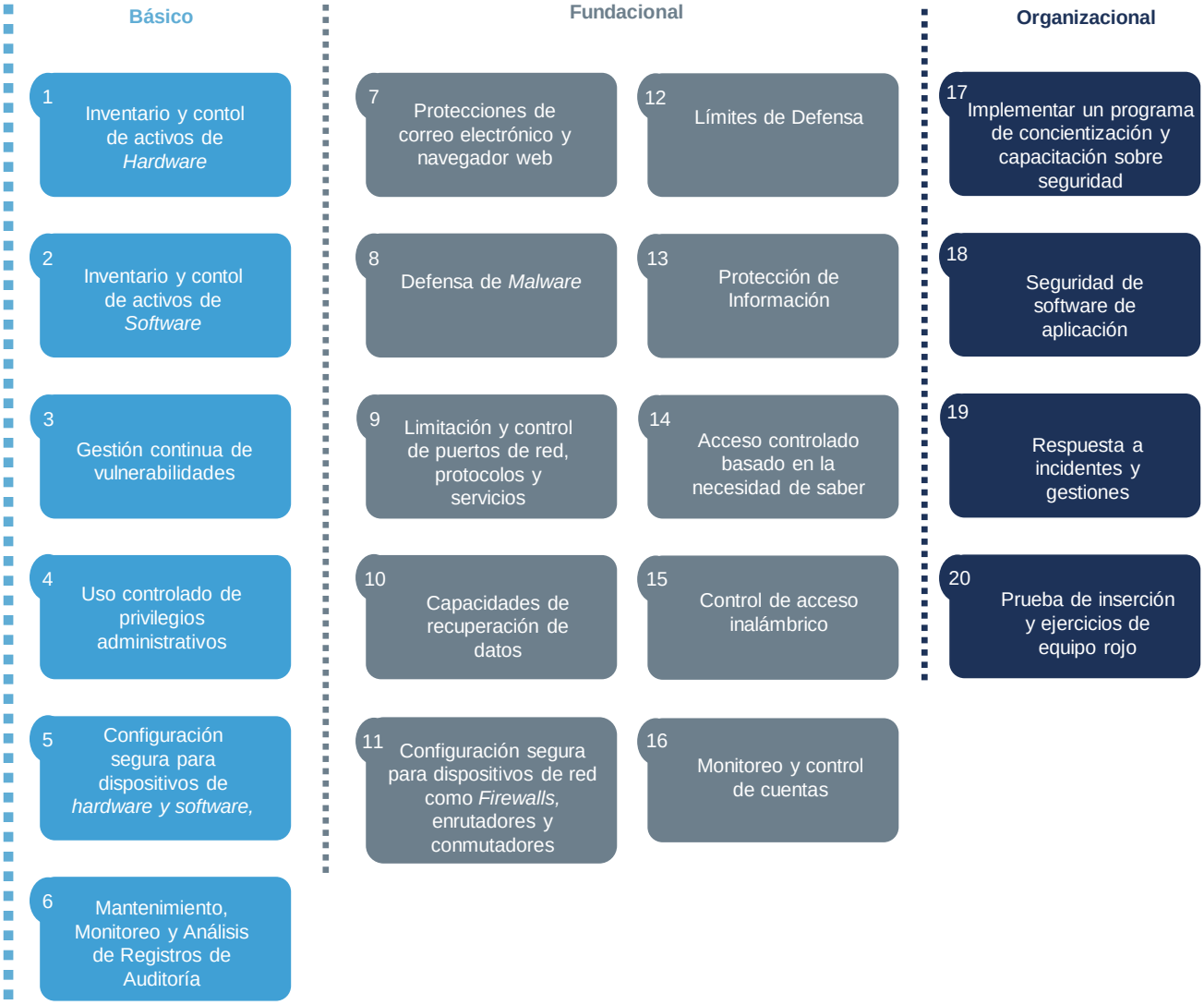
De esta forma, la Guía del IAIE propone algunas acciones mínimas que debería considerar la Auditoría Interna en materia de ciberseguridad:

- Ayudar a los órganos de gobierno en el diseño e implementación de la política de ciberseguridad.
- Asegurar que la entidad tiene la capacidad de identificar y mitigar del riesgo cibernético.
- Verificar los mecanismos diseñados para identificar incidentes internos y externos.
- Ayudar a concientizar a todas las áreas de la entidad, desde la alta dirección, sobre los riesgos cibernéticos para alcanzar los objetivos de la estrategia de ciberseguridad de la compañía.
- Integrar la ciberseguridad en el Plan de Auditoría de la entidad.
- Desarrollar el perfil de riesgo de ciberseguridad de la entidad, teniendo en cuenta las amenazas emergentes.
- Evaluar el programa de ciberseguridad con la ayuda de marcos internacionales como el NIST.
- Evaluar el enfoque preventivo de la organización en materia de educación, formación y concientización de los usuarios, y de las herramientas de control y vigilancia digital.
- Asegurar el monitoreo continuo y la adecuada gestión de incidentes.
- Identificar cualquier carencia de personal especializado en tecnologías de la información que pueda representar un impedimento para el cumplimiento de los objetivos de ciberseguridad.

En línea con lo anterior, el Centro de Seguridad del Internet (CIS, por sus siglas en inglés) propone 20 Controles Críticos de Seguridad[13] con los que se debería alinear el programa de aseguramiento de las entidades (Gráfico 6).

[13] Centro de Seguridad del Internet (CIS). “Los 20 controles y recursos CIS”. Recuperado de: https://www.cisecurity.org

Gráfico 6. 20 controles críticos de seguridad



Fuente: Centro de Seguridad del Internet (CIS). “Los 20 controles y recursos CIS”..

Estos controles varían de acuerdo con el tipo de organización y su exposición al riesgo, por lo cual es necesario diagnosticar su efectividad utilizando indicadores y métricas que permitan alcanzar los objetivos de ciberseguridad.

En los últimos años se ha destacado la importancia de cambiar el enfoque de ciberseguridad por el de ciber resiliencia. Bajo este nuevo panorama la auditoría no debería preguntarse si se presentará un ataque, sino cuándo sucederá. Este enfoque toma fuerza al evaluar las.

cifras del *"Pulso de la Auditoría Interna de 2020"*[14], en donde se concluye que el 32% de las entidades encuestadas no planean dedicar ningún recurso de auditoría a la seguridad cibernética, y cuando tienen un área de auditoría de TI, sus planes de continuidad del negocio no proporcionan ningún procedimiento para responder a un ciberataque.

En este sentido, se han propuesto nuevos modelos para auditar la ciberseguridad. Uno de ellos es desarrollado por Deloitte en el documento "Ciberseguridad: el cambio del rol del comité de auditoría y el auditor interno"[15], en el cual se define que las defensas cibernéticas deben cumplir con tres características:

- Aseguramiento: priorizar los controles sobre los riesgos conocidos y las amenazas emergentes, y cumplir con los estándares en materia de ciberseguridad dispuestos por la industria.

- Vigilancia: detectar violaciones o anomalías a través de la conciencia de que pueden presentarse situaciones de riesgos en todos los niveles de la organización.

- Resiliencia: establecer la habilidad de retornar rápidamente a la normalidad operacional, reparando los daños que puedan generarse en un ciberataque.

Bajo este modelo, es imperativo que el Auditor Interno tome liderazgo para determinar si existe un enfoque sistemático e interdisciplinario en la organización que evalúe y fortalezca la efectividad del riesgo cibernético. Así mismo, debe determinar si las capacidades de la entidad son apropiadas y están listas para proteger los sistemas contra las amenazas latentes.

Conclusiones y consideraciones finales

La pandemia del Covid-19 y el incremento de las amenazas cibernéticas dejan en un primer plano a la ciberseguridad, que se impone como uno de los principales retos de las entidades financieras que, sin dejar de hacer una adecuada gestión del riesgo cibernético, han debido adaptarse para satisfacer las necesidades de sus clientes, que requieren cada vez más servicios digitales.

En esta coyuntura, las áreas de la auditoría, tercera línea de defensa, han debido transformar sus procesos y adecuar sus capacidades para garantizar un control interno efectivo en materia de ciberseguridad. Si bien se han llevado a cabo esfuerzos significativos por construir políticas internas frente al riesgo cibernético, es necesario alinear los programas de aseguramiento con los marcos internacionales para garantizar la resiliencia de las organizaciones ante un ciberataque.

De esta forma, el Auditor Interno, más allá de proporcionar una revisión y evaluación independiente sobre la eficacia de las líneas de defensa, debe entender y hacer seguimiento al perfil de riesgo de la organización, teniendo en cuenta las nuevas tecnologías y los riesgos emergentes que impone la sofisticación de los ataques cibernéticos. Para lo anterior, se requiere una coordinación de todas las áreas de la entidad, desde la alta gerencia hasta los clientes, quienes forman parte del eslabón más débil de la cadena de la ciberseguridad.

[14] Instituto de Auditores Internos. "Pulso de la Auditoría Interna de 2020". Recuperado de: https://global.theiia.org
[15] Deloitte. "Ciberseguridad: el cambio del rol del comité de auditoría y el auditor interno". Recuperado de: https://www2.deloitte.com

Colombia
Principales indicadores macroeconómicos

	2016	2017	2018					2019*					2020*	
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	Total
Producto Interno Bruto**														
PIB Nominal (COP Billones)	**863,8**	**920,2**	231,1	234,3	248,8	264,3	**978,5**	271,8	279,5	286,4	288,9	**1126,6**	286,5	**1205,5**
PIB Nominal (USD Billones)	**287,0**	**308,4**	83,1	79,9	83,7	81,3	**301,1**	85,6	87,2	82,7	88,2	**343,8**	70,5	**305,4**
PIB Real (COP Billones)	**821,5**	**832,6**	197,7	207,8	214,9	233,5	**854,0**	203,0	214,7	222,1	241,7	**881,4**	205,2	**910,5**
PIB Real (% Var. interanual)	**2,1**	**1,4**	1,7	2,9	2,8	2,6	**2,6**	2,9	3,2	3,5	3,5	**3,3**	1,1	**3,3**
Precios														
Inflación (IPC, % Var. interanual)	**5,7**	**4,1**	3,1	3,2	3,2	3,2	**3,2**	3,2	3,4	3,8	3,8	**3,8**	3,6	**3,6**
Inflación sin alimentos (% Var. interanual)	**5,1**	**5,0**	4,1	3,8	3,7	3,5	**3,5**	3,3	3,2	3,3	3,3	**3,4**	3,3	**3,4**
Tipo de cambio (COP/USD fin de periodo)	**3010**	**2984**	2780	2931	2972	3250	**3250**	3175	3206	3462	3277	**3277**	4065	**3948**
Tipo de cambio (Var. % interanual)	**-4,4**	**-0,9**	-5,5	-3,5	1,2	8,9	**8,9**	14,2	9,4	16,5	0,8	**0,8**	28,0	**21,5**
Sector Externo (% del PIB)														
Cuenta corriente	**-4,2**	**-3,3**	-3,5	-3,9	-3,8	-4,4	**-3,9**	-4,5	-3,5	-5,0	-4,1	**-4,2**	-3,7	**-3,7**
Cuenta corriente (USD Billones)	**-12,0**	**-10,2**	-2,8	-3,3	-3,2	-3,7	**-13,0**	-3,5	-2,7	-4,0	-3,5	**-13,7**	-2,7	**-2,7**
Balanza comercial	**-4,5**	**-2,8**	-1,8	-2,6	-2,7	-3,5	**-2,7**	-3,5	-3,1	-4,9	-3,7	**-3,8**	-4,0	**-4,0**
Exportaciones F.O.B.	**14,8**	**15,4**	15,8	16,4	16,2	16,4	**16,2**	16,4	17,5	15,9	15,5	**16,2**	16,1	**16,1**
Importaciones F.O.B.	**19,3**	**18,2**	17,7	19,1	18,9	20,0	**18,9**	19,9	20,6	20,8	19,1	**20,0**	20,1	**20,1**
Renta de los factores	**-1,8**	**-2,7**	-3,7	-3,5	-3,4	-3,6	**-3,5**	-3,3	-3,2	-2,9	-3,3	**-3,1**	-2,7	**-2,7**
Transferencias corrientes	**2,1**	**2,1**	2,0	2,2	2,3	2,7	**2,3**	2,3	2,8	2,9	2,8	**2,7**	2,9	**2,9**
Inversión extranjera directa (pasivo)	**4,9**	**4,4**	2,5	4,6	3,3	3,4	**3,5**	4,3	5,2	4,0	4,5	**4,5**	4,9	**4,9**
Sector Público (acumulado, % del PIB)														
Bal. primario del Gobierno Central	**-1,1**	**-0,8**	0,0	0,1	0,0	-0,3	**-0,3**	0,0	0,9	1,4	0,4	**0,5**	...	**-5,9**
Bal. del Gobierno Nacional Central	**-4,0**	**-3,6**	-0,5	-1,6	-2,4	-3,1	**-3,1**	-0,6	-0,3	-1,2	-2,5	**-2,5**	...	**-8,2**
Bal. estructural del Gobierno Central	**-2,2**	**-1,9**	...	...	...	...	**-1,9**	...	...	...	...	**-1,5**	...	**...**
Bal. primario del SPNF	**0,9**	**0,5**	0,9	1,2	0,8	0,2	**0,2**	1,0	3,0	2,3	0,5	**0,5**	...	**-6,7**
Bal. del SPNF	**-2,4**	**-2,7**	0,3	-0,6	-1,2	-2,9	**-2,9**	0,4	0,6	-0,5	-2,4	**-2,4**	...	**-9,4**
Indicadores de Deuda (% del PIB)														
Deuda externa bruta	**42,5**	**40,0**	38,1	38,1	38,4	39,7	**39,7**	41,6	41,5	42,0	42,7	**42,0**	44,0	**44,0**
Pública	**25,1**	**23,1**	22,1	21,8	21,8	21,9	**21,9**	23,1	22,6	22,6	22,7	**22,8**	23,5	**23,5**
Privada	**17,4**	**16,9**	16,1	16,3	16,5	17,7	**17,7**	18,5	18,9	19,5	20,0	**19,2**	20,6	**20,6**
Deuda bruta del Gobierno Central	**44,1**	**44,9**	43,6	45,9	47,7	49,4	**46,7**	47,4	50,5	51,8	50,2	**50,0**	...	**...**

Colombia
Estados financieros del sistema bancario

	may-20 (a)	abr-20	may-19 (b)	Variación real anual entre (a) y (b)
Activo	**752.264**	**757.696**	**654.793**	**11,7%**
Disponible	52.641	65.555	46.530	10,0%
Inversiones y operaciones con derivados	163.531	154.500	126.210	26,0%
Cartera de crédito	507.859	508.032	459.177	7,5%
Consumo	147.640	149.099	133.150	7,8%
Comercial	278.478	277.309	250.094	8,3%
Vivienda	69.278	69.054	63.623	5,9%
Microcrédito	12.463	12.570	12.310	-1,6%
Provisiones	31.399	30.928	28.382	7,6%
Consumo	11.174	10.908	10.152	7,0%
Comercial	16.643	16.447	15.099	7,2%
Vivienda	2.536	2.497	2.261	9,1%
Microcrédito	1.046	992	871	16,8%
Pasivo	**661.150**	**666.663**	**571.324**	**12,5%**
Instrumentos financieros a costo amortizado	558.041	559.416	488.597	11,0%
Cuentas de ahorro	229.604	228.237	180.653	23,6%
CDT	163.951	160.732	160.509	-0,7%
Cuentas Corrientes	70.228	78.183	53.196	28,4%
Otros pasivos	10.216	10.346	9.364	6,1%
Patrimonio	**91.114**	**91.033**	**83.469**	**6,1%**
Ganancia / Pérdida del ejercicio (Acumulada)	**3.422**	**2.737**	**4.512**	**-26,3%**
Ingresos financieros de cartera	19.870	15.909	18.915	2,1%
Gastos por intereses	7.050	5.616	6.661	2,9%
Margen neto de Intereses	13.460	10.828	12.875	1,6%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**4,03**	**4,27**	**4,78**	**-0,75**
Consumo	3,66	4,03	5,24	-1,57
Comercial	4,15	4,40	4,81	-0,67
Vivienda	3,97	3,89	3,26	0,71
Microcrédito	6,03	6,32	7,16	-1,13
Cubrimiento	**153,5**	**142,6**	**129,2**	**-24,24**
Consumo	206,5	181,4	145,6	60,90
Comercial	144,1	134,8	125,4	18,67
Vivienda	92,3	93,1	109,1	-16,82
Microcrédito	139,2	124,8	98,8	40,44
ROA	1,10%	1,09%	1,66%	-0,6
ROE	9,25%	9,29%	13,47%	-4,2
Solvencia	13,97%	13,74%	15,07%	-1,1

Colombia

Principales indicadores de inclusión financiera

	2016	2017	2018					2019	2020				
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1
Profundización financiera - Cartera/PIB (%) EC	**50,2**	**50,1**	49,7	49,7	49,2	49,8	**49,8**	49,5	49,6	49,9	49,8	**49,8**	51,7
Efectivo/M2 (%)	**12,59**	**12,18**	12,40	12,07	12,27	13,09	**13,09**	12,66	12,84	13,20	15,05	**15,05**	13,35
Cobertura													
Municipios con al menos una oficina o un corresponsal bancario (%)	**99,7**	**100**	99,9	100	99,9	99,2	**99,2**	99,7	99,7	…	…	**…**	...
Municipios con al menos una oficina (%)	**73,9**	**73,9**	74,0	74,1	74,2	74,4	**74,4**	74,7	74,6	74,4	…	**…**	...
Municipios con al menos un corresponsal bancario (%)	**99,5**	**100**	99,9	100	98,2	98,3	**98,3**	100	100	…	…	**…**	…
Acceso													
Productos personas													
Indicador de bancarización (%) SF*	**77,30**	**80,10**	80,10	80,8	81,3	81,4	81,4	82,3	82,6	83,3	…	**…**	…
Indicador de bancarización (%) EC**	**76,40**	**79,20**	79,00	79,70	80,4	80,5	80,5	81,3	81,6	82,4	…	**…**	…
Adultos con: (en millones)													
Cuentas de ahorro EC	**23,53**	**25,16**	25,00	25,3	25,6	25,75	25,75	25,79	25,99	26,3	…	**…**	…
Cuenta corriente EC	**1,72**	**1,73**	1,74	1,81	1,8	1,89	1,89	1,95	2,00	2,00	…	**…**	…
Cuentas CAES EC	**2,83**	**2,97**	3,00	3,02	3,02	3,02	3,02	3,03	3,02	3,03	…	**…**	…
Cuentas CATS EC	**0,10**	**0,10**	0,10	0,10	0,10	0,71	0,71	2,10	2,32	2,54	…	**…**	…
Otros productos de ahorro EC	**0,77**	**0,78**	0,78	0,81	0,82	0,81	0,81	0,83	0,84	0,80	…	**…**	…
Crédito de consumo EC	**8,74**	**9,17**	7,23	7,37	7,47	7,65	7,65	7,82	8,00	8,16	…	**…**	…
Tarjeta de crédito EC	**9,58**	**10,27**	9,55	9,83	9,98	10,05	10,05	10,19	10,37	10,47	…	**…**	…
Microcrédito EC	**3,56**	**3,68**	3,41	3,50	3,49	3,51	3,51	3,49	3,48	3,50	…	**…**	…
Crédito de vivienda EC	**1,39**	**1,43**	1,34	1,37	1,38	1,40	1,40	1,41	1,43	1,45	…	**…**	…
Crédito comercial EC	**1,23**	**1,02**	0,65	0,67	0,66	…	…	…	…	0,69	…	**…**	…
Al menos un producto EC	**25,40**	**27,1**	26,8	27,2	27,5	27,64	27,64	28,03	28,25	28,6	…	**…**	…
Uso													
Productos personas													
Adultos con: (en porcentaje)													
Algún producto activo SF	**66,3**	**68,6**	67,1	68,0	68,4	68,5	68,5	69,2	69,8	70,4	…	**…**	…
Algún producto activo EC	**65,1**	**66,9**	65,7	66,6	67,1	67,2	67,2	67,8	68,4	69,2	…	**…**	…
Cuentas de ahorro activas EC	**72,0**	**71,8**	67,7	68,4	68,4	68,3	68,3	68,9	70,1	70,2	…	**…**	…
Cuentas corrientes activas EC	**84,5**	**83,7**	84,4	85,0	85,1	85,5	85,5	85,8	85,9	85,6	…	**…**	…
Cuentas CAES activas EC	**87,5**	**89,5**	89,7	89,8	89,8	89,7	89,7	89,8	89,9	82,2	…	**…**	…
Cuentas CATS activas EC	**96,5**	**96,5**	96.5	95,2	96,5	67,7	67,7	58,2	58,3	59,0	…	**…**	…
Otros pdtos. de ahorro activos EC	**66,6**	**62,7**	62,0	62,5	62,1	61,2	61,2	61,3	61,8	62,0	…	**…**	…
Créditos de consumo activos EC	**82,0**	**83,5**	82,0	81,5	81,8	82,2	82,2	81,7	81,9	81,8	…	**…**	…
Tarjetas de crédito activas EC	**92,3**	**90,1**	88,9	88,9	88,7	88,7	88,7	88,3	88,6	88,0	…	**…**	…
Microcrédito activos EC	**66,2**	**71,1**	71,2	70,4	69,4	68,9	68,9	68,9	69,2	68,9	…	**…**	…

Colombia

Principales indicadores de inclusión financiera

	2016	2017	2018					2019				2019	2020
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1
Créditos de vivienda activos EC	**79,3**	**78,9**	78,2	77,7	77,8	77,8	77,8	77,8	78,0	78,2	…	**…**	…
Créditos comerciales activos EC	**85,3**	**84,7**	59,2	58,7	57,6	…	…	…	…	61,2	…	**…**	…
Acceso													
Productos empresas													
Empresas con: (en miles)													
Al menos un producto EC	**751,0**	**775,2**	944,3	947,8	946,6	946,5	946,5	940,7	940,3	937,7	…	**…**	…
Cuenta de ahorro EC	**500,8**	**522,7**	649,7	647,7	648,9	…	…	…	…	…	…	**…**	…
Cuenta corriente EC	**420,9**	**430,7**	488,9	505,2	502,4	…	…	…	…	…	…	**…**	…
Otros productos de ahorro EC	**15,24**	**14,12**	14,4	14,1	14,0	…	…	…	…	…	…	**…**	…
Crédito comercial EC	**242,5**	**243,6**	265,3	272,2	276,5	…	…	…	…	…	…	**…**	…
Crédito de consumo EC	**98,72**	**102,5**	104,4	106,7	105,3	…	…	…	…	…	…	**…**	…
Tarjeta de crédito EC	**79,96**	**94,35**	102,1	104,4	105,1	…	…	…	…	…	…	**…**	…
Al menos un producto EC	**751,0**	**775,1**	944,3	947,8	946,6	…	…	…	…	…	…	**…**	…
Uso													
Productos empresas													
Empresas con: (en porcentaje)													
Algún producto activo EC	**74,7**	**73,3**	71,6	71,9	71,6	...	...	…	…	…	…	**…**	…
Algún producto activo SF	**74,7**	**73,3**	71,7	71,9	71,6	71,6	71,6	70,0	69,9	70,0	…	**…**	…
Cuentas de ahorro activas EC	**49,1**	**47,2**	48,1	47,7	48,2	…	…	…	…	…	…	**…**	....
Otros pdtos. de ahorro activos EC	**57,5**	**51,2**	50,8	49,5	49,5	…	…	…	…	…	…	**…**	…
Cuentas corrientes activas EC	**89,1**	**88,5**	88,5	88,2	88,6								
Microcréditos activos EC	**63,2**	**62,0**	58,5	58,5	57,2								
Créditos de consumo activos EC	**84,9**	**85,1**	83,7	83,4	83,7	…	…	…	…	…	…	**…**	…
Tarjetas de crédito activas EC	**88,6**	**89,4**	90,6	89,8	90,0								
Créditos comerciales activos EC	**91,3**	**90,8**	91,0	91,1	91,4	…	…	…	…	…	…	**…**	…
Operaciones (semestral)													
Total operaciones (millones)	**4.926**	**5.462**	- 2.926		- 3.406		**6.332**	-	3,952	-	4,239	**8,194**	-
No monetarias (Participación)	**48,0**	**50,3**	-	52,5	-	55,6	**54,2**	-	57,9	-	58,1	**57,9**	-
Monetarias (Participación)	**52,0**	**49,7**	-	47,4	-	44,3	**45,8**	-	42,1	-	41,9	**42,0**	-
No monetarias (Crecimiento anual)	**22,22**	**16,01**	- 18,66		-	30,9	**25,1**	-	48,6	-	29,9	**38,3**	-
Monetarias (Crecimiento anual)	**6,79**	**6,14**	-	6,30	-	7,0	**6,7**	-	19,9	-	17,6	**18,8**	-
Tarjetas													
Crédito vigentes (millones)	**14,93**	**14,89**	14,91	15,03	15,17	15,28	**15,28**	15,33	15,46	15,65	16,05	**16,05**	16,33
Débito vigentes (millones)	**25,17**	**27,52**	28,17	28,68	29,26	29,57	**29,57**	30,53	31,39	32,49	33,09	**33,09**	34,11
Ticket promedio compra crédito ($miles)	**205,8**	**201,8**	194,1	196,1	183,1	194,4	**194,4**	184,9	193,2	187,5	203,8	**203,8**	176,2
Ticket promedio compra débito ($miles)	**138,3**	**133,4**	121,2	123,2	120,3	131,4	**131,4**	118,2	116,3	114,0	126,0	**126,0**	113,6